L'émergence de l'identité numérique : l'influence de la révolution numérique sur l'environnement juridique

Batoul Betty Merhi

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

École de Droit de la Sorbonne
École Doctorale de Droit de la Sorbonne – Département de droit comparé

Thèse de doctorat en Droit comparé

Présentée et soutenue publiquement à Paris le 10 février 2022 par

Batoul Betty N. MERHI

« L'ÉMERGENCE DE L'IDENTITÉ NUMÉRIQUE. L'INFLUENCE DE LA RÉVOLUTION NUMÉRIQUE SUR L'ENVIRONNEMENT JURIDIQUE »

Membres du Jury :

Mme. Alexandra BENSAMOUN, *Professeure à l'Université Paris-Saclay*, *Rapporteure.*

Mme. Danièle BOURCIER, *Directrice de recherche émérite au CNRS (CERSA).*

Mme. Lucie CLUZEL-MÉTAYER, *Professeure à l'Université Paris Nanterre, Rapporteure.*

M. Thibault DOUVILLE, *Professeur à l'Université de Caen Normandie.*

M. Olivier RENAUDIE, *Professeur à l'Université Paris I Panthéon-Sorbonne, Directeur de recherche.*

Remerciements

Tout d'abord, je tiens à remercier mon directeur M. le Professeur Olivier Renaudie qui n'était pas mon directeur de recherche originel et qui a accepté de diriger mes travaux avec autant d'attention et de soin ; je tiens également à remercier ma directrice et « mère » académique et scientifique, Mme Danièle Bourcier qui, depuis notre rencontre en Master, m'a accompagnée, conseillée et guidée vers toutes les opportunités me permettant de développer et d'améliorer mes recherches ; notre « bien dévouée » et ange gardienne Mme Claire Flavigny qui a toujours été là pour l'ensemble de ses doctorants, nous motivant et nous orientant continuellement dans la bonne direction. C'est grâce à ces personnes que je suis venue à bout de mon travail et que j'ai réussi mon parcours doctoral et de recherche ; aussi, je ne les remercierai jamais assez pour tout ce qu'elles ont fait, pour la confiance, le soutien et la sollicitude qu'elles m'ont continuellement manifestées au fil des dernières années, et surtout, pour tout ce qu'elles sont, leurs identités respectives si uniques, inspirantes et motivantes. C'est une chance et un privilège que d'avoir travaillé avec elles.

Un grand merci à M. le Professeur Michel Borgetto qui a eu foi en ma personne et mes travaux, et m'a généreusement acceptée dans l'enceinte de son laboratoire de recherche – le CERSA – alors que je dépendais d'un autre ; et à M. le Professeur David Capitant pour toutes ses contributions à la réussite de ma thèse et de mon parcours doctoral et académique, en dépit des circonstances.

Je tiens à remercier mes parents, ma plus grande source de motivation comme de remise en perspective, ainsi que mes sœurs pour leur soutien et en particulier ma sœur Léa qui, en dépit de ses propres travaux de recherche, a pris le temps de relire ma thèse ; je tiens à lui transmettre tous mes sentiments d'appréciation et de gratitude pour le temps et l'énergie qu'elle m'a si gracieusement dédiés. Je remercie aussi Dara Somo, qui a été et est toujours là pour ma famille et moi, peu importe ce dont nous pourrions avoir besoin, elle l'a toujours généreusement fourni.

Je tiens également à remercier Jean et David Hilbert, et notamment Catherine Hilbert : je ne pense pas que je me serais sortie saine d'esprit et de corps de toute cette expérience sans votre présence dans ma vie, votre amitié et votre ouverture d'esprit et intelligence humaine. Et je remercie tout particulièrement Catherine pour son aide précieuse dans le travail de relecture et d'édition nécessaire à la mise au point de ce manuscrit de thèse. Un grand merci à Patrick Tabet et Romain Orhand pour votre écoute, votre attention ainsi que pour vos apports et contributions à mes réflexions scientifiques et personnelles.
Et, last but not least, un grand merci à Myriam Hilbert, "my person" et ma sœur de cœur, que je ne remercierai jamais assez pour tout ce qu'elle est, pour l'espace qu'elle fournit permettant d'être et de s'exprimer librement, et surtout, pour tout ce qu'elle m'apporte au quotidien à travers son amitié, sa personne et l'étendue de son savoir.

To A.J.E., Bassam M., Danièle B., Lina N. & Myriam H.,
and every human being who, similarly, acknowledge and teach that "Knowledge is Power"

In memory of Juddo A.M., R.N. & W.N., Amo M.N. & Khal R.N.

Liste des abréviations

ADN	Acide désoxyribonucléique
Adresses IP	*Internet Protocol address*
AI	*Artificial Intelligence*
AIPD	Analyse d'impact relative à la protection des données (ou PIA : *Privacy Impact Assessment*)
AJDA	Actualité juridique de droit administratif
AJ. pén.	Actualité juridique pénale Dalloz
Al.	Alinéa
A.N.	Assemblée nationale
APEC	*Asian-Pacific Economic Cooperation* – Coopération économique pour l'Asie-Pacifique
API	*Application Programming Interface* – Interface de programmation applicative ou Interface de programmation d'application
ARN	Acide ribonucléique
Ass. plén.	Assemblée plénière de la Cour de cassation
Art.	Article(s)
BCR	*Binding Corporate Rules* – Règles d'entreprise contraignantes
BNF	Bibliothèque nationale de France
Bull. civ.	Bulletin civil de la Cour de cassation
Bull. cri.	Bulletin criminel de la Cour de cassation
c.	Contre
Cass.	Cour de cassation
CBPR	*Cross Border Privacy Rules*
CDA	*Communications Decency Act*
CE	Communautés européennes
CEA	Commissariat à l'énergie atomique et aux énergies alternatives
CEDH	Cour européenne des droits de l'homme
CEPD	Contrôleur ou Comité européen de la protection des données (ou EDPB : *European Data Protection Board* ; EDPS *European Data Protection Supervisor*)
CERNA	Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene
CESE	Conseil économique, social et environnemental
Cf.	*Confer*
Ch.	Chambre
Ch. Crim.	Chambre criminelle de la Cour de cassation
Chap.	Chapitre(s)
CIA	*Central intelligence agency*
CJCE	Cour de justice des communautés européennes
CJUE	Cour de justice de l'Union européenne

CNAMTS	Caisse nationale d'assurance maladie des travailleurs salariés
CNCDH	Commission nationale consultative des droits de l'homme
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNIL	Commission nationale de l'informatique et des libertés
CNRS	Centre national de la recherche scientifique
CNRTL	Centre national de ressources textuelles et lexicales
Coll.	Collection
Cons.	Considérant(s)
Dalloz IP/IT	Revue Dalloz droit de la propriété intellectuelle et du numérique
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
Dir.	Direction (sous la)
DPD	Délégué à la protection des données (ou DPO : *Data Protection Officers*)
DPI	*Deep Packet Inspection*
ECTC	*European Counter Terrorism Centre*
Ed.	Édition ou Éditeur(s)
EDPB	*European data protection board*
ENFOPOL	Enforcement police (*European electronic intelligence network*)
EHESS	École des hautes études en sciences sociales
EPRS	*European parliamentary research service*
E-pub	Publicité en ligne
Etc.	Et cætera
ETSI	*European telecommunications standards institute* – Institut européen des normes de télécommunication
Ex.	Par exemple
FAI	Fournisseur d'accès internet
FBI	Federal bureau of investigation
FRA	*Försvarets radioanstalt* (*National Defence Radio Establishment*: Swedish national authority for Signals Intelligence)
fasc.	Fascicule
G29	Groupe de travail européen « article 29 » sur la protection des données
GAFAM	Acronyme pour désigner les géants du web – Google, Apple, Facebook, Amazon & Microsoft (auxquels il est possible de rajouter Netflix, Uber, etc.)
GATT	*General agreement on tariffs and trade* – Accord général sur les tarifs douaniers et le commerce
GCHQ	*Government Communications Headquarters* – Agence britannique de renseignement électronique
Http	*Hypertext transfer protocol*
IA	Intelligence artificielle
Ibid.	*Ibidem*, dans l'ouvrage cité précédemment
IBM	*International business machines corporation*
Id.	*Idem*, la même chose, au même endroit

IFOP	Institut français d'opinion publique
IMSI-Catcher	*International mobile subscriber identity-catcher*
In	Dans
Infra	Ci-dessous
INSERM	Institut national de la santé et de la recherche médicale
JO	Journal officiel
JORF	Journal officiel de la République française
JOUE	Journal officiel de l'Union européenne
LGDJ	Librairie générale de droit et de jurisprudence
Loc. cit.	*De loco citato*, au lieu cité
M€	Millions d'euros
Md€	Milliards d'euros
M^{e}	Maître (avocat de profession)
MIT	*Massachusetts institute of technology*
MIT Press	*University press affiliated with the Massachusetts institute of technology*
N°	Numéro – *Number*
NASA	*National aeronautics and space administration*
No.	Numéros
NSA	*National security agency*
OCDE	Organisation de coopération et de développement économiques
OECD	*Organisation for economic co-operation and development*
Op. cit.	*De opere citato*, dans l'ouvrage cité précédemment
p.	Page(s)
PIB	Produit intérieur brut
PLC	*Product life cycle* – Cycle de vie du produit
PME	Petites et moyennes entreprises
PNR	*Passenger name record* – Données des dossiers passagers
Primo	En premier lieu, premièrement
PUF	Presses universitaires de France
R&D	Recherche et Développement
RFDA	Revue française de droit administratif
RFID	*Radio-frequency identification*
RGPD	Règlement général sur la protection des données
RSC	Revue de science criminelle et de droit comparé
RSSI	Responsable de la sécurité des systèmes d'information
RTC	Réseaux téléphoniques commutés
s.	Suivant(es)
Secundo	En second lieu, deuxièmement
SIS	Système d'information Schengen
SLA	Sclérose latérale amyotrophique
SMS	*Short message service* – Service de messagerie
STE	Série des traités européens

STOA	Panel for the future of Science and Technology (STOA *Science and technology options assessment*) for the European parliament executed by Scientific Foresight Unit (STOA)
Sq.	*Sequiturque*, ce qui suit, et suivant
Supra	Ci-dessus
t.	Tome(s)
TFUE	Traité sur le fonctionnement de l'Union européenne
TIC	Technologies de l'information et de la communication
TPE	Très petite entreprise
Trad.	Traduit ou traduction
UE	Union européenne
UNCCT	*United Nations counter-terrorism center*
UNSA	Union nationale des syndicats autonomes
Vol.	Volume
§	Paragraphe
§§	Paragraphes

Sommaire

« Les personnes doivent jouir des mêmes droits fondamentaux lorsqu'elles ne sont pas connectées et lorsqu'elles sont en ligne. »[1]

« L'homme est une invention dont l'archéologie de notre pensée montre aisément la date récente. Et peut-être la fin prochaine. »[2]

[1] Conseil d'État, Étude annuelle 2014 – *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 35 : déclaration adoptée le 24 avril 2014 par les participants à la conférence « *NetMundial* » de Sao Paulo, « *Rights that people have offline must also be protected online* » (Note de bas de p. n°2), et le Conseil rajoute « *Cette affirmation a la force de l'évidence.* »

[2] M. FOUCAULT, *Les mots et les choses : Une archéologie des sciences humaines*, Ed. Gallimard, Coll. Bibliothèque des Sciences Humaines, 1966, p. 398.

Introduction

« *Chaque époque de l'histoire de l'humanité produit, par ses pratiques sociales quotidiennes et son langage, une structure imaginaire. La science est une section de ces pratiques sociales, et les théories scientifiques de la nature ne représentent qu'une dimension de cette structure imaginaire. […]. Ce qui est en général moins évident, c'est qu'à cette histoire humaine de la nature correspond une histoire des théories de la connaissance de soi. […]. Se reflétant l'un de l'autre, le* ***soi*** *et la nature évoluent dans le temps comme les partenaires d'une danse* » ; et l'observation de cette danse permet d'accéder à la connaissance, au savoir « *[…], dans la mesure où l'esprit humain est la source principale et l'exemple le plus accessible de la cognition et de la connaissance* »[3]. S'observe, à travers les développements suivants, l'histoire de l'humanité faisant émerger, à l'époque dite de la révolution numérique, le concept de l'identité numérique, objet principal de cette étude.

L'intérêt central de ce sujet est celui d'analyser l'influence opérée par les développements informatiques et technologiques, la mise en réseaux et la numérisation progressive et massive du monde, sur le droit en vigueur et les sociétés démocratiques, ainsi que sur les individus, dans leurs singularités, leurs constructions et développements personnels ; en somme, leurs identités humaines et tout ce qu'elles représentent socialement et légalement. Il est important de relever, d'ores et déjà, que « *telle la langue d'Ésope, l'informatique peut-être la meilleure comme la pire des choses. La pire parce qu'elle est un des symboles de cette société électronique qui, selon Marshall McLuhan, priverait « l'homme de son identité et de sa morale ». La meilleure, par les performances nouvelles qu'elle permet à la science et aux différentes techniques, notamment d'organisation* »[4].

L'avènement de l'Internet et des outils informatiques peut être autant une source de bienfaits pouvant aider, voire améliorer l'humanité, qu'une source d'atteintes et de préjudices aux droits et libertés les plus fondamentaux, aux êtres humains. Cela dit, les technologies en elles-mêmes n'ayant pas d'intention particulière d'usage ou de finalité, l'esprit humain de l'ingénieur et ses

[3] F. J. VARELA, *Invitation aux sciences cognitives*, Ed. du Seuil, Coll. Points sciences, nouvelle éd. 1996 (1989), p. 9-10.

[4] Rapport n° 72 de M. Jacques THYRAUD fait au nom de la Commission des lois, sur le projet de loi, adopté par l'Assemblée Nationale, relatif à l'Informatique et aux libertés, Sénat, Session de 1977-1978, déposé le 10 novembre 1977, p. 3 ; Disponible en ligne : https://www.senat.fr/rap/l77-072/l77-0721.pdf

intentions, ainsi que ceux du producteur et de l'utilisateur de ladite technologie imbibent implicitement le processus de construction technique. L'ère du numérique semble susciter de nouvelles tendances et stratégies relatives au mode, au style de vie des personnes ainsi qu'au mode de gouvernance des sociétés, soulevant de nombreuses questions, notamment en ce qui concerne les individus et leur droit au respect de leurs vies privées, mais aussi en ce qui concerne les sociétés et le respect des valeurs et des principes démocratiques et sociaux, à une époque de l'humanité où il est notamment question « d'individualisme connecté »[5]. En effet, « *protection […] of the dignity and integrity of the individual has become increasingly important as modern society has developed. All the forces of a technological age […] operate to narrow the area of privacy and facilitate intrusions into it. In modern terms, the capacity to maintain and support this enclave of private life makes the difference between a democratic and a totalitarian society* »[6].

Émerge donc la notion d'identité numérique dans différents secteurs et disciplines, ainsi que dans différents aspects de la vie des personnes, engageant une multitude de facettes identitaires aussi diverses que variées, transposées en données, métadonnées, voire en traces et signaux numériques, par le biais de la révolution numérique et, en particulier, des nouvelles technologies de l'information et de la communication développées et en développement. Il est, à ce stade, utile de noter que « *la technologie de l'information est seulement l'aspect le plus visible* [d'un] *vaste réseau de recherches et d'applications dont la connaissance, l'information et la communication occupent le centre* »[7] ; ces dernières forgeant le socle principal guidant la présente analyse centrée sur l'identité numérique, caractérisée par l'information ou la donnée personnelle, la communication et les réseaux sociaux, les représentations et les perceptions, la connaissance et le savoir de soi, de l'autre, de la légalité et de la réalité l'environnant à l'ère du numérique, et ayant un impact à long terme sur tous les niveaux de la société.

---

[5] P. FLICHY, "Connected Individualism between Digital Technology and Society", *In* Réseaux, Vol. n° 124, n° 2, 2004, p. 17-51; l'auteur explique ainsi que « *The sociological literature that seeks to characterize contemporary society often highlights two salient features: individuals and their identity, and networks. The former are studied mainly by sociologists of the family and private life; the latter by sociologists of the world of enterprise. I will nevertheless show that these two characteristics are often found together in the notion of "connected individualism".* », p. 17; Disponible en ligne: https://www.cairn-int.info/article-E_RES_124_0017--connected-individualism-between-digital.htm#

[6] T. I. EMERSON, « Nine Justices in Search of a Doctrine », *In* Michigan Law Review, Vol. 64, n° 219, Décembre 1965 (p. 219-234), p. 229; Disponible en ligne: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3762&context=fss_papers

[7] F. J. VARELA, *Invitation aux sciences cognitives*, *Id.*, p. 21.

Le développement et l'évolution des technologies ont induit le développement quantitatif, qualitatif et continu des données, de leur collecte et de leur utilisation soulignant de nombreuses problématiques et conséquences, et générateurs de nouveaux droits et libertés numériques tout en fragilisant l'équilibre juridique devant être maintenu entre les différents droits et libertés fondamentaux en vigueur. Le numérique représente, à l'ère du XXI^{e} Siècle, une composante de nos sociétés devenant progressivement partie intégrante des vies humaines. D'où, la question première du respect concret et effectif du droit à la vie privée qui se fait valoir, au regard des techniques et des pratiques numériques dorénavant mises en œuvre, notamment « *le traitement automatisé des informations*, [qui soulève] *des problèmes de collecte des données et d'utilisation de ces mêmes données* »[8], interceptant et recueillant, traitant et analysant toute donnée, et constituant, potentiellement, une ingérence dans la vie privée des personnes, voire une atteinte à leurs droits et libertés les plus fondamentaux. Pourtant, dès les années 60-70, la Cour européenne des droits de l'homme a bien souligné que « *la Convention a pour but de protéger des droits non pas théoriques ou illusoires, mais concrets et effectifs* »[9].

De plus, avec les dernières avancées numériques opérées, la problématique de l'informatique ne se réduit plus aux seules questions de mises en fichiers et d'entraves à la vie privée, « *en fait, l'informatique est plus que cela. Elle est aussi un fantastique outil de calcul et de communication […]* »[10], pouvant tracer, profiler, personnaliser, suggérer et ainsi de suite. Or, la Cour de justice des communautés européennes a eu l'occasion d'affirmer, depuis 1989, que « *l'objet de la protection de* [l'article 8 de la Convention, relatif au respect de la vie privée] *concerne le domaine d'épanouissement de la liberté personnelle de l'homme […]* »[11], élargissant, avant même le déploiement de l'Internet, le régime de protection relatif à la vie privée.

Face à la multiplication des nouvelles technologies et de la mise en réseau des humains, une mutation des sociétés, de ses valeurs, principes et paradigmes peut être constatée. Cela dit, existe depuis au moins 30 ans, spécialement en Europe, un cadre juridique instauré afin de fournir des garanties aux individus, et surtout afin de protéger expressément les êtres humains. Les juges européens ont ainsi souligné que « *la Convention doit se lire en fonction de son*

[8] Rapport n° 72 de M. Jacques THYRAUD, sur le projet de loi, adopté par l'Assemblée Nationale, relatif à l'Informatique et aux libertés, *Id.*, p. 8.
[9] CEDH, Affaire Airey c. Irlande du 9 octobre 1979, requête n° 6289/73, §24.
[10] Rapport n° 72 de M. Jacques THYRAUD, sur le projet de loi, adopté par l'Assemblée Nationale, relatif à l'Informatique et aux libertés, *Ibid.*, p. 7.
[11] CJCE, Affaire Hoechst *c.* Commission des Communautés européennes du 21 septembre 1989, affaires jointes 46/87 et 227/88 (Recueil 1989, p. 2924), §18.

caractère spécifique de traité de garantie collective des droits de l'homme et des libertés fondamentales (arrêt Irlande contre Royaume-Uni du 18 janvier 1978, […]). L'objet et le but de cet instrument de protection des êtres humains appellent à comprendre et appliquer ses dispositions d'une manière qui en rende les exigences concrètes et effectives (voir, entre autres, l'arrêt Artico du 13 mai 1980, […]). En outre, toute interprétation des droits et libertés énumérés doit se concilier avec "l'esprit général [de la Convention], destinée à sauvegarder et promouvoir les idéaux et valeurs d'une société démocratique" »[12].

Par ailleurs, un nouveau cadre ou « paquet européen »[13] relatif à la protection des personnes et de leurs données a été nouvellement mis en œuvre, aspirant à instaurer une « politique » de protection des données à caractère personnel. Dans ce contexte, et compte tenu du développement numérique massif dans tous les niveaux et aspects des sociétés modernes, l'ensemble de ces normes et garanties juridiques sera-t-il suffisant, *in concreto*, protégeant, à terme, les êtres humains de manière concrète et effective ?

Qu'advient-il de l'intégralité des données générées *via* les technologies de l'information ? Le traitement, qui est leur destinée première et ultime, risque d'affecter les sociétés, l'environnement juridique et social, voire les personnes dans leurs choix, dans leurs constructions et développements personnels, *in fine*, leurs identités. L'importance est donc d'analyser les effets de la révolution numérique, de manière assez globale, sur l'environnement juridique et social et, en particulier, à l'échelle de l'Homme, ses droits et libertés et sa singularité.

§1. État de l'art et définitions

Mouvement amorcé au XX^e^ Siècle, la révolution numérique, ou révolution informationnelle, englobe les technologies de l'information et de la communication mais ne s'y limite pas, et va bien au-delà, suscitant des progrès dans divers domaines et secteurs tels que l'intelligence artificielle, les objets connectés ou encore la robotique ou la santé. C'est une révolution comprenant le développement des nouvelles technologies et dispositifs informatiques, l'évolution de l'Internet et du cyberespace, ainsi que toutes les pratiques sociales élargies au monde numérique ; une révolution bien consolidée et avancée au XXI^e^ Siècle

[12] CEDH, Cour (Plénière), Affaire Soering *c.* Royaume-Uni du 7 juillet 1989, Requête n° 14038/88, §87.
[13] CNIL, « Le cadre européen » : « *Le « paquet européen de protection des données personnelles » se compose d'un règlement, applicable depuis le 25 mai 2018, qui fixe le cadre général de la protection des données (RGPD), ainsi que d'une directive, applicable uniquement aux fichiers de la sphère pénale (Directive « police-justice »*) » : https://www.cnil.fr/fr/cadre-europeen ; & *Cf.* p. 164.

présentant des capacités et des perspectives multiples, ainsi qu'un potentiel d'évolution et d'innovation inouï. En effet, « *la croissance rapide des technologies de l'information et de la communication et l'innovation dans les systèmes numériques sont à l'origine d'une révolution qui bouleverse radicalement nos modes de pensée, de comportement, de communication, de travail et de rémunération. Cette "révolution numérique" ouvre de nouvelles perspectives à la création du savoir, à l'éducation et la diffusion de l'information. Elle modifie en profondeur la façon dont les pays du monde gèrent leurs affaires commerciales et économiques, administrent la vie publique et conçoivent leur engagement politique. Elle permet de fournir rapidement une assistance humanitaire et des soins de santé et d'envisager autrement la protection de l'environnement. Elle offre même de nouveaux débouchés à l'industrie des divertissements et des loisirs. L'accès à l'information et au savoir, qui est indispensable à la réalisation des objectifs de développement énoncés dans la Déclaration du Millénaire, peut améliorer le niveau de vie de millions de personnes de par le monde* »[14] ; l'objectif ultime étant l'amélioration de la vie de l'être humain.

Le numérique, élément clé de cette thèse, se trouve donc au croisement d'une multitude de secteurs et de disciplines académiques ainsi que de nombreuses branches du droit, comme le droit pénal, le droit civil, le droit économique et commercial, les politiques publiques, le droit européen et international, les droits et libertés fondamentaux, occasionnant, *de facto* et *de jure*, plusieurs réformes et divers enjeux, de nature juridique, scientifique, philosophique, sociologique, technique ou éthique ; les développements de cette étude visent à en faire état. Étant donné qu'il conduit à la mise en donnée et à la mise en réseau générale du monde, notamment à travers la libre circulation des informations, des idées, des opinions et commentaires, et surtout des connaissances, le numérique soulève, en outre, de nombreuses interrogations, qu'il s'agisse du respect du droit en vigueur et de l'équilibre juridique à maintenir, ou de son utilisation récurrente et massive, et, en particulier, des différentes influences possibles qu'il a la capacité de provoquer sur le fonctionnement de la société et sur l'identité humaine.

[14] Sommet Mondial Sur la Société de l'Information (SMSI), Genève 2003 – Tunis 2005, « Qu'est-ce que la révolution numérique ? », ONU – UIT, Résolution 56/183 de l'Assemblée générale des Nations-Unies : http://www.itu.int/net/wsis/basic/faqs.asp?lang=fr), http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf & http://www.unesco.org/new/fr/communication-and-information/resources/multimedia/photo-galleries/world-summit-on-the-information-society-wsis/

Plus précisément, le numérique se définit « *comme la représentation de l'information ou de grandeurs physiques (images, sons) par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1. Sa puissance transformatrice tient à sa capacité à exprimer des réalités disparates (sons, images, textes, comportements humains, processus industriels …) dans un langage commun universel ouvrant la possibilité de les traiter de manière systématique et de les mettre en relation. Il en résulte des mutations techniques, économiques et sociales* »[15].

L'environnement numérique semble être alors porteur de plusieurs conséquences et changements, affectant, par ailleurs, des notions clés telles que celles de public et de privé, de frontière, de gouvernance, de représentation et de perception, de construction personnelle, d'autonomie, de sécurité, voire de traitement ; le tout en impactant la relation de chaque individu avec le monde, avec sa réalité telle que perçue et vécue. Autrement dit, « *les conséquences des bouleversements provoqués par les sciences, technologies, usages et innovations du numérique sont omniprésentes. La numérisation globale change l'expérience du monde qui nous entoure et exerce une pression formidable sur de nombreuses formes du rapport de l'humain au monde* »[16].

Symétriquement, un nouvel espace s'est mis en place, le cyberespace défini « *[…] par plusieurs pays comme un nouveau domaine (ou milieu) militaire, à côté de la terre, la mer, l'air et l'espace. Mais contrairement aux autres, ce n'est pas un milieu naturel – tout ce qui s'y passe est le produit de l'action humaine – et il est transverse à tous les autres domaines* »[17]. C'est donc un « *espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'internet, et par les données qui y sont traitées* »[18].

L'humain du XXI^{e} Siècle interagit continuellement et quotidiennement avec les machines et les technologies de l'information et de la communication, que ce soit dans le cadre de son travail, de ses relations personnelles et sociales, de ses démarches administratives et bancaires, de ses achats et loisirs, voire même de ses déplacements et comportements, de sorte que ce crée peu à peu une relation d'intimité et de dépendance à ces technologies, caractérisant la manifestation

[15] Conseil d'État, Étude annuelle 2014 – *Le numérique et les droits fondamentaux*, *op. cit.*, p. 9.
[16] CERNA, « La souveraineté à l'ère du numérique : Rester maîtres de nos choix et de nos valeurs », par J.-G. Ganascia, E. Germain et C. Kirchner, octobre 2018, p. 4 ; Disponible en ligne : http://cerna-ethics-allistene.org/digitalAssets/55/55708_AvisSouverainete-CERNA-2018.pdf
[17] F. DOUZET, « La géopolitique pour comprendre le cyberespace », *In* Hérodote N° 152-153, *Cyberespace : Enjeux géopolitiques*, La Découverte, 1er-2ème trimestre 2014, p. 13.
[18] Ministère des armées, « La Loi de programmation militaire de A à Z », du 08/02/2018, DICoD (dir.) : https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/le-lexique/la-loi-de-programmation-militaire-de-a-a-z

d'un Soi numérique connecté se développant dans l'espace numérique, et modifiant la manière dont l'être humain peut réfléchir, voire ressentir: « *along with the movement from a culture of calculation toward a culture of simulation have come changes in what computers do* ***for*** *us and in what they do* ***to*** *us – to our relationships and our ways of thinking about ourselves* »[19].

Les nouvelles technologies de l'information et de la communication représentent, substantiellement, un ensemble diversifié d'outils et de ressources technologiques employé pour transmettre, enregistrer, stocker, créer, partager ou échanger des informations ; ensemble comprenant, notamment, les ordinateurs et les machines, l'Internet (sites Web, blogs et courriels électroniques), les technologies de diffusion en direct (radio, télévision et diffusion sur le web), les technologies de transmission en différé (podcast, lecteurs audio et vidéo, et dispositifs de stockage) et la téléphonie (fixe ou mobile, satellite, visioconférence, etc.)[20]. Ces technologies se composent donc « *[…] de trois éléments : matériel informatique (ordinateurs et accessoires), équipement de communication et logiciel. L'élément logiciel se compose de logiciels standards, de logiciels sur mesure et de logiciels développés en interne* »[21].
Grâce aux dernières avancées technologiques entreprises, le dernier programme gouvernemental en matière de technologies de l'information et de la communication s'est modernisé, comprenant dorénavant six activités variées, nommément, « une nouvelle génération de composants et systèmes (ingénierie des systèmes embarqués et de composants et systèmes à faible consommation d'énergie) ; un calcul de nouvelle génération (systèmes et technologies de calcul avancés, inclus l'informatique en nuage) ; l'internet du futur (infrastructures, technologies et services) ; les technologies pour le contenu et la gestion de l'information (TIC pour le contenu digital et la créativité) ; les interfaces avancées et robotiques ; et, les technologies clés génériques (KET) liées à la micro et nanoélectronique et la photonique »[22] ; activités qui feront l'objet d'analyses à travers les différents développements de cette recherche, en vue d'observer leurs divers impacts sur la production, la gestion et le traitement des informations – informations provenant, essentiellement, de l'esprit humain et de l'activité humaine (mises en données). Par ailleurs, ce programme, tel qu'il est conçu, prévoit

[19] S. TURKLE, *Life on the Screen: Identity in the Age of the Internet*, New-York, Ed. Simon and Schuster, 1995, p. 22.
[20] UNESCO Institute of Statistics, Glossary " Information and communication technologies (ICT)" : http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict
[21] OCDE Données (2020), « Investissement dans les TIC (indicateur) » : https://data.oecd.org/fr/ict/investissement-dans-les-tic.htm#indicator-chart
[22] Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation, *Le programme Horizon 2020* « Technologies de l'information et de la communication – T.I.C. » : https://www.horizon2020.gouv.fr/cid72685/technologies-de-l-information-et-de-la-communication-t.i.c.html

deux évolutions principales : d'une part, « il est recentré autour de son cœur technologique, ainsi les activités menées autour de l'application des TIC en vue de répondre aux défis sociétaux comme l'eSanté, les TIC pour le transport et l'énergie ou encore les technologies de la langue, sont à présent intégrées directement dans six défis du pilier 3 : Santé, Énergie, Transport, Climat, Sociétés innovantes et inclusives, et Sécurité », et, d'autre part, « plusieurs activités du programme TIC seront mises en œuvre en étroite association avec l'industrie au travers de Partenariats public-privé et les Partenariats public-privé contractuels sur le Calcul à Haute Performance (*HPC-High Performance Computing*[23]), les télécoms, la photonique et la robotique »[24].

Tout individu s'avère ainsi être de plus en plus confronté à des enjeux et des défis majeurs qui impliquent le traitement de grandes quantités de données, disponibles en masse, et la réalisation de calculs complexes, de corrélations, d'interconnexions, de computations, créant de la sorte un « système », tout en soulevant de nombreux enjeux juridiques, et ce particulièrement au regard des objets et intérêts du traitement effectué ou encore du consentement du sujet. Il est utile de souligner que les nouvelles technologies, comprenant simultanément des « objets » matériels et immatériels « inter-reliés et solidaires », forment, individuellement, un système autonome, qui entretient des relations avec les autres sphères de l'activité sociale, tout en gardant son autonomie en raison de « la spécificité de ses lois de composition et d'évolution » ; en ce sens, « *la technologie engendre du fait de cette autonomie une dynamique de mouvement, de changement, qui est celle de la composante de l'innovation technologique, portée par la recomposition permanente des systèmes techniques et technologiques* »[25].
L'histoire du XXI[e] Siècle contemple l'avènement de technologies établissant un système ayant les capacités de s'auto-organiser et de s'autogérer : « *Un tel système ne requiert donc pas*

[23] European Commission, Factsheet "High Performance Computing PPP: Mastering the next generation of computing technologies for innovative products and scientific discovery", Digital Agenda for Europe, 2013: "*High Performance Computing (HPC) is a powerful tool helping us to respond to […] challenges* [that involve processing enormous amounts of data and carrying out complex computations] *in an effective way: researchers can study and understand complex phenomena with more precise simulations (e.g. designing new drugs "in silico" without animal testing); policy makers can take better decisions based on fast and accurate analysis (e.g. policies for transport planning or ageing population), and enables industry (in particular SMEs) to innovate in products and services (e.g. modelling safer cars or predicting the need of surgery for Caesareans to avoid riskier decisions at childbirth)*.": http://ec.europa.eu/research/press/2013/pdf/ppp/hpc_factsheet.pdf & https://ec.europa.eu/commission/presscorner/detail/fr/IP_13_1261
[24] Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation, *Le programme Horizon 2020* « Technologies de l'information et de la communication – T.I.C. » : *Id.*
[25] S. AÏT-EL-HADJ, « De la théorie du système technique à la systémique technologique. Une formalisation pertinente pour rendre compte de l'innovation technologique », *In* Innovations, Vol. 46, n° 1, 2015 (p. 227-250), p. 227 §§ 1 et 2 ; Disponible en ligne : https://doi.org/10.3917/inno.046.0227

d'unité centrale de traitement pour contrôler son fonctionnement. Ce transfert de règles locales à la cohérence globale est le cœur de ce qu'il était convenu d'appeler l'auto-organisation pendant les années de la cybernétique. Aujourd'hui, on préfère parler de propriétés émergentes ou globales, de réseaux dynamiques, ou non linéaires, de système complexes, ou encore même de synergétique »[26] ; des propriétés, réseaux et systèmes trouvant naturellement leurs places centrales et leurs rôles essentiels à l'époque de la société de l'information, la société numérisée. Ces nouvelles technologies forment ainsi un système autonome, auto-organisé, capable d'effectuer une multitude de traitements informatiques automatisés et computationnels, portant sur des données à caractère personnel, disponibles en quantité innombrable, et pouvant être continuellement réutilisées. En outre, « *le traitement computationnel est une opération qui est effectuée sur des symboles, c'est-à-dire sur des éléments qui représentent ce à quoi ils correspondent. La notion en jeu ici est la représentation, ou l'intentionnalité, terme du philosophe pour la qualité de ce qui est « à propos de quelque chose »* »[27] ; des représentations qui, comme il sera vu dans cette étude, constituent des processus permettant d'aboutir à la connaissance, particulièrement de soi, de son environnement et de sa réalité, consacrant par conséquent l'étude de l'identité et de la réalité sociale l'environnant.

En effet, la cognition, qui se réfère au « *processus d'acquisition de la connaissance* »[28], notion clé en matière numérique, « *[…] consiste à agir sur la base de représentations (d'un monde extérieur prédéterminé) qui ont une réalité physique sous forme de code symbolique dans un cerveau ou une machine. […]. En d'autres termes, si nous prétendons que les états intentionnels ont des propriétés causales, il nous faut montrer non seulement comment ces états sont physiquement possibles, mais aussi comment ils peuvent déterminer un comportement. C'est ici que la notion de computation symbolique intervient : les symboles ont une réalité à la fois physique et sémantique et la computation est conditionnée par cette réalité sémantique. […]. L'hypothèse est donc que les ordinateurs offrent un modèle mécanique de la pensée, ou, en d'autres mots, que la pensée s'effectue par une computation physique de symboles* »[29] ; computation qui, à l'heure du tout numérique, semble provoquer et conditionner à son tour, suivant le procédé de rétro-conception ou de rétro-ingénierie[30], la réalité de la personne

[26] F. J. VARELA, *Invitation aux sciences cognitives*, *op. cit.*, p. 61.
[27] F. J. VARELA, *Invitation aux sciences cognitives*, *Id.* p. 37.
[28] CNRTL, « Cognition » : https://www.cnrtl.fr/definition/cognition
[29] F. J. VARELA, *Invitation aux sciences cognitives*, *Id.* p. 38-39.
[30] Vocabulaire de l'informatique et de l'internet (liste de termes, expressions et définitions adoptés), Art. I, « rétro-ingénierie, n.f. » : « *Domaine : Informatique-Industrie ; Synonyme : ingénierie inverse ; Définition : Ensemble des opérations d'analyse d'un logiciel ou d'un matériel destinées à retrouver le processus de sa conception et de sa fabrication, ainsi que les modalités de son fonctionnement ; Équivalent étranger : reverse*

concernée par le traitement computationnel, informatique, effectué, alors que les juridictions et la Loi, notamment françaises et européennes, prônent et prévoient la protection du « domaine d'épanouissement de la liberté personnelle de l'homme »[31]. De plus, étudier « *[...] la dynamique d'un système à partir d'inter-connexions aléatoires* [démontre] *que celles-ci laissaient apparaître des comportements globaux cohérents* »[32], dynamique qui, tel qu'il sera observé, irrigue âprement la plupart des opérations de traitement de données effectuées de nos jours, faisant, par conséquent, émerger de nouveaux modèles, concepts, paradigmes, politiques, représentations ou conceptions, axés sur le numérique.

Notion élaborée par les sciences cognitives dans les années 70, l'émergence s'entend comme le « fait, l'action de venir à l'existence ; l'apparition d'un état de fait d'ordre social ou historique »[33]. Philosophiquement, elle correspond à l' « *apparition d'un état ou d'un être qualitativement différent et irréductible à l'état ou à l'être dont il procède* »[34], ce qui est le cas des identités numériques émergentes, prolongements du soi dans le monde numérique, mais qui ne peuvent être réduites à un seul dossier ou à un seul profil, voire à un traitement de données unique et uniforme, ou encore à une définition figée, à un humain réductible[35].

§2. Esprit et cadre de la recherche

La connaissance de soi, de son identité, incarne, en elle-même, une question aussi complexe que centrale, sujette fréquemment à des évolutions, des développements, des constructions, des influences, des mutations et métamorphoses, principalement compte tenu du fait que « *la prise de conscience d'une identité se fait dans et par une interaction continuelle de l'individu avec son environnement* »[36]. L'éclosion des nouvelles technologies dans le quotidien des individus a encore plus bouleversé cette quête naturellement continue de la connaissance, du soi et de sa réalité, en rajoutant une couche de complexité : les constructions et développements identitaires s'opèrent désormais dans un double espace, physique et numérique, générant ainsi la mise en place dudit système numérique révolutionnaire

engineering. », JORF n°0001 du 1 janvier 2013, Texte n° 114 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000026872471/

[31] CJCE, Affaire Hoechst *c.* Commission des Communautés européennes du 21 septembre 1989, *Id.,* §18 ; *Cf.* p. 12, et Note de bas de p. n° 9.

[32] F. J. VARELA, *Invitation aux sciences cognitives*, *Ibid.,* p. 54.

[33] CNRTL, « Émergence » : https://www.cnrtl.fr/definition/emergence

[34] CNRTL, « Émergence » : *Id.*

[35] *Cf.* M. DELMAS-MARTY, concept de « l'irréductible humain », p. 30 et Note de bas de p. n°75.

[36] M. ZAVALLONI et C. LOUIS-GUÉRIN*, Identité sociale et Conscience : Introduction à l'égo-écologie*, Montréal, Presses Universitaires de Montréal, 1984, (284p.).

provoquant, conséquemment, l'émergence de l'identité numérique, puisque « *c'est simplement l'existence du système lui-même qui les a fait émerger à partir d'une masse indéfinies de possibles* »[37], dans ce contexte, la masse indéfinie de données disponibles.

De façon similaire, la numérisation de la société a, potentiellement, des effets sur la vie des personnes, et surtout sur leurs constructions, perceptions, représentations, autonomies, choix et décisions, ainsi que sur leurs libertés, étant donné que « *c'est le processus continu de la vie qui a modelé notre monde par ces aller et retour entre ce que nous appelons, depuis notre perspective perceptuelle, les contraintes extérieures et l'activité générée intérieurement* »[38]. Ceci dit, il est nécessaire de laisser le choix du résultat, l'aboutissement de ce jeu d'aller et retour, à la personne concernée afin qu'elle en déduise les conséquences souhaitées et privilégiées en vue de se construire et de se développer, et ce, de manière libre et autonome. Dès lors, « *en insistant sur le fait qu'un processus historique fait émerger des régularités sans contrainte de finalité arrêtée, on conserve la notion biologique d'un monde non circonscrit* »[39], monde qui caractérise la notion d'identité, en constante évolution et toujours entendue de manière apophatique, et qui s'étend au monde numérique en raison des régularités technologiques, informatiques, instaurées dans le monde des humains faisant, subséquemment, émerger la notion d'identité numérique[40] ; le tout devant être, bien évidemment, évalué « *[…] en référence à un aspect de la réalité de l'environnement qui est pris pour acquis : des propriétés exogènes correspondant à des propriétés prédéfinies du monde, et une activité endogène qui atteint au fil de l'expérience un état de signification abstraite, une « codification optimale de la régularité de l'environnement »* »[41].

Un des objectifs majeurs de cette étude est ainsi d'appréhender l'influence de l'environnement numérique sur l'environnement juridique et humain, et particulièrement à travers sa faculté à « *[…] faire-émerger la signification, c'est donc que l'information n'est pas préétablie comme un ordre intrinsèque, mais qu'elle correspond aux régularités émergeant des activités […] elles-mêmes. Comme on devrait maintenant l'avoir compris, c'est ce recadrage qui comporte de multiples conséquences scientifiques, techniques et philosophiques autant qu'éthiques* »[42].

---

[37] F. J. VARELA, *Invitation aux sciences cognitives*, *Id.,* p. 106.
[38] F. J. VARELA, *Invitation aux sciences cognitives*, *Ibid.,* p. 104-105.
[39] F. J. VARELA, *Invitation aux sciences cognitives*, *Ibid.,* p. 116.
[40] *Cf.* p. 41.
[41] F. J. VARELA, *Invitation aux sciences cognitives*, *Ibidem,* p. 117.
[42] F. J. VARELA, *Invitation aux sciences cognitives*, *Ibidem,* p. 122-123.

Un environnement qui désigne un contexte, l' « *ensemble des éléments et des phénomènes physiques qui environnent un organisme vivant, se trouvent autour de lui* », se réfère, notamment, à l' « *ensemble des conditions matérielles et des personnes qui environnent un être humain, qui se trouvent autour de lui* »[43]. Il correspond, dans cette étude, au cadre juridique, entendu largement dans son approche de phénomène social, synonyme de science juridique, « *adjectif révélant que l'expression qu'elle qualifie est relative au droit dans son sens le plus large* »[44]. Un environnement juridique vise alors l'ensemble des règles de droit, nationales, européennes ou internationales, les acteurs de la vie juridique, les membres composant une société, les mécanismes juridiques, les différentes sources d'obligations et régimes de responsabilités ; c'est donc un ensemble qui sert à gouverner la société, à construire le social et à régir les rapports entre les hommes.

Dans cette acceptation, l'environnement juridique, impacté par le numérique et les technologies de l'information et de la communication, englobe dans le cadre de cette recherche, le droit pénal, le droit privé et public, le droit européen et international, les droits et libertés fondamentales, le droit dit du numérique invoquant des régimes de protection préexistants et nouvellement mis en œuvre ; environnement qui, parallèlement, implique et engage des concepts fondamentaux, également influencés par la révolution numérique, tels que ceux de souveraineté, de surveillance, de politique publique, de défense sociale ou encore de gouvernance.

Comme il sera observé à travers cette recherche, le nouveau « paquet européen »[45], prévoyant le régime de protection des données susmentionné, aspire à transposer dans le nouvel environnement juridique des méthodes, pratiques et obligations teintées de numérique, afin de respecter les règles prévues, mettant ainsi en place « *[…] un nouveau modèle de gouvernance, qui à la fois renforce les autorités nationales mais aussi les oblige à coopérer entre elles sur les cas transfrontières* »[46].

De même, il s'avère que moyennant les développements et les innovations technologiques, et tout le potentiel continuellement exploitable qu'offre régulièrement le numérique y compris en termes de gestion et d'auto-organisation, « *la notion de gouvernement se simplifie : le nombre*

[43] CNRTL, « Environnement » : https://www.cnrtl.fr/definition/environnement

[44] S. GUINCHARD et T. DEBARD (dir.), *Lexique des Termes Juridiques*, « juridique », Paris, Dalloz, 19ème Ed., 2012, p. 504.

[45] CNIL, « Le cadre européen », *op. cit.* ; *Cf.* Note de bas de p. n° 13, p. 13.

[46] I. FALQUE-PIERROTIN, « Interview de Madame Isabelle Falque-Pierrotin, Présidente de la CNIL », Dalloz IP/IT 2018, p. 5 ; & *Cf.* p. 230.

seul fait la loi et le Droit. Toute la politique se réduit à une question d'arithmétique »[47] ; le recours aux pratiques d'arithmétique et de calcul étant, dorénavant, également constaté dans l'économie numérique et l'économie des données, comme le montrent les développements à suivre[48]. Ces procédés évoquent, par ailleurs, à l'époque de la société de l'information et du développement du Big data, les questions de souveraineté, de surveillance et de sécurité, mobilisant autant le concept de souveraineté numérique que celui de la « guerre de tous contre tous »[49], au sens que lui rattache Hobbes : « *Ce que Hobbes appelle la guerre de tous contre tous n'est aucunement une guerre réelle ou historique, mais un jeu de représentations par lequel chacun mesure le danger que chacun représente pour lui, estime la volonté que les autres ont de se battre et jauge le risque que lui-même prendrait s'il avait recours à la force. La souveraineté – qu'il s'agisse d'une « république d'institution » ou d'une « république d'acquisition » – s'établit, non point par un fait de domination belliqueuse, mais au contraire par un calcul qui permet d'éviter la guerre. C'est la non-guerre pour Hobbes qui fonde l'État et lui donne sa forme* »[50].

Ces nouvelles stratégies et pratiques numériques et économiques se retrouvent, simultanément, dans la nouvelle politique publique adoptée ces dernières années, prévoyant entre autres, l'évolution de la cyberdéfense et de la cybersécurité, la mise en œuvre d'une coopération internationale en matière de défense, de sécurité et de sécurité civile et de sécurité numérique[51], avec pour mission centrale : le développement des secteurs technologiques, le développement de l'industrie de défense, le développement des partenariats privé-public, et celui du secteur de la surveillance, notamment des communications[52], impliquant l'interception, la collecte et le traitement de données mais aussi de métadonnées, nommées également « données des

[47] A. DE TOCQUEVILLE, *Considérations sur la Révolution* (1850-1858), I, 5, *In Œuvres*, t. 3, Paris, Ed. Gallimard, Coll. Bibliothèques de la Pléiade (n°503), 2004, p. 492.
[48] *Cf.* p. 102 et s. et p. 400 et s.
[49] *Cf.* p. 318 et s. et p. 462 et s.
[50] M. FOUCAULT, *Il faut défendre la société*, Cours au Collège de France 1975-1976, Coll. Hautes Études, EHESS, Gallimard – Seuil 1997, Résumé du Cours - p. 243.
[51] Conseil des Ministres - Communiqué de Presse, « Programmation Militaire pour les années 2019 à 2025 et dispositions intéressant la défense », du 8 février 2018 : https://www.gouvernement.fr/conseil-des-ministres/2018-02-08/programmation-militaire-pour-les-annees-2019-a-2025-et-dispo & https://circulaire.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000036584151/
[52] Assemblée générale des Nations-Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, du 17 avril 2013, Conseil des droits de l'homme 23ème session, A/HRC/23/40, p. 3, point 6 a) : « *Surveillance des communications: contrôle, interception, collecte, sauvegarde et conservation de l'information qui a été communiquée, retransmise ou recueillie sur les réseaux de communication* » ; disponible en ligne : https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/04/PDF/G1313304.pdf?OpenElement & https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

communications ». Ces dernières se réfèrent nommément aux « *renseignements sur les communications d'un individu (courriers électroniques, appels téléphoniques et messages textes envoyés et reçus, messages sur les réseaux sociaux et courrier postal), identité, comptes réseau, adresses, sites Web visités, livres et autres documents lus, consultés ou écoutés, recherches effectuées, ressources utilisées, échanges (origines et destinations des communications, personnes fréquentées, amis, famille, connaissances), et localisation temporelle et géographique d'un individu (notamment sa proximité avec les autres)* »[53].

Or, le secteur de la surveillance ne se réduit plus au seul secteur de la défense et de la sécurité nationales mais comprend, depuis la révolution numérique, une multitude de domaines, tels que les banques, l'emploi, l'e-énergie et les services publics, le divertissement, la finance, l'administration, la santé, l'assurance, les médias et la technologie, la fabrication, la police et la justice, le commerce de détail, les télécommunications, les transports et les voyages[54], s'assimilant de fait à une industrie et évoquant le concept de « capitalisme de surveillance »[55]. En d'autres termes, « *the surveillance sector covers goods, services and technologies used to monitor information, communication and people. These may be used for law enforcement and defence purposes, but also for commercial purposes, such as understanding customers' behaviour and preferences. As such, the surveillance sector is both a sub-set of the defence and security sector and an independent entity* »[56].

L'objet de cette recherche n'est pas d'étudier ou de déterminer les technologies de l'information, ou encore l'identité numérique telle qu'elle est communément perçue à l'heure actuelle, dans son acceptation purement informatique visant une authentification ou une identification et préconisant sa centralisation, mais bien de contribuer à la « *réflexion sur les relations entre l'informatique et les libertés* », entre les technologies et l'individu, ou encore entre les individus connectés et leurs droits, « *[…] c'est-à-dire entre une exigence permanente*

[53] Assemblée générale des Nations-Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, du 17 avril 2013, *Id.*, p. 3, point 6 b).
[54] R. RODRIGUES, "The Surveillance Industry in Europe", *In* Surveillance, Fighting Crime and Violence, IRISS-Increasing Resilience in Surveillance Societies, 17 décembre 2012 (p. 71-158), p. 89; Disponible en ligne : https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/Surveillance,%20fighting%20crime%20and%20violence%20report%20(D1.1)%20IRISS%202013.pdf
[55] S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, Ed. Public Affairs, 2019 (704p.).
[56] European Commission, "Final Report: Data and information collection for EU dual-use export control policy review", 6 novembre 2015, p. 146-147; Disponible en ligne : https://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154962.PDF

et impérieuse qui s'impose à tout législateur et l'attention que tout homme se doit d'apporter aux éléments de progrès qui se développent sous ses yeux »[57].

La majorité des activités économiques, juridiques et sociales sollicitent l'identité civile, outil qui a permis aux États d'individualiser les Hommes, rattachée au sujet de droit que représente toute personne, et fondement de tout acte juridique, tel que les contrats de travail ou de service, les actes de propriété, de citoyenneté, de filiation ou encore de libertés publiques. Ces différentes activités sont progressivement élargies au monde numérique, entraînant *de facto* de nombreuses conséquences pour les individus, comme par exemple le non-recours au droit, « […] *phénomène majeur dans notre société,* [qui] *s'explique par un certain retrait du service public et particulièrement une réduction des fonctions d'accueil, d'orientation et d'assistance, au profit de procédures numérisées* »[58]. En outre, la plupart de ces activités, prévoyant à présent un recours systématique aux nouvelles technologies, engendrent conséquemment une multitude d'interrogations et d'enjeux en raison du fait qu'elles produisent, par le biais desdites technologies, une masse de données et de traces numériques, souvent inconnues de leurs propres créateurs. Ces dernières, au sens du nouveau règlement européen aspirant à « bâtir un équilibre dans la régulation, entre protection, utilisation et innovation », doivent faire l'objet d'une protection et de garanties effectives : « *cette mission s'inscrit dans un contexte en constante évolution, de plus en plus globalisé, dans lequel les flux de données personnelles sont devenus un enjeu majeur, que ce soit pour l'économie, le commerce international mais aussi la vie quotidienne des personnes* »[59].

Il est vrai que l'exemple des condamnations pénales pour diffamation ou pour usurpation d'identité transposées dans l'espace numérique atteste de l'existence de la relation, désormais certaine et non-équivoque, entre l'identité numérique et l'identité physique d'une personne, susceptible de déclencher des conséquences bien réelles, puisque, tout compte fait, c'est la personne physique qui est condamnée et non l'avatar ou le représentant numérique, le profil des réseaux sociaux, l'identifiant en ligne ou encore les données et métadonnées générées.

Certes, les avancées en matière technologique présentent une source de richesse pour les êtres humains, les sociétés ainsi que les cultures et les pratiques, mais cette même source de richesse

[57] Rapport n° 72 de M. Jacques THYRAUD, sur le projet de loi, adopté par l'Assemblée Nationale, relatif à l'Informatique et aux libertés, *op. cit.*, p. 4.

[58] Conseil National des politiques de lutte contre la pauvreté et l'exclusion sociale (CNLE), *Contribution au suivi du plan pluriannuel contre la pauvreté et pour l'inclusion sociale*, Les Cahiers du CNLE, mars 2017, p. 49 ; Disponible en ligne : https://www.cnle.gouv.fr/IMG/pdf/Contribution_CNLE_suivi_du_plan_2016.pdf

[59] I. FALQUE-PIERROTIN, « Interview de Madame Isabelle Falque-Pierrotin, Présidente de la CNIL », *Id.*, p. 4.

et d'innovation, prévient la CNCDH, est « susceptible de mettre en péril les droits humains » : « *au nombre de ceux-ci, on compte des atteintes croissantes à la vie privée, la marchandisation générale des données personnelles, le ciblage par des algorithmes, ainsi que la falsification d'informations ou encore la manipulation des faits. De nombreux usagers exposent plus ou moins volontairement et de manière croissante leurs données à caractère personnel, sans nécessairement prendre conscience des risques pour le respect de leur vie privée. Certes, ces pratiques sont souvent la transposition numérique d'atteintes aux droits déjà anciennes, mais le développement de l'Internet leur donne une dimension nouvelle, qui appelle de nouvelles normes et de nouvelles actions* »[60]. Il semble donc nécessaire de se pencher sur l'étendue de ces nouvelles normes et actions légalement mises en œuvre, afin d'éviter les atteintes et les ingérences dans la vie privée des personnes, entendue largement, tout en leur accordant le droit et les moyens juridiques et techniques de connaître l'usage qui est fait de leurs données collectées et traitées, un des objectifs de cette recherche.

Dans ces circonstances, une analyse de l'identité numérique émergente et de sa réalité suggère la manifestation d'un « régime de vérité » numérique, *« une nouvelle manière de rendre le monde signifiant* », déplaçant ainsi la manière dont cette « réalité » sera saisie, « *[…] non plus au niveau de ses représentations et transcriptions ou de ses interprétations individuelles ou collectives, mais au niveau quasiment atomique ou génétique de la donnée, considérée comme un fait ultime, parlant d'elle-même sans médiation […]* »[61]. Cette étude aspire et vise à examiner la réalité sociojuridique de l'identité numérique sous le spectre du « régime de vérité » tel que conçu par Foucault, selon lequel « *chaque société a son régime de vérité, sa « politique générale » de la vérité* »[62] instaurant de nouvelles « *[…] formes de savoir et, par conséquent, des relations entre l'homme et la vérité qui méritent d'être étudiées* »[63]. En effet, les nouvelles

[60] CNCDH, Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, Texte n° 63, JORF n°0126 du 3 juin 2018, p. 2, point 6.
[61] A. ROUVROY, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des *big data* », *In* Conseil d'État, Étude annuelle 2014 – *Le numérique et les droits fondamentaux*, *op. cit.*, p. 413.
[62] M. FOUCAULT, « La fonction politique de l'Intellectuel », *In Dits et Écrits*, t. II (1976-1988), Paris, Ed. Gallimard, Coll. Quarto, 2001, p. 112 : « *Chaque société a son régime de vérité, sa « politique générale » de la vérité : c'est-à-dire les types de discours qu'elle accueille et fait fonctionner comme vrais ; les mécanismes et les instances qui permettent de distinguer les énoncés vrais ou faux, la manière dont on sanctionne les uns et les autres ; les techniques et les procédures qui sont valorisées pour l'obtention de la vérité ; le statut de ceux qui ont la charge de dire ce qui fonctionne comme vrai*. »
[63] M. FOUCAULT, « La vérité et les formes juridiques », Conférence à l'université pontificale catholique de Rio de Janeiro, du 21 au 25 Mai 1973, *In Dits et Écrits t. I* (1954-1975), Paris, Ed. Gallimard, Coll. Quarto, 2001, p. 1408-1409 : « *L'hypothèse que j'aimerais proposer, c'est qu'il y a deux histoires de la vérité. La première est une sorte d'histoire interne de la vérité, l'histoire d'une vérité qui se corrige à partir de ses propres principes de régulation : c'est l'histoire de la vérité telle qu'elle se fait dans ou à partir de l'histoire des sciences. De l'autre*

méthodes et technologies ou les nouveaux procédés, dispositifs et systèmes, mis en place avec la révolution numérique, méritent d'être analysés comme un « régime de vérité » afin de saisir, pragmatiquement, l'étendue et les implications de l'identité numérique, en ce sens que l'intégralité de ces méthodes, procédés, technologies ou systèmes, et tout ce qui peut en découler, caractérise ce qui est tenu pour vrai, « les procédures de manifestation du vrai » à l'ère de la numérisation des sociétés : « *On parle de régime politique […] pour désigner en somme l'ensemble des procédés et des institutions par lesquels les individus se trouvent engagés, d'une manière plus ou moins pressante […]. On peut parler [également] de régime pénal, par exemple, pour désigner l'ensemble, là aussi, des procédés et institutions par lesquels les individus sont engagés, déterminés, contraints à se soumettre à des lois de portée générale. Alors, dans ces conditions, pourquoi en effet ne pas parler de régime de vérité pour désigner l'ensemble des procédés et des institutions par lesquels les individus sont engagés et contraints à poser, dans certaines conditions et avec certains effets, des actes bien définis de vérité ? […] Le problème ce serait d'étudier les régimes de vérité, c'est-à-dire les types de relation qui lient les manifestations de vérité avec leurs procédures et les sujets qui en sont les opérateurs, les témoins ou éventuellement les objets […]* »[64].

De ce fait, à travers les différents développements suivants, les notions de donnée, d'information ou d'identité sont souvent employées de manière synonyme, et ce dans le but de tracer une vision globale de la réalité et de la vérité environnant désormais la question de l'identité numérique, porteuse de nombreux enjeux et ayant la capacité, à terme, d'instaurer une nouvelle conception de l'être humain[65]. Il faut reconnaître que « *nos sociétés sont confrontées à une mise en cause sourde de leurs valeurs : l'homme est moins un citoyen et un sujet de droit, mais de plus en plus une somme de données à exploiter. Ce n'est pas notre conception de la personne humaine, ce n'est pas non plus le modèle de société que nous portons et dans lequel s'incarnent nos valeurs de respect de tous et de chacun* »[66].

---

côté, il me semble qu'il existe dans la société, ou du moins dans nos sociétés, plusieurs autres lieux où la vérité se forme, où un certain nombre de règles de jeu sont définies […] et par conséquent l'on peut, à partir de là, faire une histoire externe, extérieure de la vérité. Les pratiques judiciaires, la manière par laquelle, entre les hommes, on arbitre les torts et les responsabilités […] me semblent l'une des formes par lesquelles notre société a défini des types de subjectivité, des formes de savoir et, par conséquent, des relations entre l'homme et la vérité qui méritent d'être étudiées. »

[64] M. FOUCAULT, *Du gouvernement des vivants*, Cours au Collège de France 1979-1980, Coll. Hautes études, EHESS, Paris, Gallimard – Seuil, 2012, p. 91-92 et 98-99.

[65] *Cf.* p. 556 et s.

[66] Rapport n°7 de M. G. LONGUET, fait au nom de la commission d'enquête du Sénat, sur la souveraineté numérique déposé le 1er octobre 2019, t. I, p. 7 ; disponible en ligne : https://www.senat.fr/rap/r19-007-1/r19-007-10.html#toc0 ; https://www.senat.fr/rap/r19-007-1/r19-007-1.html

§3. Problématique et hypothèses de recherche

La problématique de l'identité numérique s'attache ainsi à la relation hybride et entrecroisée entre une personne, ses perceptions, représentations et interactions, tout ce qui la représente et l'identifie dans l'espace physique et numérique, et, le sujet de droit qui la symbolise dans l'environnement juridique.

À quoi correspond alors l'identité numérique, fait émergent de la numérisation de la société et du développement massif et accéléré des nouvelles technologies ? Formulée autrement, comment se conçoit l'influence qu'opère l'essor de l'environnement numérique sur celui juridique et social faisant, en chœur, émerger la conception de l'identité numérique, objet fondamental de cette étude ?

En outre, ces interrogations en entraînent d'autres au regard des nombreuses implications académiques et juridiques que la manifestation de ce concept suscite, notamment, la question de savoir ce qu'il risque d'advenir de l'identité humaine dont découle l'identité numérique ; les deux s'avérant être entremêlées et interdépendantes, la dernière ne pouvant exister sans la première, pionnière.

Quelles sont, *in fine*, les étendues et les implications des identités numériques ? Plus particulièrement, quels sont *in concreto* les impacts et les résultats de cette révolution numérique et de la conception de l'identité numérique sur l'environnement juridique actuellement en vigueur ?

Ces diverses questions, traitées à travers les développements de cette recherche, deviennent de plus en plus fondamentales à cerner pour tout individu du XXI[e] Siècle, essentiellement compte tenu du fait qu' « *une sorte d'accoutumance aux procédures intrusives s'est créée qui a élargi les seuils de tolérance à leur égard. Car la pénétration croissante des technologies dans tous les interstices de la société a fait reculer les « allergies à la modernité ». La vulgate techno-utopique sur la transparence communicationnelle et l'idéologie de l'individu-consommateur souverain, libre de ses choix et capable de « résister », si besoin est, à partir de son quant à soi ont fait florès dans les mentalités collectives* »[67].

[67] Cultures & Conflits, « Société de la connaissance, société de l'information, société de contrôle. Entretien avec Armand Mattelart », *In* Cultures & Conflits n°64 – *Identifier et surveiller*, hiver 2006, mis en ligne le 21 mars 2007, p. 13, §49 : http://journals.openedition.org/conflits/2051

De plus, « *le cercle grandissant de l'angoisse vécue par certains secteurs de la population face à la pratique réitérée de la violence unie à l'exploitation de l'« émotion populaire » par les autorités pour faire passer en douce des batteries de mesures destinées à assurer « plus de sécurité » ont fait le reste* »[68], soulignant, de façon similaire et égale, diverses interpellations qu'il serait utile de cerner, telles que l'essor d'une culture de la peur ou des réseaux sociaux, ou encore la mise en place d'un droit pénal et d'une politique criminelle gouvernementale centrés, entres autres, sur le risque, la prévention et la surveillance, en particulier, des données personnelles.

À l'heure actuelle, il semble bien que toute personne qui développe un usage régulier et fréquent du web et des nouvelles technologies possède, souvent à son insu, une identité numérique à travers toute donnée ou trace numérique laissée, collectée, enregistrée et traitée, et cela que la personne le sache, le veuille, le souhaite ou non. Cette identité, « aujourd'hui galactique »[69], devient de plus en plus difficile à définir et, *a fortiori*, à gérer, imposant par conséquent la nécessité de changer radicalement de perspective : « *Comme les données elles-mêmes, leur protection traverse l'espace public et l'espace privé. […]. Nous assistons en effet à une dynamisation et à une mise en procédure des notions identitaires : se connecter une fois par jour à Facebook pour consulter son compte est ainsi une procédure composante de l'identité numérique* »[70]. En effet, avec les avancées numériques, le processus de collecte, de stockage et de traitement des données personnelles devient automatique, rapide, bénéfique, bon marché, avantageux et valorisant, attestant ainsi, de manière certaine, que la valeur est dans la donnée ; processus qui invite et qui encourage, *de facto,* une collecte maximale et indifférenciée desdites données qui proviennent, essentiellement, des données générées en naviguant sur Internet ou moyennant des applications, objets connectés, et appareils intelligents utilisés et portés quotidiennement par un individu, voire appelés à être portés méthodiquement. Malgré le fait qu'initialement, dans chaque cas de figure, les données ont été collectées en poursuivant des intérêts précis et légitimes, tels que signifiés par le nouveau cadre juridique en la matière, deux risques majeurs demeurent : « *D'une part, il est tentant, pour chaque entreprise, de*

[68] Cultures & Conflits, « Société de la connaissance, société de l'information, société de contrôle. Entretien avec Armand Mattelart », *Id.*, p. 13, §49
[69] J. PERRIAULT, « Protection des identités numériques personnelles : des futurs incertains », *In* B. Galinon-Mélénec et S. Zlitni (dir.), *Traces numériques : De la production à l'interprétation,* CNRS Éditions, Paris, 2013, p. 27 ; disponible en ligne : https://books.openedition.org/editionscnrs/21699?lang=en
[70] J. PERRIAULT, « Protection des identités numériques personnelles : des futurs incertains », *Id.*, p. 27.

changer l'usage de ces données, car cet usage, et donc la valeur des données, peut ne pas apparaître lors de leur collecte initiale. D'autre part, même si les données que je transmets sont initialement anonymisées, le grand nombre d'applications et d'interfaces collectrices de données permettent à terme la réidentification des utilisateurs – une réidentification qu'ils ne désirent pas, mais rendent possible en confiant à des entreprises distinctes des informations qui, recoupées, dessinent un profil si précis qu'il finit par désigner un seul individu »[71].

Une recherche sur l'identité numérique, à l'époque de la révolution numérique, suggère donc la manifestation de divers enjeux et risques, voire de dérives, qu'ils soient de nature économique, juridique ou sociale, ayant la capacité de provoquer, à terme, des enjeux humains, touchant à la nature humaine et aux libertés auxquelles chaque être humain aspire et se trouve rattaché, et ayant, également, la capacité de s'intégrer à des problématiques plus vastes affectant de plus en plus de secteurs et de disciplines, tels que l'économie, l'assurance, l'administration, la sociologie, la philosophie, les sciences humaines et sociales, ou encore les sciences criminelles.

Comme l'ont si bien noté les législateurs français dès 1977, lors des débats parlementaires sur la loi Informatique et libertés, « *la civilisation de l'informatique ne va-t-elle pas devenir celle de l'indiscrétion et de l'implacabilité, celle qui n'oublie, ni ne pardonne, qui enfonce le mur de l'intimité, enfreint la règle du secret de la vie privée, déshabille les individus ? Traits fâcheux déjà lorsque les données stockées par l'ordinateur sont exactes mais combien plus graves encore quand elles sont erronées ! Or l'ordinateur n'a, dit-on, aucune « faculté d'étonnement » devant les erreurs de droit ou de fait, qui peuvent affecter les données. Il n'en a point davantage devant les déductions fausses imputables au programme* »[72].

Il s'avère, dès lors, que la vraie question n'est plus la seule atteinte à la vie privée ; elle a plutôt changé de paradigme se positionnant, aujourd'hui, autour de l'atteinte à la liberté personnelle de se construire et de se développer, à la liberté de choisir et de déterminer sa propre identité, et ce particulièrement en raison du fait que, avec tous les progrès et les développements technologiques entrepris, la distinction entre données personnelles et données non personnelles devient progressivement chimérique, complexe et énigmatique. À ce propos, précise l'OCDE, « *distinguishing between personal and non-personal data is becoming increasingly difficult.*

[71] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, Avis du Conseil économique, social et environnemental, Les Éditions des JO, janvier 2015, p. 41.
[72] Débats parlementaires – Compte-rendu intégral – 2ème Séance, 1ère Séance du 4 octobre 1977, JO Année 1977-1978 – N° 79 A.N., 5 octobre 1977, p. 5782.

"Once any piece of data has been linked to a person's real identity, any association between this data and a virtual identity breaks the anonymity of the latter.". Today's techniques can often enable data relating to search terms, websites visited, GPS positions, and IP address, to be linked back to an identifiable individual ».[73]

De même, cela évoque les enjeux liés à l'apparition de l'économie numérique en plein essor qui a autant recours aux nouvelles technologies et outils numériques en vue de tracer, profiler, suggérer ou personnaliser pour tenter, attirer, captiver, gérer, améliorer et innover le quotidien des humains, monitorer leurs réputations, leurs activités sportives ou leur santé, et ainsi de suite ; le tout, en employant des systèmes d'identification ou d'authentification – domaine initialement réservé aux autorités étatiques, « un privilège de l'État », qui « *[…] est de plus en plus contesté par des entreprises privées, au premier rang desquelles Facebook et Google. Leurs solutions d'identification, ensuite réutilisables sur d'autres sites internet privés, […], sont devenues le premier moyen de prouver son identité sur internet* »[74]. Et l'intégralité de ces procédures d'identification, générant, de manière égale, une masse de données, font, par la suite, l'objet de traitements, d'analyses, de corrélations et d'interconnexions, remaniant cette multitude d'informations produites et reproduites dans le but de profiler et de déterminer, avec beaucoup de certitude, un individu tel qu'il se perçoit, se représente, se construit, s'identifie, et se développe ; *in fine*, afin de déterminer l'identité et la réalité derrière les données.

Dans ce contexte, il semble ainsi que l'humain se transforme progressivement en un produit, en un être réductible à une masse de données ; ce qui remet, également, en cause le concept juridique et social de l'« irréductible humain » tel que perçu par la Professeure Delmas-Marty qui a pourtant déjà précisé qu' « *[…] il y a urgence à mieux cerner cet irréductible humain qui, au nom des droits indérogeables, protégerait en effet bien plus que la vie ou même la dignité d'un individu, car il s'agit d'une valeur à la fois individuelle (le plus précieux de chaque être) et collective (l'idée même d'humanité)* »[75].

À l'heure du Big data et de la numérisation des sociétés, toute personne devient mêlée et liée aux données qu'elle génère de son esprit et de ses activités ou actions qui, à leur tour, constituent la source fondamentale des outils et technologies de l'information et de la communication

[73] OECD, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, N° 220, OECD Publishing, Paris, 2013, p. 8; Disponible en ligne: http://dx.doi.org/10.1787/5k486qtxldmq-en

[74] Rapport n°7 de M. G. LONGUET, fait au nom de la commission d'enquête du Sénat, sur la souveraineté numérique, *op. cit.*, p. 58-59.

[75] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », RSC, 1994, p. 477.

produisant, conséquemment, lesdites données, métadonnées et traces numériques tout en multipliant, de fait, les enjeux démocratiques, juridiques, économiques, philosophiques, sociaux et humains. En tout état de cause, il semble bien que la totalité de ces enjeux se manifeste de manière simultanée et parallèle parce que, dans le cyberespace, comme il sera vu, les enjeux qui y sont liés sont « inextricables »[76], et « *parce qu'en raison de l'omniprésence des systèmes d'information et de communication dans nos vies quotidiennes, les décisions qui y seront prises affecteront tous les aspects de notre vie* »[77].

Par ailleurs, la révolution numérique et la diversité de ses applications multiples et régulières, impliquant l'émergence de l'identité en question, révèlent l'avènement d'une culture d'asservissement et de dépendance au numérique, attestant de la relation qui se développe et qui, désormais, s'affermit et se fortifie entre l'humain et les technologies. Comme le souligne Alain Supiot, « *les techniques d'inféodation des personnes se présentent aujourd'hui sous le nom de ce qu'on appelle des réseaux. La représentation du monde comme un réseau de particules communicantes a été portée après la Seconde Guerre mondiale par la cybernétique, avant d'inspirer la philosophie postmoderne de la doctrine Law and Economics. Cette représentation se trouve aujourd'hui mise en œuvre par les techniques de management participatif, qui assujettissent l'action des hommes à la réalisation d'objectifs et non plus à l'observation de règles* »[78].

Il y a donc urgence à mieux cerner la problématique assez vaste de l'identité numérique, et d'essayer de la définir et d'envisager ses contours et interprétations sans, toutefois, la réduire ou la délimiter, l'identité étant « *[…] tout sauf une notion « inconsistante » […] : elle est, au contraire, constitutive de l'existence humaine, à condition qu'on la définisse correctement […]* »[79]. En effet, l'identité se définit par ce qu'elle n'est pas, entendue, selon Heinich, comme « *[…] la résultante de l'ensemble des opérations par lesquelles un prédicat est affecté à un sujet* »[80]. L'auteure nous explique ainsi que[81] : de prime abord, l'identité correspond à un « ensemble de représentations, plus ou moins incorporées, objectivées, institutionnalisées – et cela suffit largement à en faire un outil partagé d'orientation dans la réalité » ; c'est donc un « phénomène ouvert, en progrès, processuel », qui requiert une perspective « constructiviste et

[76] F. DOUZET, « La géopolitique pour comprendre le cyberespace », *op. cit.*, p. 4.
[77] F. DOUZET, « La géopolitique pour comprendre le cyberespace », *Id.*, p. 14.
[78] A. SUPIOT, *La gouvernance par les nombres*, Cours au Collège de France (2012-2014), en partenariat avec l'Institut d'études avancées de Nantes, Ed. Fayard, Coll. Poids et mesures du monde, 2015, p. 310.
[79] N. HEINICH, *Ce que n'est pas l'identité*, Ed. Gallimard, Coll. Le débat, Paris, 2018, p. 110.
[80] N. HEINICH, *Ce que n'est pas l'identité*, *Id.*, p. 105.
[81] N. HEINICH, *Ce que n'est pas l'identité*, *Ibid.*, p. 105-109.

non pas essentialiste » pour en rendre compte. En outre, l'identité « n'est pas unidimensionnelle mais multidimensionnelle, car ses points d'appui sont nombreux », évoquant la réalité « complexe, plurielle, articulée » qui l'entoure continuellement, nécessitant ainsi une approche « pluraliste, et non réductionniste ».

L'identité n'est pas « donnée, mais produite, « fabriquée » : elle est, avant tout, parlée, comme l'est toute représentation mentale partagée ; elle est actée, par le traitement qu'on fait d'une personne ou d'une entité abstraite ; elle est symbolisée par des objets, des outils ou des données ; elle est instituée par des décisions administratives et juridiques ; elle est, de même, plus ou moins investie dès lors que les opérations qui « font » l'identité passent par des manifestations émotionnelles, témoignant de l'attachement que lui vouent les sujets », l'exemple des réseaux sociaux et de la e-réputation en sont une bonne représentation. De ce fait, son étude réclame « l'observation d'actions concrètes, en situation », et rejetant le postulat d'un état abstrait, en adoptant une méthodologie « pragmatique, axée sur les actions en situation réelle ». Par ailleurs, les « paramètres qui construisent l'identité peuvent s'exprimer sous la forme de différents qualificatifs », de telle façon qu'étudier l'identité, c'est « mettre en évidence les fondements d'une sorte de grammaire de l'identité », au sens de l'adage bien connu selon lequel « l'identité est structurée comme un langage » et, de nos jours, de plus en plus comme un langage informatique.

D'autre part, « *loin d'être une expérience solipsiste, mettant un sujet face à lui-même, l'identité n'a de sens – y compris à son stade le plus intériorisé qu'est l'autoperception – qu'à travers des mots et des liens avec autrui, avec l'image de soi envoyée à d'autres et renvoyée par d'autres. Affecter un prédicat, c'est communiquer une représentation qu'on a du monde, afin de la partager. Ainsi, même lorsqu'elle est celle d'un individu, l'identité n'est jamais un phénomène purement individuel […]* »[82] ; exigeant ainsi l'adoption d'une perspective « interactionniste » afin de pouvoir l'analyser de manière appropriée et réelle. Enfin, un sujet, objet de l'opération identitaire, a « la particularité d'être doté d'une capacité de réflexivité, lui permettant de s'auto-prédiquer[83] et d'avoir des avis et des opinions », nécessitant, dès lors, non seulement de déterminer un statut objectif mais aussi, et surtout, de « comprendre la façon dont le sujet se vit » : « *c'est bien le sentiment d'identité qui est en jeu. Il devient possible d'analyser le rapport qu'il entretient avec sa propre identité, de mettre en évidence ses conditions de*

[82] N. HEINICH, *Ce que n'est pas l'identité*, *Ibid.*, p. 108-109.

[83] N. HEINICH, *Ce que n'est pas l'identité*, *Ibidem*, p. 109 : selon l'auteur, « *[…] c'est-à-dire de s'auto-percevoir autant que de se présenter – et d'avoir un avis sur les désignations qui lui sont renvoyées de lui-même*. »

félicité ou, au contraire, ses facteurs de crise […] »[84], de plus en plus possible à l'ère du numérique, réclamant, de ce fait, une perspective « compréhensive » pour l'appréhender adéquatement.

§4. Méthodologie et présentation de la recherche

La méthodologie privilégiée pour aborder la problématique principale de l'identité numérique, dans ses multiples perspectives et dimensions, est relativement similaire aux perspectives susmentionnées pour analyser l'identité[85] selon les développements de cette étude dont l'orientation juridique est principalement centrée sur le droit européen, le droit comparé, le droit pénal et la politique criminelle, ainsi que le droit et les libertés fondamentales ; l'ambition de cette recherche étant d'apporter une contribution à la réflexion sur le droit des nouvelles technologies et du numérique, mais aussi sur l'évolution du droit à la protection des données et des droits de l'homme.

Ceci permet d'examiner méthodologiquement ladite question – autant que possible de façon complète et compréhensive, à l'image d'une toile ou d'un casse-tête – suivant une logique constructiviste, analytique, pragmatique, historique, sociologique et de sciences juridiques et comparées, et ce, parce que « *dans la culture contemporaine du présentisme et du subjectivisme exacerbés, l'écoute active de la mémoire collective sera l'ultime rempart contre l'action frénétique qui échoue le double test de la réalité et de la sérénité…* »[86], mais surtout, parce que « *face à ces grands systèmes techniques qui capturent nos habiletés, il est de plus en plus nécessaire d'apprendre à ne pas désapprendre* »[87] ; le tout en poursuivant la vision du doyen Carbonnier qui a affirmé : « *juriste ou sociologue, il faut savoir se taire pour écouter l'Autre du Droit et de la société* »[88].

---

[84] N. HEINICH, *Ce que n'est pas l'identité*, *Ibidem*, p. 109.
[85] *Cf.* p. 31 à 33 ; N. HEINICH, *Ce que n'est pas l'identité*, *Ibidem.*
[86] J.-G. BELLEY, « Le rayonnement intellectuel de Jean Carbonnier au Québec : le succès d'estime d'un honnête homme », *In* Les colloques du Sénat, « Jean Carbonnier (1908-2003). Art et Science de la législation », du 5 et 6 novembre 2008, Palais du Luxembourg, Colloque international organisé par la Bibliothèque Cujas en coopération avec le Sénat et l'Association Française Droit et Cultures, avec le soutien de la Mission de recherche Droit et Justice, sous la responsabilité de R. Verdier et J.-E. Tosello-Bancal, p. 111 ; Disponible en ligne : https://www.senat.fr/fileadmin/Fichiers/Images/evenement/colloque/ActesColloque-Jean-Carbonnier-Novembre2008.pdf
[87] D. CARDON, *À quoi rêvent les algorithmes – Nos vies à l'heure des big data*, Ed. Seuil et La République des Idées, France, octobre 2015, p. 102-103.
[88] Les colloques du Sénat, « Jean Carbonnier (1908-2003). Art et Science de la législation », du 5 et 6 novembre 2008, *Id.*, p. 111 : « *Dans l'œuvre législative également, ne croyez pas que je restais enfermé. Je consultais, je consultais beaucoup les praticiens, pour les questions de droit de la famille. Je cite les notaires au hasard parce qu'ils étaient particulièrement concernés. Non, je ne me plains pas de l'absence d'interlocuteurs. Je les écoutais, j'écoute plus facilement que je ne parle, je le reconnais. J'aime bien que les gens s'expriment d'abord.*

Au regard de ce contexte, il semble dès lors utile de rechercher, dans un premier temps, la réalité de l'existence de l'identité numérique, afin de révéler sa manifestation sociale et juridique et l'étendue de ses implications, caractérisant ainsi le rôle et l'influence certaine et polymorphe portée par la révolution numérique ayant engendré l'identité numérique en question (Partie I).

Ces premiers développements, présentant une perspective assez théorique (théorico-juridique), permettent, dans un second temps, de s'attarder sur la vérité et la réalité des enjeux et des défis qui accompagnent le concept analysé, au moment où il est observé et étudié, soulignant, *in concreto*, l'influence pragmatique et équivoque que suscite finalement la révolution numérique sur l'identité humaine via, *in fine*, l'identité numérique (Partie II).

Peut-être ai-je surtout écouté, mais, pour les faire parler, il fallait bien que je m'exprime moi-même. Donc, je pense que le dialogue s'est noué » (note de bas de p. n°186)

PARTIE I – LA RÉALITÉ DE L'EXISTENCE DE L'IDENTITÉ NUMÉRIQUE : UNE INFLUENCE CERTAINE ET POLYMORPHE

« *La corporéité implique que l'entité cognitive a – par définition – une perspective. Cela signifie que ses liens avec l'environnement ne sont pas « objectifs », indépendants de la situation, des attitudes et de l'historique du système. Bien au contraire, ces liens dépendent étroitement de la perspective établie par les propriétés sans cesse émergentes de l'agent lui-même, et du rôle joué par ces redéfinitions dans la cohérence du système entier.* »[89]

Le dessein de cette première partie est d'explorer la perspective de l'existence de l'identité numérique, et de constater la réalité de ses implications et de ses caractéristiques, face à l'influence provoquée par l'ère numérique et les avancées technologiques édifiant un nouvel environnement ; d'autant que la nature de la réalité et des choix effectués durant cette époque commande que l'on s'interroge sur « *la nature du possible non actualisé et de la réalité de son existence* »[90].

Synonyme d'existence ou de vérité, la réalité suppose le « *caractère établi ou fondé de ce qui constitue une accusation, une hypothèse*, *[…] ce qui existe indépendamment du sujet, ce qui n'est pas le produit de la pensée* », impliquant alors l'« *environnement concret et matériel de l'homme*, […] la] *somme des événements sociaux qui constitue la situation dans laquelle se trouve une personne* »[91]. La notion d'existence qui s'entend, de manière générale, comme une « *manière de vivre*, [un] *mode de vie* », et qui désigne, dans un sens plus littéraire, « *l'être vivant* »[92], se réfère, dans le cadre de cette recherche, à la « présence », à la « nature »[93], de l'identité au sein des environnements sociaux et juridiques actuels et passés, faisant un constat de la vérité, de la réalité, sociale, légale, virtuelle et technologique que représente dorénavant l'identité numérique. Celle-ci suppose un « *spectre de l'identité* » varié prenant différentes formes, pouvant aller « *[…] de l'anonymat à l'identité vérifiée en passant par le pseudonyme ou un profil sur un réseau social* »[94]. Elle paraît ainsi comprendre toute trace ou donnée à

[89] F. J. VARELA, *Invitation aux sciences cognitives*, *op. cit.,* p. III.
[90] H. ATLAN, *Les étincelles du hasard, t. 2. Athéisme de l'écriture*, Ed. Seuil, Coll. La librairie du XXIe Siècle, 2003, p. 77.
[91] CNRTL, « Réalité » : https://www.cnrtl.fr/definition/réalité//0
[92] Dictionnaire Larousse, « Existence » : https://www.larousse.fr/dictionnaires/francais/existence/32144
[93] CNRTL, « Existence » : https://www.cnrtl.fr/definition/existence
[94] D. FOREST, « Identité(s) Numérique(s) : Tous authentifiés ? », *In* CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », 2012, p. 38.

caractère personnel, et, uniformément, toute variante et variation des notions d'identité, d'identification, d'identifiable, d'individualisation ou d'authentification ; le tout composant les multiples facettes et représentations de l'identité d'un individu, telle qu'il la perçoit. Ce contexte peut, *de facto*, engendrer des confusions pour les personnes et plusieurs conséquences pouvant affecter leur existence, voire la construction et le développement de leurs identités, de leurs personnalités, que ce soit sur un plan social ou légal ; l'objectif de cette partie étant d'explorer ce contexte éclectique et hétérogène avec comme point focal le cadre juridique environnant, depuis la révolution numérique, la notion en question : « *We know. We are lost in technology and our personal information is out of control. We are not any longer a few idealists voicing this and the choir is now composed of many authoritative singers* »[95].

Cette manifestation de l'identité numérique, telle qu'elle apparaît à l'heure actuelle, résulte principalement des nombreux impacts suscités par la révolution numérique et les avancées technologiques qui se présentent, à travers l'analyse suivante, comme étant de nature certaine et polymorphe. En effet, cette influence s'avère être certaine, puisque « *sans abolir l'indétermination de l'identité,* [elle] *individualise, souligne la spécificité (connue ou censée être connue)* », et semble être *« […] équivalent de donné, fixé, défini avec en outre l'idée que la précision pourrait être donnée si on l'exigeait* »[96], soulignant dès lors la nature « déterminée », « qui ne fait pas de doute, conforme aux critères de la vérité »[97], de l'impact occasionné. Parallèlement, l'influence en cause se caractérise, de manière égale, par son aspect polymorphe, influence « *qui offre des apparences, des formes diverses* »[98], tout en étant sujette « *[…] à changer de forme* »[99], une des spécificités de la révolution numérique de par sa propre nature. C'est donc une influence d'origine numérique ayant la capacité de déclencher une multitude d'incidences se présentant sous différentes formes : sociale, culturelle, économique, philosophique, sociologique, juridique, et évoquant, simultanément, les notions de réalité sociale et de réalité juridique. Ces deux notions sont initialement distinctes mais semblent devenir, avec la numérisation progressive des sociétés, interdépendantes, faisant toutes deux

[95] G. BUTTARELLI, Speech on "Privacy by design - Privacy engineering" given at the 11th International Computers, Privacy and Data Protection Conference (CPDP), EDPS side event, 25 January 2018, p. 1; disponible en ligne: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/privacy-design-privacy-engineering_en

[96] CNRTL, « Certain[1] » : https://www.cnrtl.fr/definition/certaine

[97] CNRTL, « Certain[2] » : *Id.*

[98] CNRTL, « Polymorphe » : https://www.cnrtl.fr/definition/polymorphe

[99] Dictionnaire de l'Académie Française, 9ème Ed., « Polymorphe » : « *Emprunté du grec polumorphos, « qui a plusieurs formes », lui-même composé à l'aide de polus, « abondant, nombreux », et morphê, « forme »* » : https://www.dictionnaire-academie.fr/article/A9P3257

appels à celle de réalité informatique, numérique, qui accompagne désormais cette réalité sociojuridique.

L'étude de cet environnement, et des nombreux effets qu'il génère, permet de constater l'existence de l'identité numérique et la réalité qu'elle suggère et constitue depuis lors, allant bien au-delà de la seule dimension technologique et comprenant, à la fois, des concepts sociojuridiques tels que, principalement, ceux d'identité et de données à caractère personnel.

Or, ces derniers suscitent, avec les avancées et les innovations technologiques, de nombreuses interrogations et angoisses, explorées dans les développements de cette partie, notamment au niveau européen à l'aune de la mise en œuvre du RGPD. En effet, « *being European means the right to have your personal data protected by strong, European laws. Because Europeans do not like drones overhead recording their every move, or companies stockpiling their every mouse click. This is why Parliament, Council and Commission agreed in May this year a common European Data Protection Regulation. This is a strong European law that applies to companies wherever they are based and whenever they are processing your data. Because in Europe, privacy matters. This is a question of human dignity* »[100].

Comment se manifeste et se conçoit alors l'existence de l'identité numérique ? Et, comment cette existence, constatant sa réalité, sa vérité, se traduit-elle légalement, en particulier, depuis la mise en place du RGPD, un des éléments constitutifs du paquet européen susmentionné ?

L'environnement actuel imbibé de nouvelles technologies et d'innovations numériques et juridiques requiert, dans ce cadre, l'étude de la réalité sociale entourant les notions d'identité et d'identité numérique en vue de tracer leur existence sociojuridique, révélant ainsi la réalité sociale que constitue dorénavant l'identité numérique (Titre I). En outre, cet environnement nécessite, d'autre part, l'analyse de la réalité légale consacrant le concept d'identité numérique et sa portée juridique (Titre II), permettant alors de démontrer sa vérité légale ; ces approfondissements attestant, *in fine*, de l'existence certaine et polymorphe de l'identité numérique à l'époque de la révolution numérique.

[100] J.-C. JUNCKER, European Commission (2016), 'State of the Union address 2016', Speech/16/3043, 14 September 2016, *In* FRA European Union Agency For Fundamental Rights, Fundamental Rights Report 2017, Chap. 6 – Information society, Privacy and Data protection, p. 160 : https://fra.europa.eu/en/publication/2017/fundamental-rights-report-2017

TITRE I – UNE RÉALITÉ SOCIALE

« *Si le sujet se constitue, ce n'est pas sur le fond d'une identité psychologique mais à travers des pratiques qui peuvent être de pouvoir ou de connaissance, ou bien par des techniques de soi*. »[101]

Afin d'envisager le concept d'identité numérique en particulier, il est nécessaire de s'attarder sur les questions entourant la notion d'identité et tout ce qu'elle représente à l'heure actuelle, époque du XXI[e] Siècle. L'individu vit et évolue davantage avec différentes identités et représentations, y compris l'identité et les représentations numériques, or, *« nous vivons dans l'illusion que l'identité est une et indivisible, alors que c'est toujours un unitas multiplex. Nous sommes tous des êtres poly-identitaires […]* » dans le sens où nous unissons en nous plusieurs facettes identitaires[102]. Ces dernières se construisent et se développent dans le cadre de sociétés, de communautés, de groupes sociaux, asseyant la dimension sociale de la réalité complexe entourant et affectant la notion d'identité. Précisément, « *nous avons besoin d'une méthode de connaissance qui traduise la complexité du réel, reconnaisse l'existence des êtres, approche le mystère des choses* »[103], afin d'appréhender efficacement et objectivement la portée de l'identité numérique.

Une réalité qui suppose, dans un sens large, la « manifestation concrète », le « contenu », d'un processus ou d'un événement, *« ce à quoi se réfère une désignation, une représentation* », désigne, plus concrètement, « *ce qui constitue le monde de l'homme* »[104]. Suivant cette approche, cela évoque le concept de réalité sociale, l'étude « *désignant un champ de connaissance, l'objet d'une science ou d'une discipline* »[105] relatif au social, à « *la société* », à « *la vie des hommes en société* »[106], et qui invoque les concepts de « sciences sociales, de corps social, de psychologie sociale, de pacte social, de climat social, d'intérêt social ou encore

---

[101] J. REVEL, *Le vocabulaire de Foucault*, Ed. Ellipses Marketing, Coll. Le vocabulaire de…, 2009, p. 63.
[102] E. MORIN, *Penser l'Europe*, Ed. Gallimard, Paris, 1987, revue et complétée en 1990, p. 199, où l'auteur affirme ainsi : *« Nous sommes tous des êtres poly-identitaires dans le sens où nous unissons en nous une identité familiale, une identité locale, une identité régionale, une identité nationale, une identité transnationale (slave, germanique, latine) et, éventuellement, une identité confessionnelle ou doctrinale. Il y eut souvent tragédie quand il y eut conflit d'identité, comme chez l'enfant de père allemand et de mère française dans la première moitié de ce siècle. Mais il peut aussi y avoir bonheur à concilier en soi les richesses de deux identités en conflit, comme je le fis moi-même de mes multiples "matries" et comme le feront les jeunes "beurs" de France quand ils transformeront en complexité ce qui est pour eux contradiction*. »
[103] E. MORIN, *La Méthode 1. La Nature de la nature*, Ed. Points, Coll. Points Essais (n°123), 2014 (416p.), 4ème de couverture.
[104] CNRTL, « Réalité » : *loc. cit.*
[105] CNRTL, « Réalité » : *Id.*
[106] CNRTL, « Social » : https://www.cnrtl.fr/definition/social

d'acquis social »[107]. Autant de concepts, donc, qui touchent et qui interpellent, à la fois, celui d'environnement juridique, le droit se consacrant fondamentalement à la gestion des individus et de la société. Une représentation sociale suggère plusieurs éléments et concepts sociaux, tels que la classe sociale, le groupe social, la catégorie sociale, l'appartenance sociale, traduisant une sorte de "vision" du monde, de « *modalités de pensée pratique orientées vers la communication, la compréhension et la maîtrise de l'environnement social, matériel et idéal* »[108].

C'est donc le monde dans lequel les hommes vivent et évoluent qui est particulièrement visé dans ce cadre, et qui témoigne, à l'ère du numérique, de la complexité de la société, mais surtout, de la complexité des individus, et de leur identité, composant ladite société. Une réalité sociale complexe semble ainsi se concrétiser, ou un « fait social » suivant la vision de Durkheim qui le conçoit comme « *[…] toute manière de faire, fixée ou non, susceptible d'exercer sur l'individu une contrainte extérieure ; ou bien encore, qui est générale dans l'étendue d'une société donnée tout en ayant une existence propre, indépendante de ses manifestations individuelles* »[109]. Les faits sociaux tirent leur réalité des hommes, or, comment rendre compte de cette réalité si ce n'est en observant la mémoire, la pensée et les perspectives collectives : « *Tous les éléments de la réalité sociale (aussi divers que l'argent, la délégation politique, les convictions et les programmes, les groupes d'appartenance ou les archives) n'ont d'existence objective que parce que collectivement nous y croyons, nous leur assignons une fonction (de symbolisation, de représentation, de signification), nous élaborons à côté des faits bruts, objets des sciences, des faits institutionnels, objets des sciences humaines* »[110].

Dans cette perspective, une étude sur l'identité numérique suppose alors une étude de la réalité sociale qu'elle semble représenter dorénavant. Le numérique, et la révolution qu'il induit, devient-il un fait social suscitant la réalité sociale que forge depuis lors l'identité numérique ?

Quelles sont les étendues et les caractéristiques du concept d'identité numérique ?

L'étude, en premier lieu, de l'environnement social et du monde des hommes permet alors d'apporter des clarifications, puisque l'observation de la réalité sociale et des faits sociaux souligne les diverses influences conceptuelles et interactives ayant impacté le concept d'identité

---

[107] CNRTL, « Social » : *Id.*

[108] D. JODELET, « Représentation sociale : phénomènes, concept et théorie », *In* S. Moscovici (dir.), *Psychologie sociale,* PUF, Coll. Quadriges, Paris, 10 octobre 2003 [1984] (p. 357-378), p. 371 ; Voir également, D. JODELET (dir.), *Les représentations sociales*, PUF, Coll. Sociologie d'aujourd'hui, Paris, 26 mai 2003 (454 p.)

[109] E. DURKHEIM, *Les Règles de la méthode sociologique*, Flammarion, Coll. Champs, Paris, 1988 [1894], p. 107.

[110] J. R. SEARLE, *La construction de la réalité sociale [The Construction of Social Reality],* Trad. de l'anglais par C. Tiercelin, Gallimard, Coll. NRF Essais, Paris, 1998 (320 p.) 4ème de couverture.

numérique, et ayant entraîné son émergence et ses multiples interprétations technologique, sociale ou légale. Précisément, il s'avère que ce concept, tel qu'il se présente au XXI^{e} Siècle, découle principalement de l'influence conceptuelle vécue, au fil des époques et des courants, par la notion d'identité (Chap. I). Ce qui dénote, en outre, la valorisation rattachée à l'identité numérique, ainsi que tout ce qu'elle caractérise et englobe, due à l'influence interactive portée par l'ère du numérique et les développements informatiques (Chap. II) ; l'ensemble cristallisant la réalité sociale complexe que constitue, désormais, l'identité numérique.

Chapitre I. L'identité au XXIe Siècle : Une influence conceptuelle

« *But let there be no scales to weigh your unknown treasure;*
And seek not the depths of your knowledge with staff or sounding line.
For self is a sea boundless and measureless. »[111]

Comprendre l'étendue de ce qui caractérise et conceptualise l'identité au XXIe Siècle nécessite une analyse de la notion en particulier, en vue d'examiner sa portée et ses interprétations sous le spectre et l'influence des sciences sociales et juridiques, également impactées par les époques et les courants de pensées menant vers la révolution numérique et l'émergence de l'identité numérique, attribut de l'identité humaine.

En parlant de l'influence 'conceptuelle', observée dans le cadre de l'étude sur l'identité, cela évoque ce « *qui est de l'ordre du concept* », ce « *qui constitue un concept, une idée générale* »[112]. Du latin « *conceptus* », un concept s'entend comme une « *idée générale et abstraite que se fait l'esprit humain d'un objet de pensée concret ou abstrait, et qui lui permet de rattacher à ce même objet les diverses perceptions qu'il en a, et d'en organiser les connaissances* » ou comme la « *manière dont une entreprise est conçue ;* [un] *projet* »[113]. Cette notion suppose alors une « faculté de se représenter une chose concrète ou abstraite », une « représentation » ; et philosophiquement, elle correspond notamment à une « *représentation mentale abstraite et générale, objective, stable, munie d'un support verbal* »[114]. En outre, le concept de représentation, afférent à celui de conceptuel, est, tel qu'il se présente dans les développements suivants, fortement rattaché à celui d'identité s'avérant être aussi « nomade » que celui de représentation sociale : « *Il est considéré comme hétérogène et polysémique et est un très bon exemple de concept dit « nomade » passant d'une science à l'autre* »[115].

Comment se conçoit alors l'identité d'un individu au XXIe Siècle ? est-il possible de la définir et d'en délimiter les contours ? De façon générale, la conceptualisation de l'identité humaine a-t-elle été affectée par les courants, les pensées, les lois et les technologies des dernières époques de l'histoire de l'homme ?

---

[111] G. KHALIL GIBRAN, *The Prophet*, Vintage Books New-York (1923), 2015, Chap. XVII – On Self-Knowledge, p. 58.
[112] CNRTL, « Conceptuel » : https://www.cnrtl.fr/definition/conceptuel
[113] Dictionnaire Larousse, « Concept » : https://www.larousse.fr/dictionnaires/francais/concept/17875
[114] CNRTL, « Concept » : https://www.cnrtl.fr/definition/concept/substantif
[115] L. JOVIC, « Représentations (sociales) », *In* Monique Formarier (éd.), *Les concepts en sciences infirmières*, 2ème éd., Toulouse, Association de Recherche en Soins Infirmiers, « Hors collection », 2012 (p. 265-267), p. 265.

Il semble que l'influence conceptuelle constatée relève de ou se rapporte à des idées, pensées, époques, disciplines, courants, voire des mouvements, aussi divers que variés impliquant, à la fois, le monde social et le monde juridique ; une étude de ce contexte permettant de ce fait d'apporter des éclaircissements relatifs à la représentation et à l'étendue sociojuridiques du concept d'identité. Dans ce cadre, l'analyse de ce concept exige alors une étude transversale de la notion d'identité et de ses multiples implications, permettant d'obtenir une idée générale de ce que ce concept d'identité représente (Section 1), mais aussi, d'avoir une vue globale de ce qu'évoque le concept d'identité numérique en particulier qui, pour sa part, nécessite une approche dynamique (Section 2) ; le tout soulignant conséquemment, et par là même, l'aspect actif et évolutif, dynamique, du concept d'identité numérique, ainsi que l'aspect transversal de celui, plus global, d'identité.

Section 1 – Le concept d'identité : une notion transversale

Le concept d'identité semble ainsi incarner une dimension transversale et interdisciplinaire dont la construction et la mise en œuvre ont été, fondamentalement et simultanément, marquées par le monde social (§1) ainsi que le monde légal (§2), manifestant alors la nature transversale rattachée à ce concept.

§1. Le rôle du monde social

Le monde social joue un rôle majeur dans la perception, la construction et l'élaboration de l'identité qui s'avère être, d'une part, le fruit d'un processus d'interaction et d'appartenance (A), et, d'autre part, le fruit d'un processus de représentation et d'évaluation (B).

A. L'identité, fruit d'un processus d'interaction et d'appartenance

La notion d'identité n'a pas de définition unique, sa définition faisant l'objet de débats au sein des sciences humaines et sociales. Néanmoins, un certain consensus se retrouve sur l'essence de ce concept.

Étymologiquement, le terme « identité » trouve son origine du latin *identitas*, « *caractère de ce qui est identique* »[116], dérivé du latin classique *idem*, qui signifie le même. De façon générale et grossière, l'identité est définie comme « *le caractère permanent et fondamental de quelqu'un, d'un groupe, qui fait son individualité, sa singularité* »[117], ou encore comme

[116] Dicolatin : « Identitas » : http://www.dicolatin.com/FR/LAK/0/IDENTITAS/index.htm
[117] Dictionnaire Larousse : « Identité » : https://www.larousse.fr/dictionnaires/francais/identité/41420

l'ensemble « *des données de fait et de droit qui permettent d'individualiser quelqu'un (date et lieu de naissance, nom, prénom, filiation, etc.*) »[118]. Elle désigne également le « *caractère de deux ou plusieurs êtres identiques (identité qualitative, spécifique ou abstraite)* »[119] ainsi que le « *caractère de ce qui demeure identique ou égal à soi-même dans le temps (identité personnelle)* »[120]. Dès lors, cette notion semble couvrir différentes variations de sens, telle que la similitude, l'unité, l'identité personnelle, l'identité culturelle et la propension à l'identification[121].

Dans un premier temps, la philosophie s'est emparée de cette notion et des interrogations qu'elle suscite, les philosophes présocratiques recourant déjà à l'identité et l'employant comme concept central de leurs réflexions[122]. Au Moyen-Âge, cette notion traduisait la conformité au groupe[123]. Aux XVII^{e} et XVIII^{e} Siècles, les empiristes l'ont employé pour soulever le problème de l'identité personnelle[124]. Locke s'est ensuite penché sur la question de l'unité de l'identité personnelle dans le temps, qu'il résout en postulant qu'une personne est une conscience de soi incarnée capable de garder à l'esprit les phases successives de son existence[125]. Au XIX^{e} siècle toutefois, particulièrement sous l'influence de Hegel, les questions entourant l'identité se sont déplacées dans le champ vaste des rapports sociaux. L'identité, concept influencé par différents courants de recherche, semble donc, dans cette période, résulter de la reconnaissance réciproque du moi et de l'autre, elle se met en place par le biais d'un processus conflictuel où se construisent des interactions individuelles et des pratiques sociales objectives et subjectives[126]. En 1902, les travaux de C. Cooley définissaient le Soi comme se construisant et se développant à partir des interactions sociales[127]. Dans les années 30, les travaux de G. Mead montraient le « Soi » comme un dialogue continu entre un « Je » réagissant aux attitudes des autres et un

[118] Dictionnaire Larousse : « Identité », *Id.*
[119] CNRTL, « Identité » : http://www.cnrtl.fr/definition/identité
[120] CNRTL, « Identité », *Id.*
[121] J. REY-DEBOVE et A. REY (dir.), *Le nouveau Petit Robert. Dictionnaire alphabétique et analogique de la langue française*, Paris, 1993, « Identité ».
[122] Y. BATTISTINI, *Trois présocratiques. Héraclite, Parménide, Empédocle*, Paris, 1955.
[123] D. IOGNA-PRAT, « Introduction générale : la question de l'individu à l'épreuve du Moyen Âge », *In* B.M. BEDOS-REZAK et D. IOGNA-PRAT (dir.), *L'Individu au Moyen Âge, individuation et individualisation avant la modernité*, Paris, 2005, p. 7-29.
[124] R. LANGBAUM, *The Mysteries of Identity. A Theme in Modern Literature*, Oxford University Press, 1977, p. 25.
[125] S. CHAUVIER, « La question philosophique de l'identité personnelle », *In* C. Halpern et J.-C. Ruano-Borbalan (dir.), *Identité(s) : L'individu, le groupe, la société*, Ed. Auxerre, Coll. Sciences Humaines, 2004, p. 25-32.
[126] C. TAYLOR, *Hegel et la société moderne*, Presses de l'Université Laval, Paris, Ed. du Cerf, 1998 [1979], p. 14-23.
[127] C. H. COOLEY, *Human Nature and the Social Order,* New York, Charles Scribner's sons, 1902.

« Moi » qui consiste en l'internalisation des attitudes d'autrui[128]. Dans les années 50, cette notion a été associée aux domaines de la psychologie et de la sociologie, disciplines ayant pour aspiration l'explication de la condition humaine. Les perturbations sociales et politiques survenues au sein de la société américaine ont également contribué au succès de cette notion. Ainsi, dans le courant des années 70, le concept d'identité prit un essor considérable aux États-Unis premièrement, puis dans le monde, à travers la création de départements minoritaires au sein des universités américaines ainsi qu'une utilisation croissante de ce concept dans d'autres domaines de la recherche[129].

Il semble donc que les réflexions philosophiques et psychosociales sur l'identité se sont articulées, dès l'origine, autour d'une question centrale : celle de décrire et d'expliquer la dichotomie et la dialectique qui existent entre identité sociale et identité personnelle. Les principales théories développées et les nombreux travaux entourant la notion d'identité effectuées confèrent tous une place centrale à autrui et au monde social dans la construction identitaire.

Le terme « identité » est concrètement, en tant que tel, employé pour la première fois par Erikson, psychanalyste de formation, dans son ouvrage Enfance et Société paru au XX^{e} Siècle[130]. Durant cette période, le concept d'identité s'enrichit grâce à son étude et à ses développements dans divers domaines de la recherche. La psychologie, en particulier, se l'approprie en mettant avant tout l'accent sur l'individu. Ainsi, dans la tradition freudienne, l'identité se construit dans le conflit : d'une part, entre l'identité pour soi et l'identité pour autrui, et d'autre part, entre les différentes instances de l'individu que sont le Ça, le Moi et le Surmoi[131]. Erikson prend contact avec les écrits d'anthropologues américains qui tendent à relier les caractéristiques psychologiques d'un individu avec les expressions particulières des cultures dans lesquelles il évolue[132]. Il entreprend alors, dans son ouvrage précité, d'aller plus loin que la théorie freudienne en soulignant le rôle des interactions sociales sur la construction de la personnalité d'un individu.

Il est vrai que ce terme, avec toutes les problématiques l'entourant, s'est invité à se développer au sein de divers domaines et selon différentes perspectives. Toutes les questions entourant la

---

[128] G.H. MEAD, *L'Esprit, le Soi et la Société*, Paris, PUF, 1963 & Coll. le Lien Social, 2006.
[129] C. HALPERN, « Faut-il en finir avec l'identité ? », *In* C. Halpern et J.-C. Ruano-Borbalan (dir.), *Identité(s) : L'individu, le groupe, la société*, *Id.*, p. 11-20.
[130] E. ERIKSON, *Enfance et société*, Ed. Delachaux et Niestlé, 1982 (1950).
[131] A. OPPENHEIMER, « Identité », *In* A. De Mijolla (dir.), *Dictionnaire international de la psychanalyse*, 1, Ed. Calmann-Levy, Coll. Psychologie, Psychanalyse, Pédagogie, 2002, p. 783-784.
[132] A. KARDINER et M. MEAD, *Dictionnaire de l'ethnologie et de l'anthropologie*, P. BONTE et M. IZARD dir., Paris 2002 (1991), p. 403-404 et 458-459.

notion d'identité entraînent une interrogation sur le statut de l'être humain à qui est conféré cette « identité ». À ce titre, M. Mauss affirme, entre autres, que la reconnaissance et l'identité d'une « personne humaine » peuvent varier selon les situations ou les moments sociaux traversés par l'individu et indique que la « personne humaine » se constitue dans la société[133] ; or, ce point de vue ne faisait pas l'unanimité. En effet, un autre courant associe fortement ce concept avec la notion d'ethnicité. Dans ce contexte, l'identité ethnique semble être une réalité universelle et fondamentale de la vie sociale, ce qui implique, *de facto* quoiqu'implicitement, que l'identité est une donnée naturelle et immuable. Toutefois, ce postulat est remis en question dans les années 50 et, en particulier, lorsque F. Barth annonce dans son ouvrage que les identités sont créées et maintenues par le jeu des interactions entre différents groupes[134] ; celui-ci s'inspirant de la théorie de l'interactionnisme symbolique développée en sociologie. L'attention portée à l'interaction dans la constitution de l'identité a surtout été soulevée par Mead qui considère que le comportement d'un individu tient du « soi », lui-même opposé à « l'esprit »[135]. Cet « esprit » se constitue par le jeu des interactions sociales, et la conscience de soi se manifeste par un acte permettant le rapport conscient et contrôlé à autrui. De ce fait, la conscience de soi mène à l'identité sociale partagée. L'interactionnisme symbolique paraît donc être une théorie expliquant comment se mettent en place les catégories de la vie sociale au cours d'activités de groupes diverses et complexes[136]. Le sociologue E. Goffman en fait un outil d'analyse de l'identité et montre que c'est par le « stigmate »[137], perçu en termes de relations avec autrui et non pas en tant que marque ou attribut physique spécifique, que les partenaires sont amenés à jouer un rôle[138]. Le stigmate s'analyse en termes relationnels et se définit dans

---

[133] M. MAUSS, « L'âme, le nom et la personne » [1929], *In* M. Mauss et V. Karady (présentation), *Œuvres : Représentations collectives et diversité des civilisations*, t. II, Paris, Les Éditions de Minuit, Coll. Le sens commun, 1968-1969, p. 131-135 ; et M. MAUSS, « Une catégorie de l'esprit humain : la notion de personne, celle de "moi" » [1938], *In* M. Mauss, *Sociologie et anthropologie*, Paris, Presses Universitaires de France, Coll. Bibliothèque de sociologie contemporaine. 1968, p. 331-362.

[134] F. BARTH, *Ethnic Groups and Boundaries: The Social Organisation of Culture Difference*, Waveland Press, 1998.

[135] G.H. MEAD, *L'Esprit, le Soi et la Société*, *Id.,* p. 185-226, et l'auteur indique ainsi que : « *Ainsi le soi parvient à son développement accompli en organisant les attitudes individuelles des autres en attitudes organisées du groupe ou de la société et en devenant ainsi une réflexion individuelle du modèle général de conduite sociale ou groupale dans lequel il est engagé avec autrui.* »

[136] E. GOFFMAN, *La mise en scène de la vie quotidienne, 1. La présentation de soi*, Les Editions de Minuit, Coll. Le sens commun, 1973, p. 22-24

[137] C'est Erving Goffman qui a fait du « stigmate », étymologiquement une marque durable sur la peau, un concept sociologique, en l'étendant à tout attribut social dévalorisant, qu'il soit corporel ou non : handicapé, homosexuel, juif, etc. : C. ROSTAING, « Stigmate », *Les 100 mots de la sociologie*, Paugam Serge (dir.), Paris, Presses universitaires de France, « Que Sais-Je ? », p. 100.

[138] E. GOFFMAN, *Stigmate. Les usages sociaux des handicaps*, Les Éditions de Minuit, Coll. Le sens commun, 1975 (1963), p. 11-13, où l'auteur indique que « *Le mot de stigmate servira donc à désigner un attribut qui jette un discrédit profond, mais il faut bien voir qu'en réalité c'est en termes de relations et non d'attributs qu'il*

le regard d'autrui ; il ne constitue pas un attribut en soi et tend plus à évoquer le concept de la « norme » : toute personne qui ne correspond pas à ce qui est attendue d'une personne considérée comme « normale » est susceptible d'être stigmatisée. Le stigmate naît donc de la représentation faite suite à l'interaction, et est ainsi lié à des stéréotypes.

L'identité semble alors être un jeu de négociations « *lorsque la différence n'est ni immédiatement apparente, ni déjà connue (ou que, du moins, elle n'est pas connue pour être connue), lorsque, en deux mots, l'individu n'est pas discrédité, mais bien discréditable […]* »[139]. Par conséquent, l'individu « stigmatisable » s'attache au contrôle de l'information relevant de son stigmate, soit en le cachant ou en le révélant ou par n'importe quel autre moyen ; l'individu « stigmatisé » est ainsi confronté à une tension entre la norme sociale et sa réalité personnelle. Celui-ci se trouve généralement réduit à son stigmate et toutes ses actions sont alors perçues et raisonnées à travers ce prisme. Dans ce contexte, il paraît donc que les composantes de l'identité s'établissent dans le jeu de l'interaction avec autrui. Premièrement, l'identité sociale résulte de la conformité ou non entre la première impression produite par autrui et les signes qu'il manifeste[140]. Puis, l'identité personnelle s'articule autour du contrôle de l'information à l'occasion d'une situation relationnelle en particulier[141]. À cet égard, il est utile de mentionner les travaux de Ricœur[142] qui aborde la question de l'identité de manière similaire mais son analyse en est différente et se rapproche partiellement de la dernière composante développée par Goffman, à savoir l'identité pour soi. Ricœur distingue deux facettes de l'identité : la « mêmeté », le semblable qui constitue la part objective de l'identité personnelle, et l' « ipséité », le « soi-même » la part subjective de l'identité personnelle[143].

L'identité pour soi, l'identité « sentie », désigne selon Goffman « *le sentiment subjectif de sa situation et de la continuité de son personnage que l'individu en vient à acquérir par suite de ses diverses expériences sociales* »[144]. L'identité d'un individu qui se forme par le jeu de

---

convient de parler. L'attribut qui stigmatise tel possesseur peut confirmer la banalité de tel autre et, par conséquent, ne porte par lui-même ni crédit ni discrédit. »

[139] E. GOFFMAN, *Stigmate, Id.*, p. 57.

[140] E. GOFFMAN, *Stigmate, Id.*, p. 12 et 81-82.

[141] E. GOFFMAN, *Stigmate, Ibid.,* p. 57-58 et 72-74.

[142] P. RICŒUR, *Soi-même comme un autre*, Paris, Éd. du Seuil, 1990.

[143] Selon l'auteur, le *soi* renvoie à la question de l'identité. Mais l'identité elle-même a deux facettes : d'un côté, elle renvoie au même, au semblable, celui dont il est question sur la « carte d'identité », par exemple ; d'autre part, elle signifie le « soi-même », le propre, l'unique que je suis par rapport à un autre, et l'autre que je suis par rapport à lui. Cette interrogation sur le même – *idem*– et le propre – *ipse*– renouvelle l'ancienne dialectique du Même et de l'Autre, puisque l'autre se dit de multiples façons et que le *soi* peut aussi être considéré en tant qu'autre. Soi-même comme un *autre* : l'ipséité est impossible sans l'invariant de l'identité, mais l'identité prend sens par la singularité affirmée de l'ipséité : P. RICOEUR, *Soi-même comme un autre, Id.*, Cinquième & Sixième études – « L'identité personnelle et l'identité narrative » & « Le soi et l'identité narrative », p. 137-198.

[144] E. GOFFMAN, *Stigmate, Id.,* p. 127.

l'interaction résulte, par conséquent, de l'opposition entre une identité définie par autrui (identité « pour autrui ») et une identité pour soi. L'identité pour autrui se compose donc de *« l'identité personnelle et de l'identité sociale d'un individu* [qui] *ressortissent au souci qu'ont les autres de les définir* »[145]. Selon Goffman, chaque membre d'une société a une identité sociale et toute personne en rencontrant une autre va la catégoriser et la classer selon ce que celle-ci laisse voir. C'est ce qui explique la distinction entre « *les identités sociales réelles et virtuelles* »[146]. Par ailleurs, il est important de souligner que l'identité sociale inclut « *des attributs personnels tels que l' « honnêteté », tout autant que des attributs structuraux comme la « profession »* »[147]. L'opposition entre identité pour autrui et identité pour soi ne semble donc pas être figée dans la mesure où « *certes, l'individu se sert pour édifier son image de lui-même des mêmes matériaux que les autres ont déjà utilisé pour lui bâtir une identification sociale et personnelle. Il n'en reste pas moins une grande liberté quant au style de la construction* »[148]. Ce qui induit en conséquence le contrôle (monitoring) de l'information sociale visible ou le maniement de « désidentificateurs » pour dissimuler le stigmate.
Dans ce cadre, pour appréhender le concept d'identité, deux manières semblent se dégager : d'une part, l'identité apparaît comme une donnée stable, naturelle, appliquée à des entités collectives selon la logique anthropologique et, d'autre part, elle semble résulter de l'interaction ce qui la relativise et la centre davantage sur l'individu, suivant les théories de l'interaction. *In fine*, dans la vision des sociologues, le concept d'identité serait plutôt l'une des marques de la modernité et s'appliquerait, de préférence, aux sociétés contemporaines, où il trouverait plus de succès[149].

La notion d'identité devient véritablement centrale à la fin des années 80 lors du « tournant critique », mouvement de l'historiographie française[150]. Un renversement de perspective s'opère, lié, tout d'abord, au développement de l'histoire des représentations. Une histoire culturelle du social se manifeste, qualifiée également d'histoire sociale des représentations[151]. L'idée selon laquelle les groupes sociaux doivent être perçus comme des constructions sociales qui reposent sur l'identification de ceux qui en sont membre émerge. Ils ne doivent plus être

[145] E. GOFFMAN, *Stigmate, Id.,* p. 127.
[146] E. GOFFMAN, *Stigmate, Ibid,* p. 12.
[147] E. GOFFMAN, *Stigmate, Ibid,* p. 12.
[148] E. GOFFMAN, *Stigmate, Ibid,* p. 127-128.
[149] C. DUBAR, *La Crise des identités. L'interprétation d'une mutation,* Paris, Presses Universitaires de France, Coll. Le Lien Social, 3ème Ed., 2007.
[150] Mouvement historiographique qui a vu le jour avec l'éditorial « *Histoire et sciences sociales. Un tournant critique ?* », Annales ESC N° 2, mars-avril 1988, p. 291-293.
[151] R. CHARTIER, « *Le monde comme représentation* », Annales ESC 6, novembre- décembre, 1989.

considérés comme des substances, des catégories immuables et prédéfinies construites de manière artificielle par un historien ou un chercheur qui les envisage comme objet d'analyse. Il paraît dès lors important d'étudier la relation des individus aux catégories auxquelles ils sont supposés appartenir, et une prise en compte des sentiments d'appartenance est centrale pour y parvenir. En réalité, il n'est pas question d'analyser les identités individuelles en soi mais plutôt d'élaborer un outil d'analyse pour juger de la pertinence de telle ou telle catégorie dans une certaine société. Plutôt que d'étudier les catégories sociales d'une façon immuable, il s'agit à ce stade d'analyser les catégories auxquelles les individus s'identifient. Dans cette perspective, catégorie sociale et identité sociale tendent à s'assimiler et à se superposer.

Durant la même période, une autre réflexion entourant la problématique de l'identité s'est manifestée, née en Italie du courant de la micro-histoire, celle des rapports entre le particulier et le général. Ainsi, au XX^{e} Siècle, un micro-historien M. Gribaudi propose une étude nouvelle de la classe ouvrière en prenant en compte les stratégies des différents acteurs sociaux, en traçant leurs trajectoires individuelles[152]. Cette catégorie sociale n'apparaît plus comme un ensemble homogène mais plutôt comme un faisceau d'interactions fluctuantes, complexes. Les identités sociales s'actualisent, dans ce contexte, à travers les interactions et ne constituent pas des substances informant, *a priori*, les comportements des individus, acteurs sociaux. L'histoire des groupes sociaux s'établit alors au niveau des individus*, in fine,* de leurs stratégies et de leurs identités. Par conséquent, toute opération de classification de la société en catégories pertinentes suppose une prise en compte des identité sociales puisqu'elles ne sont que le produit d'interactions complexes et fluctuantes. En effet, « *les hommes ne sont pas dans les catégories sociales comme des billes dans des boîtes, et d'ailleurs les boîtes n'ont d'autre existence que celles que les hommes, en contexte, leur donnent* »[153].

À ce titre, il est important d'évoquer les travaux de S. Fitzpatrick[154] sur les identités sociales en Union soviétique où l'auteure met en exergue les rapports complexes entre classes sociales et identités. En effet, elle démontre que l'identification des individus aux catégories sociales instaurées par l'État soviétique était précaire et instable, en dépit du fait que certains phénomènes d'intériorisation des structures sociales ont pu avoir lieu. En outre, C. Klapisch-Zuber[155] étudie une catégorie en particulier, celle de magnat, dans la société florentine, et

[152] M. GRIBAUDI, *Itinéraires ouvriers. Espaces et groupes sociaux à Turin au début du XXe siècle*, Paris, Éd. de l'École des Hautes Études en Sciences Sociales (E.H.E.S.S.), 1987.
[153] B. LEPETIT, « Histoire des pratiques, pratique de l'histoire », *In* B. Lepetit (dir.), *Les formes de l'expérience. Une autre histoire sociale*, Paris, Albin Michel, 1995, p. 13.
[154] S. FITZPATRICK, *L'identité de classe dans la société de la NEP*, Annales ESC, mars-avril 1989, p. 251-271.
[155] C. KLAPISCH-ZUBER, « La construction de l'identité sociale. Les magnats dans la Florence du Moyen Âge », *In* B. Lepetit (dir.), *Les Formes de l'expérience*, *Id.,* p. 151-164.

montre que cette catégorie se réduisait à un statut juridique, dépourvu dans son essence de tout contenu social. En d'autres termes, cette catégorie s'apparente à une catégorie institutionnelle imposée et à laquelle ne s'identifiaient pas les acteurs sociaux qui en faisaient partie. Ainsi, le critère d'appartenance, de la relation individuelle entre un sujet et le groupe auquel il appartient, s'avère être essentiel permettant de se prononcer sur la pertinence des catégories sociojuridiques et évitant alors de prendre le mot pour la chose[156]. À cet égard, une autre question peut être soulevée : celle de de la relation problématique entre des individus et leur supposée catégorie d'appartenance. Si l'existence d'un statut spécifique est reconnue, la question de savoir si ce statut est porteur d'identité demeure quand même. En effet, les identités étant mouvantes, leur pertinence à une époque en particulier reste à déterminer afin d'éviter une construction artificielle faisant écran avec la réalité sociale.

Par ailleurs, cette relation entre un individu et son groupe d'appartenance engendre le recours et le développement de stratégies dites identitaires. Ces stratégies servent à s'affirmer, à se prononcer devant les autres acteurs sociaux et aident à dessiner, à tracer l'identité de la personne. Inversement, pour cerner l'identité d'un individu, il est donc intéressant d'étudier ses stratégies identitaires, tel que son comportement ou ses paroles. B. Lepetit affirme à cet égard que les identités et les liens sociaux « *n'ont pas de nature, mais seulement des usages* »[157]. Étant donné que les identités ne sont pas fixes mais n'existent que dans leurs actualisations, les stratégies des acteurs sociaux constituent donc un moyen privilégié pour les analyser[158]. En effet, Bayart affirme qu' « *il n'y a pas d'identité « naturelle » qui s'imposerait à nous par la force des choses. […]. Il n'y a que des stratégies identitaires, rationnellement conduites par des acteurs identifiables […] et des rêves ou des cauchemars identitaires auxquels nous adhérons parce qu'ils nous enchantent, ou nous terrorisent. Mais nous ne sommes pas condamnés à demeurer prisonniers de tels sortilèges qui avaient démontré leur inanité bien avant qu'ils ne révèlent leur cruauté ultime […]* »[159]. La thèse de l'auteur consiste à démontrer que toute identité culturelle est identité politique et que, tout au mieux, il n'y a que des constructions politiques, économiques, culturelles, des stratégies identitaires.

[156] C. KLAPISCH-ZUBER, « La construction de l'identité sociale. Les magnats dans la Florence du Moyen Âge », *Id.,* p. 153-160.
[157] B. LEPETIT, « Histoire des pratiques, pratique de l'histoire », *Id.*, p. 13.
[158] J.-F. BAYART, *L'Illusion identitaire*, Librairie Arthème Fayard, Coll. Pluriel, 2018, ouvrage dans lequel l'auteur affirme principalement qu'il n'y a pas d'identité naturelle, mais uniquement des stratégies identitaires.
[159] J.-F. BAYART, *L'Illusion identitaire*, *Id.,* p. 10.

En raison de sa transversalité disciplinaire, la notion d'identité s'avère ainsi être polysémique, complexe et multiforme, caractéristique de l'être humain. De façon générale, elle représente un ensemble de caractéristiques individuelles et collectives qui permettent de définir clairement un objet, lui accordant ainsi une identité. Comme il a été vu précédemment, dans la psychologie et la philosophie sociale, l'identité se définit comme le résultat d'une interaction particulière entre le psychologique et le social chez un individu. En d'autres termes, elle est le produit des processus interactifs entre l'individu et la société, donc le champ social, qui s'actualise dans une représentation de soi. Dès lors, il semblerait que le rapport entre identité personnelle et identité sociale, souvent assimilé à une opposition entre le personnel et le collectif, représente le noyau principal de la problématique de l'identité. C'est « *dans l'interaction avec autrui que se construit, s'actualise, se confirme ou s'infirme l'identité* »[160] annonce Lipiansky. Elle représente donc une tension entre ces deux pôles, ce qui rejoint également la philosophie de Ricœur sur la notion d'identité narrative. Tel qu'il a été vu, selon l'auteur l'identité personnelle est polarisée entre mêmeté et ipséité. Or, l'identité narrative, celle construite dans et par le récit qu'il soit littéraire ou historique, sert de médiation entre ces deux pôles de l'identité. En outre, Mucchielli, dans son ouvrage Identité, définit celle-ci comme « *un ensemble de significations apposées par des acteurs sur une réalité physique et subjective, plus ou moins floue, de leurs mondes vécus, ensemble construit par un autre acteur. C'est donc un sens perçu donné par chaque acteur au sujet de lui-même ou d'autres acteurs* »[161]. Dans cette perspective, l'identité semble être unique, permettant de se distinguer des autres, de se reconnaître et de s'identifier à autrui. Selon l'auteur, l'identité de chaque individu a une double face : l'une, intérieure, subjective, c'est la valorisation de soi et l'autre extérieure, objective, celle énoncée par autrui. L'identité subjective, valorisante de soi correspond à un jugement porté sur soi-même alors que celle énoncée par autrui se forme notamment par les jugements des partenaires, des autres individus ; ce qui se manifeste, à l'ère du numérique, à travers les concepts de e-réputation ou de notoriété numérique[162]. Mucchielli en déduit ainsi que l'identité que nous énonçons est fonction de la situation dans laquelle nous sommes et des besoins d'information de nos partenaires[163].

L'approche de Mucchielli s'assemble, s'allie sur celle multidimensionnelle développée par Erikson. En effet, le concept de ce dernier, s'inspirant des apports de la psychanalyse, se traduit

[160] E. -M. LIPIANSKY, *Identité et Communication : l'expérience groupale*, Paris, PUF, Coll. Psychologie sociale, 1992, p. 162.
[161] A. MUCCHIELLI, *L'Identité*, Paris, PUF, Coll. Que sais-je ?, 2013, p. 119.
[162] *Cf.* p. 103, 168 et 198.
[163] A. MUCCHIELLI, *L'Identité*, *Id.,* p. 120-122.

par la définition de soi, à savoir par les caractéristiques qu'un individu identifie comme étant siennes et auxquelles il accorde une valeur importante pour s'affirmer et se reconnaître. Le terme d'identité, ou de « sentiment d'identité », correspond pour Erikson au « *sentiment subjectif et tonique d'une unité personnelle (sameness) et d'une continuité temporelle (continuity)* »[164]. Ce sentiment constitue alors le résultat d'un double processus s'opérant en même temps « *au cœur de la culture de l'individu ainsi qu'au cœur de la culture de sa communauté* »[165]. Zavalloni développe en ce sens un concept égo-écologique[166] dans lequel se manifeste la nature interactive et dynamique de l'identité. L'auteure met notamment en valeur l'interdépendance étroite qui existe entre les processus intrapsychiques et socio-psychologiques dans la formation de l'identité. L'identité sociale désigne pour Zavalloni la représentation que le sujet se fait de son environnement social, à savoir des différents groupes sociaux auxquels l'individu s'associe, de ses groupes d'appartenance mais également de ses groupes d'opposition (de non appartenance). Selon la conceptualisation de l'auteure, les notions d'identité et d'appartenance sont étroitement liées et l'identité se manifeste comme une structure organisée des représentations de soi et des autres. C'est donc l'ensemble des représentations vécues découlant du rapport entre individu et société.

Dès lors, le concept de représentation sociale, introduit par Zavalloni pour l'étude de l'identité, souligne l'importance des processus d'inclusion et d'exclusion qui caractérisent les constructions identitaires à partir de l'opposition « Nous – Eux »[167]. Ainsi, l'identité se forme à partir des organisations de soi et de groupes d'appartenance en tant qu'entité ou « *structure cognitive liée à la pensée représentationnelle* » indique Baugnet[168]. En d'autres termes, le concept d'identité « *désigne donc le noyau central de la personnalité individuelle, sorte de résultante d'un ensemble donné de composantes psychologiques et sociologiques* »[169].

---

[164] E. H. ERIKSON, *Adolescence et crise. La quête de l'identité*, Paris, Ed. Flammarion, Coll. Champs Essais, 2011 (1972), p. 173.
[165] E. ERIKSON, *Enfance et société*, *Id*, p. 17.
[166] M. ZAVALLONI, *Égo-écologie et Identité : une approche naturaliste*, Paris, PUF, Coll. Psychologie sociale, 2007.
[167] M. ZAVALLONI et C. LOUIS-GUÉRIN, *Identité sociale et Conscience : Introduction à l'égo-écologie*, Montréal, PUM, 1984.
[168] L. BAUGNET, *Métamorphoses identitaires*, Bruxelles, P.I.E.- Peter Lang S. A., 2001, p. 21.
[169] M. ZAVALLONI, « L'identité psychosociale, un concept à la recherche d'une science », *In* S. Moscovici (éd.), *Introduction à la psychologie sociale,* Paris, Larousse, 1972, t. II, (p. 245-265), p. 245.

B. L'identité, fruit d'un processus de représentation et d'évaluation

Afin de comprendre la construction de la réalité sociale, l'identité semble donc être un objet privilégié puisque le rapport à la société, au monde s'élabore à travers ces appartenances sociales et culturelles[170].

Pour Zavalloni, « *l'identité serait constituée par le contenu, la structure et l'organisation dynamique de l'environnement intérieur subjectif en tant que lieu de contrôle et d'anticipation et en même temps, reflet des actions quotidiennes. Les concepts d'identité psychosociale et d'environnement intérieur opératoire peuvent ainsi être considérés comme interchangeables dans cette perspective* »[171]. Selon l'auteure, l'égo-écologie comprend l'étude de Soi dans ses relations complexes et fluctuantes avec son environnement. Le postulat de départ dans cette étude égo-écologique est de considérer l'individu dans son rapport au monde comme situé, de façon objective, à l'intérieur d'une matrice sociale. Les éléments composant cette matrice sont les différents groupes auxquels l'individu appartient de fait et par affiliation, en tant que membre d'une certaine société ou culture particulière, ainsi que les groupes ou les individus significatifs avec lesquels l'individu entretient des relations symboliques ou réelles. Selon l'auteure, la construction de la réalité sociale, telle qu'elle émerge dans la perception, dans la conscience individuelle, désigne l'environnement interne opératoire d'un individu et l'étude de cet environnement représente alors l'égo-écologie. Par conséquent, les éléments de la matrice sociale forment les parties constituantes d'un individu en tant qu'acteur social tout en constituant, à la fois, un milieu au sens écologique qui couvre une large part de la réalité environnante[172]. Comme le souligne Zavalloni, l'égo-écologie a mis l'accent sur les processus interactifs reliant l'individu à son environnement en plus de ses caractéristiques individuelles. Par ailleurs, la méthode élaborée analyse concrètement le substrat qui sert de support au discours au lieu de le déduire en tant que « construit hypothétique »[173].

De plus, l'auteure distingue « l'identité sociale subjective », le soi individuel, de « l'identité sociale objective » le soi social, manière de se situer dans l'environnement social à travers « l'environnement intérieur opératoire » ; celui-ci comprenant des images, des jugements, des concepts qui concernent le rapport soi-autrui et le monde social. Cet environnement est également constitué de catégories et de représentations qui s'articulent de manière différente avec les stimuli internes (images, souvenirs ...) ou externes (perceptions de l'environnement).

[170] M. ZAVALLONI et C. LOUIS-GUÉRIN, *Identité sociale et Conscience, Id.,* p. 8.
[171] M. ZAVALLONI et C. LOUIS-GUÉRIN, *Identité sociale et Conscience, Id.*, p. 12.
[172] M. ZAVALLONI et C. LOUIS-GUÉRIN, *Identité sociale et Conscience, Ibid.*, p. 201.
[173] M. ZAVALLONI et C. LOUIS-GUÉRIN, *Identité sociale et Conscience, Ibid.,* p. 9.

Selon Zavalloni, le contenu de cet environnement s'exprimerait sous l'action de stimulations externes, tels que les mots d'un discours, ou une image sur un réseau. Ensuite, elle affirme que l'identité serait une forme de mémoire d'expériences et de représentations chargées affectivement qui guident, de manière inconsciente, le discours sur soi, l'autre et la société, et qui intervient dans la relation entre la personne et son environnement socio-culturel[174]. L'identité, en tant que production sociale et cognitive, vise ainsi la relation qui s'établit entre l'individu et l'environnement puisque c'est à l'interface du psychologique et du social que se construit la notion de représentation sociale[175]. De ce fait, l'identité objective se constitue par les groupes sélectionnés et l'identité subjective concerne, pour sa part, les représentations que l'individu se fait de ces groupes. Par conséquent, l'identité sociale objective ou « matrice sociale » semble indiquer que la réalité sociale, à savoir les sociétés, les divers groupes sociaux auxquels un individu est confronté, correspond à l'essence de son identité. Les représentations s'incorporent donc dans cette structure médiatrice entre le soi social et le soi individuel et s'associent à l'expérience unique de l'individu. La construction de l'identité d'une personne ne relève pas alors uniquement des groupes d'appartenance, mais s'élabore aussi à travers les groupes auxquels elle n'appartient pas[176], étant donné que les représentations sociales sont utilisées là où elles ont un sens pour le sujet.

D'un autre point de vue, les analyses de Tajfel sur l'identité sociale situent avant tout l'identité comme munie de cognitions à la fois d'ordre collectif et individuel. L'identité est constituée selon l'auteur « *par les aspects de l'image de soi d'un individu qui dérivent des catégories sociales auxquelles il voit qu'il appartient* »[177]. La catégorisation sociale constitue donc le processus cognitif intermédiaire permettant d'accorder un sens à l'individu sur divers aspects du monde social qui l'entoure[178]. L'auteur synthétise en un ensemble cognitivement cohérent les différentes informations qui concernent ces différents groupes d'appartenance. Pour Tajfel,

---

[174] M. ZAVALLONI, "E-motional memory and the identity system: Its interplay with representations of the social world", *In* K. Deaux & G. Philogène (éds.), *Representations of the Social: Bridging theoretical traditions*, Oxford, UK, Blackwell publishing, 2001, p. 285-304.

[175] L. BAUGNET, *Métamorphoses identitaires*, *Id.*, p. 25.

[176] H. CHAUCHAT, « Du fondement social de l'identité du sujet », *In* H. Chauchat, A. Duran-Delvigne, *De l'identité du sujet au lien social*, Paris, PUF, 1999, p.11.

[177] A.M. DE LA HAYE, *La catégorisation des personnes*, Grenoble, Presses Universitaires de Grenoble, 1998, p. 35, et, H. TAJFEL et J. TURNER, "An integrative theory of intergroup conflict", *In* J. A. Williams & S. Worchel (éds.), *The social psychology of intergroup relations,* Monterey, CA, Ed. Brooks/Cole, 1979, p. 33-47.

[178] Tajfel souligne que « *les caractéristiques de son propre groupe (son statut, sa richesse ou sa pauvreté, sa couleur de peau, sa capacité à atteindre ses buts) n'acquièrent de signification qu'en liaison avec les différences perçues avec les autres groupes et avec leurs différences évaluatives [...] un groupe devient un groupe en ce sens qu'il est perçu comme ayant des caractéristiques communes ou un devenir commun, que si d'autres groupes sont présents dans l'environnement.* », H. TAJFEL, « La catégorisation sociale », *In* S. Moscovici (éd.), *Introduction à la psychologie sociale*, Paris, Larousse Vol. I, 1972, (p. 272-302), p. 295.

l'identité sociale est définie comme « *la connaissance qu'on a d'appartenir à certains groupes sociaux et la signification émotionnelle et évaluative qui résulte de cette appartenance* »[179]. Il semble alors que les groupes sociaux bénéficient, pour se définir, des images et des informations dont ils disposent sur les autres groupes grâce à la catégorisation sociale, qui présente également une autre fonction : celle d'ordonner et de systématiser l'environnement social. L'identité sociale, telle qu'elle est conçue par Tajfel est donc principalement une identité individuelle qui intègre la diversité des appartenances collectives. Pour Turner, le soi ne se forme pas comme un ensemble de représentations stables, fixes mais plutôt comme des catégories de soi versatiles suivant les relations sociales développées[180]. Selon Augoustinos, il existe des relations fonctionnelles entre catégorie sociale, représentation sociale et identité sociale qu'il définit ainsi : « *la centralité et la signification des catégories sociales particulières et leurs représentations sociales associées dépendent de la position d'un sujet et de la position du groupe dans sa relation à la catégorie* »[181].

In fine, ce qui importe dans ce contexte n'est pas particulièrement la réalité sociale des catégories auxquelles les individus appartiennent, mais plutôt le sens que ces catégories ont pour eux. Celles-ci semblent être en interaction permanente avec les représentations sociales, facilitant l'adaptation d'une personne à son environnement et s'avérant être une source essentielle pour la construction et le changement identitaires. Les représentations évoquent, dans cette perspective, les activités de traitement de l'information et les développements des technologies de l'information et de communication qui permettent une adaptation plus facile de l'individu à son environnement.

D'un autre côté, Doise considère le Soi comme étant une représentation sociale puisqu'il note des « *ressemblances frappantes des descriptions de soi à travers les frontières de différentes catégories d'appartenance* »[182]. De ce fait, l'identité personnelle s'entend comme une représentation sociale, « *comme un principe générateur de prise de position [...] concernant le moi* »[183]. Le monde social fournit donc des références essentielles aux individus ainsi qu'aux

---

[179] H. TAJFEL, « La catégorisation sociale », *Id.*, p. 296.
[180] J. C. TURNER, "Some currents issues in research on social identity and self categorisation theories" *In* N. Ellemers, R. Spears, et B. Doosje (éds.), *Social Identity: Context, commitment, content*, Oxford, UK, Blackwell, 1999, p. 6-34.
[181] M. AUGOUSTINOS, "Social categorization: Toward theorical Integration", *In* K. Deaux & G. Philogène (éds.), *Representations of the Social: Bridging theoretical traditions*, Oxford, UK, Blackwell, 2001, (p. 201-216), p. 207.
[182] W. DOISE, « L'individualisme comme représentation collective », *In* J.-C. Deschamps, J.-F. Morales, D. Paez et S. Worchel (éds.), *L'identité sociale,* Grenoble, Presses Universitaires de Grenoble, 1999, (p. 195-212), p. 199.
[183] W. DOISE, « L'individualisme comme représentation collective », *Id.*, p. 211.

groupes pour la construction de leurs identités. Par ailleurs, une conception cognitive du Soi est proposée par Markus qui montre l'existence de « schémas de soi »[184]. Ceux-ci sont constitués par les représentations cognitives issues d'évènements particuliers et de situations qui impliquent l'individu, mais aussi, par les représentations plus globales issues de la catégorisation et de l'évaluation du comportement de l'individu par soi-même ou par autrui. Ces schémas correspondent ainsi à un ensemble de représentations de soi établies à partir des expériences du sujet dans le monde social. Dès lors, construire son identité comprend une démarche individuelle ainsi qu'une démarche collective qui dépend largement des références sociales et culturelles dominantes partagées au sein d'une même société. Comme l'annoncent Oyserman et Markus, « *les représentations sociales sont des blocs sur lesquels le soi se construit* »[185]. Dans ce contexte, changer d'environnement entraîne *de facto* une modification des références identitaires ainsi qu'une rupture avec une certaine conceptualisation de soi. Il faut donc chercher le sens du soi à travers les images, les idées, le langage, les cultures nouvelles au sein du nouvel environnement social. Selon ces auteurs, le but d'aborder le soi comme représentation sociale permet la prise en compte de divers contextes dans lesquels les individus se trouvent simultanément impliqués. L'individu, pour se définir, se sert des termes et des références rendus disponibles par les représentations, impliquant par conséquent le fait que les représentations sociales contribuent à la construction de la réalité sociale en renforçant certaines perceptions tout en en réduisant d'autres.

Il paraît alors que la construction de l'identité s'opère, d'une part, dans le monde extérieur objectif et, d'autre part, dans le travail intérieur de traitement et de sélection pour soi des références identitaires proposées. L'identité se forme, indique Duveen, au moyen d'une action d'intégration de certaines représentations, relativement volontaire, et relève deux types de relation entre l'identité et les représentations sociales[186] : la première relation, qualifiée d' « obligation impérative », correspond aux représentations sociales qui obligent les individus à adopter une identité en fonction de catégories sociales données, telles que l'identité de genre par exemple ; la seconde, qualifiée pour sa part d' « obligation contractuelle », vise les représentations sociales exerçant leur influence à partir du moment où un individu rejoint volontairement un groupe social et s'engage à adopter une certaine identité sociale. Les

[184] H. R. MARKUS, *Self-schemata and Processing Information about the Self*, Journal of Personality and Social Psychology, Vol. 35, Février 1977, N° 2, p. 63-78.
[185] D. OYSERMAN & H. R. MARKUS, "Self as social representation", *In* S. U. Flick (éd.), *The Psychology of the Self*, Cambridge, Cambridge University Press, 1998, (p. 107-125), p. 118.
[186] G. DUVEEN, "Representations, Identities, Resistance", *In* K. Deaux & G. Philogène (éds.), *Representations of the social: Bridging theoretical traditions*, Oxford, UK, Blackwell publishing, 2001, p. 257-270.

représentations sociales semblent donc imposer une construction identitaire élaborée en référence à l'ensemble des normes implicites ou explicites existantes, et applicables, dans le monde social au sein duquel l'individu évolue. Dans cette perspective, l'identité désigne principalement un produit social et culturel.

Dans une autre optique, des auteurs avancent que certaines représentations sociales s'incorporent dans l'environnement intime des acteurs sociaux entraînant alors des transformations. L'identité personnelle se réfère, dans ce contexte, à une entité cognitive et émotionnelle qui se fonde sur les représentations sociales en les réinterprétant, de manière subjective, pour se construire. Ainsi, nous informe Breakwell, les groupes produisent, de manière individuelle et collective, des représentations sociales qui comportent deux dimensions : les représentations sociales en tant que processus de transformation de la réalité sociale mais aussi les représentations comme produit de ce processus[187]. Pour Guichard, l'existence de deux structures fondent la conceptualisation de la représentation de soi et d'autrui : les cadres cognitifs identitaires ainsi que les formes identitaires subjectives[188]. Les cadres cognitifs identitaires sont « *relatifs à des catégorisations sociales et communautaires de toutes sortes : de genre (homme-femme), de religion, de position sociale, d'orientation sexuelle, d'âge, de métier, de participation à un loisir, de choix politique, etc. Ils peuvent renvoyer à des caractérologies (« stressé-cool ») ou à des typologies (une astrologie, par exemple)* »[189]. Autrement dit, tout individu possède en mémoire des structures cognitives comme des catégories, des schémas, des scripts, des modèles mentaux, des représentations sociales qui lui permettent d'établir sa propre vision du monde et de se construire. Guichard rajoute que « *les valeurs par défaut des attributs des cadres identitaires semblent correspondre à des stéréotypes sociaux »*[190]. Il poursuit en partant de l'hypothèse que dans la mesure où les concepts n'existent pas indépendamment les uns des autres mais forment un système, ces cadres cognitifs identitaires constituent par conséquent, pour chaque individu, un système de cadres cognitifs identitaire. D'après l'auteur, ce cadre « *constitue la représentation intériorisée par l'individu de l'offre identitaire de la société où il interagit, telle qu'il a pu se la construire en fonction de*

[187] G. BREAKWELL, "Integrating paradigms, methodological implications", *In* G.M. Breakwell et D. V. Canter (éds.), *Empirical approaches to social representations*, Oxford, UK, Oxford University Press, 1993, p. 180-201.
[188] J. GUICHARD, « Se faire soi », *L'Orientation scolaire et professionnelle, 33/4*, Éd. INETOP, 2004, p. 499-533 ; Disponible en ligne : http://osp.revues.org/226
[189] J. GUICHARD, « Se faire soi », *Id.*, p. 507.
[190] J. GUICHARD, « Se faire soi », *Id.*, p. 507 ; l'auteur donne ainsi un ex. *« Par exemple, hic et nunc, le cadre identitaire « ingénieur » comprend l'attribut « genre » dont la valeur par défaut est « masculin » (Guichard & Bidot, 1989).* ».

ses interactions, compte tenu des positions qu'il occupe dans les différents champs sociaux où il se situe »[191] ; le tout pouvant différer d'une personne à une autre en fonction de la diversité de l'insertion sociale. Ces cadres identitaires représentent ainsi « *des substrats permettant la représentation, le jugement et l'action* »[192]. Cependant, un autre processus qui se fonde sur les cadres identitaires doit être employé pour la construction de soi, à savoir les formes identitaires qui s'entendent « *comme une vision d'autrui ou de soi-même ou comme une construction de soi selon la structure d'un cadre identitaire déterminé* »[193]. Ces formes sont donc conçues en tant qu'agencement historique et social de mode de désignations, d'appartenances, mais également en tant que rapports entre processus d'identification pour soi et pour autrui. Ce qui incite Dubar à indiquer que si l'identité relève de processus, il faut donc la percevoir comme une identification et distinguer les identifications attribuées (identité pour autrui) des identifications revendiquées (identité pour soi)[194]. En effet, indique l'auteur, « […] *il existe un mouvement historique, à la fois très ancien et très incertain, de passage d'un certain mode d'identification à un autre. Il s'agit, plus précisément, de processus historiques, à la fois collectifs et individuels, qui modifient la configuration des formes identitaires définies comme modalités d'identification* »[195]. En prenant comme référence Weber, l'auteur distingue deux formes identitaires idéales-typiques : les formes identitaires « communautaires » et celles « sociétaires ». Les premières, étant les plus anciennes, Dubar les qualifie de communautaires, celles qui « *supposent la croyance dans l'existence de groupements appelés "communautés" considérés comme des systèmes de place et de noms préassignés aux individus et se reproduisant à l'identique à travers les générations. Dans cette perspective, chaque individu a une appartenance considérée comme principale en tant que membre de sa « communauté » et une position singulière en tant qu'occupant une place au sein de celle-ci. [...]. Qu'il s'agisse de "cultures" ou de "nations", d' "ethnies" ou de corporations, ces groupes d'appartenance sont considérés, par les Pouvoirs et par les personnes elles-mêmes, comme des sources « essentielles » d'identités* »[196]. Alors que les secondes formes, celles qui sont les plus récentes « voire en émergence », sont nommées sociétaires puisqu'elles « *supposent l'existence de collectifs multiples, variables, éphémères, auxquels les individus adhèrent pour des périodes*

[191] J. GUICHARD, « Se faire soi », *Ibid.,* p. 508.
[192] J. GUICHARD, « Se faire soi », *Ibid.,* p. 508.
[193] J. GUICHARD, « Se faire soi », *Ibidem,* p. 508-509.
[194] C. DUBAR, *La Crise des identités, op. cit.*, pp. 1-6.
[195] C. DUBAR, *La Crise des identités, Id.*, p. 4.
[196] C. DUBAR, *La Crise des identités, Id.*, p. 4-5, et l'auteur précise ainsi que « *Ces manières d'identifier les individus à partir de leur groupe d'appartenance persistent dans les sociétés modernes et peuvent être assumées par les personnes elles-mêmes : elles peuvent être « pour soi » aussi bien que « pour autrui ».* »

limitées et qui leur fournissent des ressources d'identification qu'ils gèrent de manière diverse et provisoire »[197].

Dans son analyse, Dubar traite des crises économiques et du « lien social » qui traversent les individus sommés de se constituer et de s'assumer en tant que sujets sociaux socialement dépendants, mais aussi comme sujets incités à l'autonomisation, à la réalisation de soi. Pour l'auteur, l'identité personnelle ne se définit pas par l'appartenance « héritée » à une culture fixe, « figée », ni par le rattachement à une catégorie statutaire immuable, « donnée », c'est « *un processus d'appropriation de ressources et construction de repères, un apprentissage expérientiel, la conquête permanente d'une identité narrative (Soi-projet) par et dans l'action collective avec d'autres choisis* »[198]. Elle implique donc une « attitude réflexive (Soi-même) » permettant la construction de sa propre histoire, « Soi », en même temps que sa propre insertion dans l'Histoire, « Nous »[199]. Dans cette logique, plusieurs types d'identités personnelles existent, « *plusieurs manières de construire des identifications de soi-même et des autres, plusieurs modes de construction de la subjectivité, à la fois sociale et psychique, qui sont autant de combinaisons des formes identitaires initialement définies* »[200].

Finalement, comme l'a relevé Goffman, « *ce n'est probablement pas par un pur hasard historique que le mot personne, dans son sens premier, signifie un masque. C'est plutôt la reconnaissance du fait que tout le monde, toujours et partout, joue un rôle, plus ou moins consciemment. [...]. C'est dans ces rôles que nous nous connaissons les uns les autres, et que nous nous connaissons nous-mêmes. [...]. En un sens, et pour autant qu'il représente l'idée que nous nous faisons de nous-même – le rôle que nous nous efforçons d'assumer –, ce masque est notre vrai moi, le moi que nous voudrions être. À la longue, l'idée que nous avons de notre rôle devient une seconde nature et une partie intégrante de notre personnalité. Nous venons au monde comme individus, nous assumons un personnage, et nous devenons des personnes* »[201],

---

[197] C. DUBAR, *La Crise des identités, Ibid.*, p. 5, l'auteur rajoute que « *Dans cette perspective, chacun possède de multiples appartenances qui peuvent changer au cours d'une vie. Ces formes sont liées à des croyances différentes des précédentes, en particulier celles du primat du sujet individuel sur les appartenances collectives et de la primauté des identifications « pour soi » sur les identifications « pour autrui ». Les identifications de type sociétaire peuvent produire des identités « pour autrui » comme des identités « pour soi » selon la nature des catégories utilisées.* ».

[198] C. DUBAR, *La Crise des identités, Ibid.*, p. 200.

[199] C. DUBAR, *La Crise des identités, Ibidem*, p. 200, l'auteur souligne ainsi que « *L'identité personnelle des sujets apprenants n'est donc pas donnée, telle quelle, à la naissance. Elle se construit durant toute la vie.* »

[200] C. DUBAR, *La Crise des identités, Ibidem*, p. 173, et l'auteur indique à cet égard « *Avec l'hypothèse complémentaire d'une forme dominante qui assure, pour un temps, une certaine cohérence (ipséité) et, dans la durée, une certaine permanence (mêmeté) à l'identité personnelle ; […].* » (note de bas de p. n° 2)

[201] E. GOFFMAN, *La mise en scène de la vie quotidienne, 1. La présentation de soi*, *op. cit.,* p. 27.

mais l'identité, contributrice au rôle que l'individu choisi, demeure fluctuante et versatile appuyant ou limitant les caractéristiques du personnage sélectionné.

§2. Le rôle du monde légal

Le monde légal a eu une influence quant à l'édification du concept d'identité qui se révèle à travers, d'un côté, le processus d'identification et d'individualisation des personnes (A), mais également celui de leur auto-construction et de leur auto-détermination (B), de l'autre, aboutissant à la caractérisation de leur identité.

A. L'identité, un processus d'identification et d'individualisation

Dans un cadre purement légal, l'identité est conçue comme « *l'ensemble des composantes grâce auxquelles est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalité, filiation, etc.)* »[202]. Elle désigne, en particulier, l'identité civile, judiciaire et s'envisage comme un agrégat de composantes permettant de différencier une personne de ses semblables. Néanmoins, dresser une liste exhaustive des attributs composants l'identité d'une personne semble être, même du côté juridique, un défi quasi-irréalisable.

Historiquement, tracer l'identité des individus se fondait essentiellement sur la reconnaissance entre ceux-ci qui vivaient principalement dans des communautés fermées et stables. Puis, en réponse aux besoins des États et de leurs fonctionnements, vinrent les premiers dispositifs de recensement de la population et d'État civil portant, d'abord, sur la mobilisation des troupes militaires, qui se sont propagés par la suite dans les domaines de fiscalité et de police et justice ; l'identité et sa détermination permettant ainsi à l'État d'individualiser une personne pour répondre à ses besoins de recensement. Il semble alors que l'identité évolue en fonction de l'évolution des sociétés, de ces cadres, de ces contextes, de ces choix politiques et de ces institutions. Précisément, les papiers d'identité ont vu le jour avec l'essor des transports, l'urbanisation, la montée de l'individualisme, l'industrialisation et ainsi de suite. Disposer d'un moyen d'identifier une personne sans s'appuyer sur une tierce personne la reconnaissant devenait, par conséquent, une nécessité.

Avec le développement de l'administration, et afin que l'individualisation d'une personne puisse se faire à tout moment, les États ont mis en place un système d'identification permettant,

[202] S. GUINCHARD et T. DEBARD (dir.), *Lexique des Termes Juridiques*, « Identité », Paris, Dalloz, 19e éd., 2012, p. 449.

dès cette époque, de tracer chaque individu tout en conservant les éléments le caractérisant. Pour ce faire, un certain nombre de critères, considérés comme fondamentaux, ont été choisis pour décrire un individu. En droit français, un système de constatation de l'état civil a été établi et il est d'ordre public ; dès lors, toute personne dispose d'un état dont elle ne peut se dispenser. Cet état civil est également opposable de plein droit aux tierces personnes et sans publicité. En effet, « *aucun citoyen ne pourra porter de nom, ni de prénom autres que ceux exprimés dans son acte de naissance. Ceux qui les auraient quittés sont tenus de les reprendre.* »[203]. L'individualisation, ou individuation, paraît ainsi être déclenchée, et de façon irréversible, par le biais de l'identité civile, propriété de sa singularité, une singularité partiellement « quelconque » : *« […] une manière jaillissante est également le lieu de la singularité quelconque, son principium individuationis. Pour l'être qui est sa propre manière, celle-ci n'est pas, en effet, une propriété qui le détermine et l'identifie comme une essence, mais plutôt une impropriété ; ce qui toutefois le rend exemplaire, c'est que cette impropriété est assumée et appropriée comme son être unique. L'exemple n'est que l'être dont il est l'exemple : mais cet être ne lui appartient pas, il est parfaitement commun. L'impropriété, que nous exposons comme notre être propre, la manière, dont nous faisons usage, nous engendre, elle est notre seconde nature, la plus heureuse* »[204].

En France, « l'encartement » date de 1749 quand « *un certain Guillaute, officier de la maréchaussée d'Île-de-France, adresse au roi un Mémoire sur la Réformation de la Police de France, dans lequel il propose de mettre en place un système d'immatriculation des hommes, des rues et des immeubles. Le contenu de ce texte résume à lui seul toute la teneur de ce qui constitue alors la priorité majeure des forces de l'ordre : surveiller, surveiller toujours plus et mieux* »[205].

Apparaissent ensuite le « passe-port à l'Intérieur » institué, selon Piazza, le 1er février 1789 et le « livret ouvrier » qui date, quant à lui, de 1749. À la suite de cela, Alphonse Bertillon, devenu responsable du service de l'Identité judiciaire de la préfecture de Paris, rationalise toutes les pratiques policières en matière de photographie et de relevé des marques corporelles[206]. Sa technique anthropométrique consistant à relever, de manière systématique et normalisée, les

[203] Loi du 6 Fructidor An II (23 août 1794) portant qu'aucun citoyen ne pourra porter de nom ni de prénom autres que ceux exprimés dans son acte de naissance (N° 240), Art 1er : https://gallica.bnf.fr/ark:/12148/bpt6k56373g/f464.image

[204] G. AGAMBEN, *La communauté qui vient : Théorie de la singularité quelconque*, Ed. du Seuil, Coll. La librairie du XXIe siècle, 1990, p. 35.

[205] P. PIAZZA, *Histoire de la Carte Nationale d'Identité*, Ed. Odile Jacob, Coll. Histoire et Document, 2004, p. 31.

[206] P. PIAZZA, *Histoire de la Carte Nationale d'Identité*, *Id.*, p. 85.

« signes particuliers » et les mensurations physiques en y intégrant progressivement la photographie, s'applique au début, indique l'auteur, aux vagabonds, nomades et délinquants récidivistes. Avec le temps, cette méthode a été concurrencée par la « dactyloscopie », procédé d'identification par le relevé d'empreintes digitales. En outre, pendant cette période, la France met en place un « carnet anthropométrique d'identité » comprenant des « photographies de profil et de face », une « empreinte simultanée et non roulée des doigts réunis : auriculaire, annulaire, médius, index gauche » ainsi qu'une « empreinte prise séparément du pouce gauche »[207]. Puis, en 1921, le Préfet de police « *institue une carte d'identité que peuvent obtenir tous les français domiciliés à Paris ou dans le département de la Seine. [...]. En quelques années, elle fait l'objet d'une reconnaissance et d'une diffusion de plus en plus massive* »[208]. Celle-ci prévoyait d'inclure une photo « faites de face, sans chapeau » ainsi qu'une empreinte digitale. À partir de 1943, elle commence à être délivrée dans douze départements, dont Paris[209]. Et par un décret du 22 octobre 1955, le Ministère de l'Intérieur mis en place la première « *carte nationale d'identité certifiant l'identité de son titulaire* »[210].

Depuis lors, les éléments d'identité d'un sujet, tels que son nom, son sexe, sa nationalité ou autre, peuvent être démontrés, prouvés par tout moyen grâce aux divers documents officiels mis en place : carte d'identité nationale, passeport en cours de validité, livret de famille, ou encore, extrait d'acte de naissance. Ces différents agrégats, présents dans ces divers documents, ont la caractéristique d'être immuable, indisponible et imprescriptible, sous certaines réserves prévues expressément par la loi. Ainsi, ils contribuent à ce qu'un individu soit « lui-même » tout en marquant son existence en tant que « sujet de droit », détenant une « personnalité juridique ». Dans cette perspective, ces différents attributs traduisent, de façon partielle et

---

[207] P. PIAZZA, *Histoire de la Carte Nationale d'Identité*, *Ibid.*, p. 115. Selon l'auteur, il existait 20 000 exemplaires de « carnet anthropométrique d'identité » délivré aux nomades en 1913 et 30 000 exemplaires en 1923.

[208] P. PIAZZA, *Histoire de la Carte Nationale d'Identité*, *Ibid.*, p. 128.

[209] P. PIAZZA, *Histoire de la Carte Nationale d'Identité*, *Ibidem*, p. 164. L'auteur relève ainsi « le rôle déterminant des Préfectures », l'importance attachée à « la rédaction du signalement », « l'apposition des empreintes digitales », « la qualité des photographies », « les données de l'état civil », « l'archivage minutieux » mais aussi « les services statistiques » dirigés par René Carmille : p. 169-187.

[210] Décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité, Art. 1 « *[...]. La carte nationale d'identité mentionne :*
1° Le nom de famille, les prénoms, la date et le lieu de naissance, le sexe, la taille, la nationalité, le domicile ou la résidence de l'intéressé ou, le cas échéant, le lieu où il a fait élection de domicile dans les conditions prévues à l'article L. 264-1 du code de l'action sociale et des familles, et, si celui-ci le demande, le nom dont l'usage est autorisé par la loi ;
2° L'autorité de délivrance du document, la date de celle-ci, sa durée de validité avec indication de sa limite de validité, le nom et la signature de l'autorité qui a délivré la carte ;
3° Le numéro de la carte.
Elle comporte également la photographie et la signature du titulaire. ».

implicite, la conception duale de l'identité de Ricœur et en particulier son concept de la « mêmeté » susvisé (l'identité *idem*)[211].

Il est, de plus, important de souligner qu'en droit français, il ne s'est pas avéré nécessaire, semble-t-il, de fournir une définition légale de ce qu'est l'identité. Même la loi du 27 mars 2012 relative à la protection de l'identité[212] ne fournit pas de définition précise de ce qu'elle protège, objet de sa conception et de sa protection, en précisant uniquement que « *l'identité d'une personne se prouve par tout moyen* »[213]. Les documents administratifs, notamment la carte nationale d'identité ainsi que le passeport, permettant de constater l'état civil d'une personne, comportent, aux termes de ladite loi, les données suivantes : « le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance, le nom dont l'usage est autorisé par la loi, le domicile, la taille et la couleur des yeux, les empreintes digitales ainsi que la photographie de l'individu »[214]. Certains de ces éléments forment, par conséquent, le noyau dur de l'identité d'une personne, à savoir le nom de famille, le sexe, la nationalité ainsi que la filiation, éléments qui contribuent directement à l'individualisation de la personne, sans pour autant être exhaustifs. À cet égard, il est utile de noter que la Cour européenne des droits de l'homme a eu maintes occasions pour affirmer et constater que des éléments comme le sexe, le nom, l'orientation sexuelle ou la vie sexuelle, composant les éléments d'identité de ces documents officiels, constituent des composantes importantes de la sphère personnelle des individus, se rapportant à « un aspect intime de la vie privée », tel qu'il est prévu et protégé par l'article 8 de la Convention[215]. Dans cette perspective, la « singularité » ne paraît pas être *« ici une détermination extrême de l'être, mais la manière dont ses limites s'effrangent ou s'indéterminent : une individualisation paradoxale par indétermination* »[216].

En effet, l'identité d'une personne peut être indirectement reconnue et établie, et ce à l'aide d'autres attributs : ainsi, un individu peut être rattaché à un lieu de résidence, ou à l'endroit où il est susceptible de se retrouver et d'être localisé géographiquement, d'être « géo-localisé ». Cette identification peut aussi s'opérer à travers un numéro, particulièrement le numéro

---

[211] *Cf.* p. 43 et s.

[212] Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, JORF N° 75 du 28 mars 2012.

[213] Loi relative à la protection de l'identité de 2012, Art. 1er : « *L'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier.* »

[214] Loi relative à la protection de l'identité de 2012, Art. 2 : « *La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes : [...]* »

[215] CEDH, Affaire Dudgeon c. Royaume-Uni du 22 octobre 1981, Requête N° 7525/76, § 41 ; Affaire B. c. France du 25 mars 1992, Requête N° 13343/87, § 63 ; Affaire Burghartz c. Suisse du 22 février 1994, Requête N° 16213/90 ; et Affaire Laskey, Jaggard et Brown c. Royaume-Uni du 19 février 1997, Requête N° 21627/93, 21826/93 et 21974/93, § 36.

[216] G. AGAMBEN, *La communauté qui vient*, *Id.*, p. 60.

d'inscription au répertoire national d'identification des personnes physiques (NIR), plus communément connue comme le « numéro de sécurité sociale »[217]. Celui-ci a la capacité d'identifier jusqu'à 10 000 milliards de personnes et est utilisé par la sécurité sociale, mais aussi, par d'autres services de l'administration, ainsi que par des entités privées. L'identité peut également être dévoilée *via* le numéro de téléphone d'une personne ou encore sa date de naissance qui permet, notamment, de déterminer l'âge pour la conclusion d'actes juridiques. Dans ce cadre, tout possesseur d'une carte nationale d'identité ou d'un passeport peut prouver son identité « *à partir des données inscrites sur le document lui-même ou sur le composant électronique sécurisé [...]* »[218].

Parmi tous ces attributs, il semble que le nom de famille soit le plus fondamental à l'égard de l'état civil, caractérisant l'individu de façon permanente et continue. En effet, il doit être connu et utilisé publiquement sous peine de sanctions pénales : ainsi, l'article 433-19 du Code pénal dispose qu'est puni le fait *« de prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil,* [ou] *de changer, altérer ou modifier le nom ou l'accessoire du nom assigné par l'état civil* »[219]. En effet, pour les gouvernements, une singularité déterminée, individualisée et identique, est de loin préférable à une « singularité quelconque », notamment compte tenu du fait que « *quelconque est la figure de la singularité pure. La singularité quelconque n'a pas d'identité, n'est pas déterminée par rapport à un concept, mais elle n'est pas non plus simplement indéterminée ; elle est plutôt déterminée uniquement à travers sa relation à une idée, c'est-à-dire à la totalité de ses possibilités* »[220].

---

[217] Historiquement connu comme le « numéro Carmille » d'après son créateur René Carmille, contrôleur général de l'Armée, pionnier de la mécanographie. Il avait travaillé depuis 1934 sur un numéro de matricule militaire qui se fonde sur la date et le lieu de naissance, et en avait même proposé, en 1938, un modèle à 12 chiffres. En 1940, il reçoit l'ordre de créer un « Service de la démographie », devenu « Service national des statistiques » (SNS) puis récemment l'Insee en 1946, qui était principalement chargé de gérer les soldats démobilisés et les prisonniers de guerre, et reprendre les services de recrutement. Puisqu'il s'agissait d'un projet à finalité civile, le numéro de matricule, ou numéro de code individuel fut alors également attribué aux femmes, d'où l'avènement d'un treizième chiffre, première colonne, permettant de distinguer les hommes (1) et les femmes (2) ; Pour plus de détails, E. BLACK, *IBM and the Holocaust : The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, Washington DC, Dialog Press, Expanded Ed., 2012.

[218] Loi relative à la protection de l'identité de 2012, Art. 6.

[219] Code Pénal, Art. 433-19 : « *Est puni de six mois d'emprisonnement et de 7 500 euros d'amende le fait, dans un acte public ou authentique ou dans un document administratif destiné à l'autorité publique et hors les cas où la réglementation en vigueur autorise à souscrire ces actes ou documents sous un état civil d'emprunt :*
1° De prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil ;
2° De changer, altérer ou modifier le nom ou l'accessoire du nom assigné par l'état civil. » :

[220] G. AGAMBEN, *La communauté qui vient*, *Id.*, p. 68, où l'auteur indique ainsi que « *À travers cette relation, la singularité voisine, comme dit Kant, avec la totalité du possible et reçoit ainsi son omnimoda determinatio, non pas au moyen de la participation à un concept déterminé ou à une certaine propriété actuelle (l'être rouge, français, communiste), mais uniquement grâce à ce voisinage. Elle appartient à un tout, mais sans que cette*

Dans la mesure où le nom intéresse l'État pour le processus d'identification des citoyens, celui-ci s'apparente, dans cette perspective, à une institution de police civile. Le nom participe au processus d'individualisation en permettant à un individu d'être rattaché à une famille, de nouer des relations avec autrui, de se faire reconnaître et de se distinguer des autres individus. Ceci n'implique pas néanmoins la suppression totale de pseudonyme, notamment pour les personnages publics notoires afin de préserver leur tranquillité, évoquant par conséquent le « principe de non-nuisance » formulé par J. S. Mill selon lequel « *la sphère privée est un contexte de liberté inviolable. Le seul aspect de la conduite d'un individu pour lequel il est redevable envers la société, est celui qui concerne les autres. Mais pour ce qui ne concerne que lui, son indépendance est, de droit, absolue* »[221]. Ainsi, une mise en œuvre de ce « principe de non-nuisance » prenant en compte « la nécessité de garantir non seulement la liberté d'action mais aussi la capacité même des individus de se soustraire au regard public », semble instituer la *privacy* comme « le droit d'être laissé tranquille »[222].

Par ailleurs, toute personne dispose d'un « droit au respect de son nom » lui permettant de se défendre à l'occasion d'utilisation irrégulière ou frauduleuse. L'article 434-23 du Code pénal français réprime, à ce titre, l'usurpation du nom d'autrui, « *le fait de prendre le nom d'un tiers* »[223] ainsi que toute « *fausse déclaration relative à l'état civil d'une personne* »[224]. Plus récemment, la loi du 14 mars 2011[225] a instauré le délit d'usurpation d'identité ou d'usage de données permettant d'identifier un individu, délit réprimé désormais par l'article 226-4-1 du Code pénal qui dispose que « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni […]* ». Étant donné que le nom de famille tout comme la nationalité sont des effets de la filiation, le

appartenance puisse être représentée par une condition réelle : l'appartenance, l'être-tel ne sont ici constitués que par la relation à une totalité vide et indéterminée. » (p. 68-69)

[221] A. A. CASILLI, « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *In* Conseil d'État, Étude annuelle 2014 – *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 428.

[222] A. A. CASILLI, « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *Id.*, p. 429.

[223] Code Pénal, Art. 434-23, Al. 1e : « *Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.* ».

[224] Code Pénal, Art. 434-23, Al. 3 : « *Est punie des peines prévues par le premier alinéa la fausse déclaration relative à l'état civil d'une personne, qui a déterminé ou aurait pu déterminer des poursuites pénales contre un tiers.* ».

[225] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

droit considère ces éléments comme étant permanents et les impose à tout individu, sans lui laisser de choix, sous réserve de certaines exceptions.

Cette vision de l'identité représente ainsi une certaine perception du rapport entre l'individu et l'État. C'est dans le but d'affermir l'emprise de l'État-nation, « *seul cadre où l'on puisse dresser des comptes et les seules sources véritables d'initiatives politiques* »[226], sur tout individu, lequel est conçu de façon abstraite. En outre, les éléments d'identité n'étant pas figés, plusieurs autres attributs sont par la suite venus compléter au fur et à mesure la liste de ceux-ci ; en effet, « *en matière d'identification, le recours de plus en plus systématique à la biométrie qui, depuis les attentats du 11 septembre 2001, se dessine dans de nombreux pays, offre de prometteurs chantiers de recherche* »[227].

Toutefois, les attributs de l'identité juridique ne sont pas uniquement ceux imposés par l'État à travers un ensemble de caractéristiques stables suivant la conception de la « mêmeté ». Ils peuvent, de façon partielle et exceptionnelle, être choisis par la personne, ce qui évoque, dans cette perspective, le concept de « l'identité construite », contribuant dès lors à l'ipséité, le propre du Soi. À cet égard, il est utile de noter que la Cour européenne des droits de l'homme a depuis longtemps affirmé que « *le respect de la vie privée exige que chacun puisse établir les détails de son identité d'être humain et que le droit d'un individu à de telles informations est essentiel du fait de leurs incidences sur la formation de la personnalité* »[228].

B. L'identité, un processus d'auto-construction et d'auto-détermination

En se fondant sur une interprétation extensive du droit au respect de la vie privée, le droit pour chacun d'établir et de choisir les détails de son identité d'être humain a été reconnu. Tout comme la notion d'identité, celle de vie privée ou d'intimité privée ne fait l'objet d'aucune définition exhaustive, en des termes stricts et figés[229]. En effet, selon les juges européens, la « vie privée » est un concept étendu et ne peut faire l'objet d'une définition formelle, précisément afin de tenir compte des évolutions sociales et technologiques[230]. Face au concept

---

[226] Z. BAUMAN, *Le coût humain de la mondialisation*, Librairie Arthème Fayard, Coll. Pluriel, 2010, p. 89.
[227] P. PIAZZA, *Histoire de la Carte Nationale d'Identité*, *op. cit.,* p. 379-380.
[228] CEDH, Affaire Gaskin c. Royaume-Uni du 7 juillet 1989, série A n° 160, Requête N° 10454/83, § 39.
[229] CEDH Cour (Chambre), Affaire Costello-Roberts c. Royaume-Uni du 25 mars 1993, Requête N° 13134/87, §36 « *La Cour admet, avec le Gouvernement, que la notion de "vie privée" est large et - elle l'a noté dans son récent arrêt Niemietz c. Allemagne du 16 décembre 1992 (série A no 251-B, p. 11, par. 29) - ne se prête pas à une définition exhaustive. Des mesures adoptées dans le domaine de l'enseignement peuvent, à l'occasion, toucher au droit au respect de la vie privée […].* »
[230] U. KILKELLY, « Le droit au respect de la vie privée et familiale : un guide de mise en œuvre de l'article 8 de la Convention européenne des droits de l'homme », Conseil de l'Europe, Précis sur les droits de l'homme n° 1, mars 2003, p. 9-10.

de « *privacy* » (droit à l'intimité), celui de « vie privée » est plus large et englobe la sphère au sein de laquelle tout individu peut librement construire et développer sa personnalité, s'autodéterminer et s'épanouir. La Cour européenne a ainsi déclaré, en 1992, qu'il n'est ni possible ni nécessaire de chercher à définir de manière précise cette notion tout en affirmant qu' « *il serait toutefois trop restrictif de la limiter à un "cercle intime" où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables* »[231]. Dès lors, la notion de vie privée comprend à la fois celle d'intimité et celle d'autonomie de la personne, conformément à la vision des juges européens.

La vie privée représente un droit fondamental consacré par la Déclaration universelle des droits de l'Homme[232], le Pacte international relatif aux droits civils et politiques[233], la Convention de sauvegarde des droits de l'homme et des libertés fondamentales[234] ainsi que la Charte des droits fondamentaux de l'Union Européenne[235]. En France, ce droit figure principalement à l'article 9 du Code Civil qui dispose que « *chacun a droit au respect de sa vie privée* ». Ce droit à la vie privée est certes absent des Constitutions de 1946 et de 1958, mais le Conseil Constitutionnel, sur le fondement de l'article 2 de la Déclaration des droits de l'homme et du citoyen[236], lui reconnaît une valeur constitutionnelle en affirmant que « *la liberté proclamée par cet article implique le respect de la vie privée* »[237]. De plus, le Conseil fait de la vie privée une composante de la liberté individuelle en déclarant « *que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* »[238].

---

[231] CEDH Cour (Chambre), Affaire Niemietz c. Allemagne du 16 décembre 1992, Requête N° 13710/88, §29.
[232] Déclaration universelle des droits de l'homme du 10 décembre 1948, Art. 12 : « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* »
[233] Pacte international relatif aux droits civils et politiques du 23 mars 1976, Adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale dans sa résolution 2200 A (XXI) du 16 décembre 1966, Art. 17 : « *1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.*
2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »
[234] Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, telle qu'amendée par les Protocoles n° 11 et n° 14, du 4 novembre 1950, Art. 8 – Droit au respect de la vie privée et familiale « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.* »
[235] Charte des droits fondamentaux de l'Union Européenne, 7 décembre 2000 (2000/C 364/01), Art. 7 – Respect de la vie privée et familiale « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.* »
[236] Déclaration des droits de l'homme et du citoyen du 26 août 1789, Art. 2 « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression.* »
[237] Conseil Constitutionnel, Décision N° 99-419 DC du 9 novembre 1999, Cons. 73.
[238] Conseil Constitutionnel, Décision N° 94-352 DC du 18 janvier 1995, Cons. 3.

De manière classique, cette notion correspond « à la sphère secrète de la vie d'où l'individu aura le pouvoir d'écarter les tiers »[239]. C'est donc permettre à toute personne de s'opposer à toute ingérence, immixtion ou intrusion non consentie dans sa sphère intime, un droit de se masquer, d'empêcher toute « divulgation d'informations confidentielles »[240]. Ce droit vaut pour toute personne « *quel que soit son rang, sa naissance, sa fortune, ses fonctions présentes ou à venir* »[241], et ce dans toutes les sphères de la vie sociale. La protection de la vie privée englobe donc l'ensemble des éléments matériels de la vie d'un individu tel que son patrimoine, son domicile ou sa correspondance, ainsi que l'ensemble des éléments immatériels de celle-ci comme son image, son corps ou ses relations avec les autres, assurant par conséquent le processus de construction et d'auto-détermination de l'identité d'une personne.

Par ailleurs, comme l'ont annoncé les juges européens, la notion de vie privée a tendance à évoluer et comprend dernièrement une sphère externe. En effet, le souci de la vie privée évolue, tout comme la notion de l'identité, avec l'évolution des sociétés et de ses structures, il est finalement « *le produit de dynamiques culturelles, politiques et techno-médiatiques de longue haleine, qui se poursuivent dans la société en réseau. Il s'enchâsse dans des univers de pratiques et d'usages quotidiens et reflète la structuration de chacune des forces sociales en présence. […]. Si historiquement l'exigence de la protection de la vie privée a été inégalement ressentie au sein des populations, c'est parce qu'elle est une préoccupation sensible aux hiérarchies et aux formes d'assujettissement propres aux diverses époques* »[242].

Comme il a été proclamé par la Cour strasbourgeoise, l'article 8 de la Convention européenne protège « *un droit à l'identité et à l'épanouissement personnel et celui de nouer et de*

---

[239] J. CARBONNIER, Droit Civil, Vol. 1, Paris, Presses Universitaires de France, 2004, p. 518.

[240] Convention Européenne des droits de l'Homme, Telle qu'amendée par les Protocoles nos 11 et 14, complétée par le Protocole additionnel et les Protocoles nos 4, 6, 7, 12, 13 et 16, du 4 novembre 1950, Art. 10 – Liberté d'expression « *2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire.* »

[241] Cour de Cass., (1ère ch. civile), arrêt du 23 octobre 1990, Pourvoi N° 89-13163, Bulletin 1990 I N° 222, p. 158.

[242] A. A. CASILLI, « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *op. cit.*, p. 429, où l'auteur indique en outre que « *Dans la mesure où les démocraties modernes prônent, du moins nominalement, un espace politique universellement accessible, le souci de la vie privée s'étend. Comme le rappelait Hannah Arendt, la possibilité même d'accéder à la vie active, professionnelle et publique, qui rend nécessaire une ligne de séparation entre ce qui relève de l'accomplissement collectif et ce qui est confinée au particulier à l'intime. Si cette possibilité était initialement circonscrite à une catégorie particulière d'individus, hommes libres et au revenu stable, elle s'élargit aujourd'hui à tous ceux (femmes, enfants, citoyens défavorisés…) dont l'exclusion de la vie publique rendait auparavant inutile de protéger la vie privée.* » (p. 429-430)

développer des relations avec ses semblables et le monde extérieur »[243]. Les juges européens consacrent ainsi un droit à l'identité, un droit à s'autodéterminer, à se découvrir et se développer personnellement, mais aussi un droit d'établir et d'entretenir des rapports avec d'autres humains, au nom du droit au respect de la vie privée[244]. De plus, ils soulignent que « *bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, la Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8* »[245].

Construire et choisir les éléments composant son identité semblent donc correspondre à une tendance qui se justifie par le souci de mettre en adéquation ces différents attributs avec l'identité ressentie, celle personnellement perçue et vécue. Dès lors, la fonction attribuée à l'état civil des personnes se trouve modifiée, contribuant en conséquence à rendre effectif un droit à l'épanouissement personnel, suivant la conception de Ricœur sur l'ipséité. Comme le souligne H. Arendt, « *in acting and speaking, men show who they are, reveal actively their unique personal identities and thus make their appearance in the human world, while their physical identities appear without any activity of their own in the unique shape of the body and sound of the voice. This disclosure of "who" in contradiction to "what" somebody is – his qualities, gifts, talents, and short-comings, which he may display or hide – is implicit in everything somebody says and does. It can be hidden only in complete silence and perfect passivity, but its disclosure can almost never be achieved as a willful purpose, as though one possessed and could dispose of this "who" in the same manner he has and can dispose of his qualities* »[246].
Existe donc, dans ce contexte, un droit de connaître ses origines puisque toute personne se construit et entrevoit son avenir à partir de ses origines. Un accouchement sous X, par exemple, n'est pas sans effet sur la vie privée et l'épanouissement de l'enfant et de son identité. Il en résulte alors que dans la mesure où il est impératif pour une personne de savoir d'où elle vient, elle doit également avoir la possibilité d'écrire et de construire sa propre histoire. C'est dans ce cadre qu'a été, en outre, établi le droit des transsexuels et des transgenres de demander la

[243] CEDH, Affaire Bensaid c. Royaume-Uni du 6 février 2001, Requête N° 44599/98, §47.
[244] Voir CEDH, Affaires Burghartz c. Suisse, du 22 février 1994, N° 16213/90, série A no 280-B, p. 37, § 47 et Friedl c. Autriche, du 31 janvier 1995, N° 15225/89, série A no 305-B, avis de la Commission, p. 20, § 45.
[245] CEDH, Cour (4ème Section), Affaire Pretty c. Royaume-Uni du 29 avril 2002, N° 2346/02, Recueil des arrêts et décisions 2002-III, § 61.
[246] H. ARENDT, *The human condition*, The University of Chicago Press, 2ème Ed., 1998, p. 179.

modification de la mention relative au sexe sur les registres de l'état civil[247], ce qui leur permet d'éviter la révélation d'informations intimes, sensibles, à des tiers et conséquemment d'être marginalisé ou stigmatisé. En ce sens, la Cour de Cassation a eu l'occasion de casser et annuler un arrêt de la Cour d'appel d'Aix-en-Provence puisqu'en « *refusant de tenir compte d'une modification morphologique [...], et d'un changement vrai d'identité sexuelle, affirmé personnellement et reconnu socialement, la cour d'appel n'a pas assuré le respect de la vie privée de l'exposant, et son droit d'établir et d'entretenir des relations avec d'autres êtres humains, notamment dans le domaine affectif, pour le développement et l'accomplissement de sa propre personnalité au sens de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, [...]* »[248].

Dès lors, la notion de vie privée recouvre l'intégrité physique et morale de la personne[249] ainsi que, entre autres, des aspects de son identité physique et sociale[250]. Par conséquent, des éléments tels que « *l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle relèvent de la sphère personnelle protégée par l'article 8* »[251]. Plus encore, les juges européens estiment que « *sur le terrain de l'article 8 de la Convention en particulier, où la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de cette disposition, la sphère personnelle de chaque individu est protégée, y compris le droit pour chacun d'établir les détails de son identité d'être humain* »[252].

C'est donc la reconnaissance pour toute personne d'une capacité à être soi-même, telle qu'elle le ressent et le vit. Dans ce contexte, cette vision étendue des notions d'identité et de vie privée, perçues comme une protection de l'autonomie de l'individu ainsi que son droit à l'autodétermination et d'établir des relations avec des tiers, a des incidences en matière de

---

[247] Cour de Cass. (Ass. Plén.), arrêt du 11 décembre 1992, pourvoi n°91-11900, Bull. civ. 1992, A.P. N° 13, p. 27 : Dans un attendu de principe, les juges annoncent ainsi : « *Attendu que lorsque, à la suite d'un traitement médico-chirurgical, subi dans un but thérapeutique, une personne présentant le syndrome du transsexualisme ne possède plus tous les caractères de son sexe d'origine et a pris une apparence physique la rapprochant de l'autre sexe, auquel correspond son comportement social, le principe du respect dû à la vie privée justifie que son État civil indique désormais le sexe dont elle a l'apparence ; que le principe de l'indisponibilité de l'état des personnes ne fait pas obstacle à une telle modification* ».

[248] Cour de Cass. (Ass. Plén.), arrêt du 11 décembre 1992, *Id.*

[249] CEDH Cour (Ch.), Affaire X et Y c. Pays-Bas du 26 mars 1985, Requête N° 8978/80, série A no 91, p. 11, § 22.

[250] CEDH Cour (1ère Section), Affaire Mikulić c. Croatie du 7 février 2002, Requête N° 53176/99, Recueil des arrêts et décisions 2002-I, § 53.

[251] Voir CEDH, Arrêts B. c. France du 25 mars 1992, série A no 232-C, N° 13343/87, p. 53-54, § 63, Burghartz c. Suisse, *loc. cit.*, série A no 280-B, p. 28, § 24, Dudgeon c. Royaume-Uni, du 22 octobre 1981, série A no 45, N° 7525/76, p. 18-19, § 41, et Laskey, Jaggard et Brown, du 19 février 1997, N° 21627/93 et autres, p. 131, § 36.

[252] CEDH, Cour (Grande Chambre), Affaire Christine Goodwin c. Royaume-Uni du 11 juillet 2002, N° 28957/95, Recueil des arrêts et décisions 2002-VI, § 90.

l'indisponibilité de l'état-civil des sujets (nom, sexe) et de protection des rapports affectifs et sociaux.

Finalement, il s'avère qu'en admettant le processus de construction et d'auto-détermination de l'identité, celle-ci s'étend pour comprendre une multitude d'attributs autres que ceux présents dans l'état-civil tel que déterminé par l'État pour les besoins d'identification, tout en contribuant à l'individualisation des personnes. Comme le précise le Professeur Lessig, « *by "identity", I mean something more than just who you are. I mean as well your "attributes", or more broadly, all the facts about you that are true. Your identity, in this sense, includes your name, your sex, where you live, what your education is, your driver's license number, your social security number, your purchases [...], whether you're a lawyer – and so on. These attributes are known by others when they are communicated. In real space, some are communicated automatically: for most, sex, skin color, height, age range, and whether you have a good smile get transmitted automatically. Other attributes can't be known unless they are revealed either by you, or by someone else: your GPA in high school, your favorite color, your social security number, your last purchases [...], whether you've passed a bar exam* »[253].

Ce rôle accordé à l'autonomie et à la volonté individuelle dans la sélection des détails composants et révélant l'identité est cependant relativisé avec l'essor des nouvelles technologies numériques qui s'inscrivent, en particulier, dans une optique de transparence. En effet, l'accroissement progressif des différents domaines de la vie devenus connectés au réseau numérique soulèvent de nombreuses questions concernant les notions d'identité et de vie privée, remettant en cause leurs conceptions et leurs perceptions. Plus particulièrement, compte tenu du fait qu'elles maîtrisent une quantité massive de données personnelles, les grandes entreprises du web, nommées les GAFAM en référence à Google, Apple, Facebook, Amazon et Microsoft, ont, de nos jours, une emprise étendue sur les vies privées et la construction des identités des individus, dont les États et les sociétés civiles ne peuvent se désintéresser[254]. Autrement dit, reprenant les propos de Dubar, « *l'ancien modèle a été ébranlé mais y en a-t-il un nouveau ? Manifestement pas. Ce qui se dessine c'est une pluralité de modes de vie, de conceptions, de configurations c'est-à-dire de combinaisons inédites de formes identitaires [...]* »[255].

---

[253] L. LESSIG, *Code – Version 2.0*, Ed. Basic Books, New York, 2006, p. 39-40.

[254] Audition de M. Côme Berbain, conseiller chargé de la transformation numérique de l'État et de la sécurité numérique, Rapport N° 592 fait au nom de la Commission des Lois Constitutionnelles, de la législation et de l'administration générale de la République sur le Projet de loi relatif à la Protection des données personnelles (n°490) par Mme. Paula Forteza, Enregistré à la Présidence de l'Assemblée nationale le 25 janvier 2018.

[255] C. DUBAR, *La Crise des identités, op. cit.*, p. 93 ; et l'auteur rajoute que « *L'une des raisons majeures de la crise identitaire est sans doute qu'alors que les rôles familiaux sont remis en cause, plus ou moins radicalement, les identités intimes « réflexives », ne sont pas légitimées et manquent de ressources (langagières, et plus*

En effet, la révolution numérique change la donne en ce sens que la protection de l'autonomie dans la construction et la détermination de l'identité, au titre du droit au respect de la vie privée, paraît insuffisante compte tenu du fait qu'une nouvelle forme d'influence subtile voit le jour affectant et façonnant les choix et les actions des individus. Plus précisément, « *we have already seen that autonomy is curtailed when we are limited in our capacity to ground our actions and decisions on beliefs, desires, and goals with which we fully identify* », or, indique H. Nissenbaum, avec l'émergence de l'ère du numérique et des nouvelles technologies de l'information et de la communication, « *the manipulation that deprives us of autonomy is more subtle than the world in which lifestyle choices are punished and explicitly blocked. […]. If, as a result of these manipulations, people choose jobs, banks, or products not primarily because they comply with our own values, but because they have been kept in the dark about more relevant options, they are victims of a form of deception or coercion, even subtler than that of the conman or blackmailer. According to Dworkin, being deceived or simply kept in the dark has implications for autonomy: "both coercion and deception infringe upon the voluntary character of the agent's actions. In both cases a person will feel used, will see herself as an instrument of another's will"* »[256]. Émerge ainsi à l'occasion de cette nouvelle période que constitue le numérique et les nouvelles technologies, une nouvelle approche de l'identité, celle de l'identité numérique.

Section 2 – Le concept d'identité numérique : une notion dynamique

Ce concept d'identité numérique s'est bâti graduellement, de façon dynamique, suivant l'évolution et les avancées informatiques et juridiques, à travers, d'une part, une conception personnaliste de la notion de donnée personnelle (§1), et, d'autre part, la révolution numérique et les avancées technologiques manifestées (§2), qui ont eu, de manière simultanée et complémentaire, un rôle fondamental dans sa mise en œuvre.

largement subjectives) pour pouvoir s'exprimer et se reconnaître. De même, alors que les identités « culturelles », généalogiques, se brouillent, les identifications narratives, les projets de vie sont plus que jamais incertains, […]. » (Note de bas de p. n°1)

[256] H. NISSENBAUM, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, p. 82-83.

§1. Le rôle de la conception personnaliste de la notion de donnée personnelle

Une conception personnaliste de la notion de donnée personnelle a eu un impact et a joué un rôle non négligeable dans la conceptualisation de l'identité numérique, un rôle qui se traduit par le lien irréductible qui existe désormais entre les notions de « vie privée » et de « donnée personnelle » (A), mais aussi par l'adoption progressive d'une conception large de la notion de « données à caractère personnel » (B).

A. Le lien irréductible entre vie privée et donnée personnelle

Avec l'avènement d'internet et des nouvelles technologies, un lien irréductible commence à se tisser entre l'informatique, l'intimité, la vie privée d'un individu ainsi que ses libertés individuelles, dont sa liberté nouvelle d'exploiter l'informatique qui génère des données : « *il faut donc garantir la liberté des citoyens et la liberté nouvelle de l'informatique, l'une par l'autre, par un système de réciprocité. La liberté des citoyens est garantie par un pouvoir concret, leur droit à l'information et leur pouvoir d'accès aux données qui les concernent personnellement* »[257]. Les nouvelles pratiques numériques conçoivent, pour leur part, le traitement des données personnelles sans prendre en compte la problématique de la vie privée, comme si le traitement effectué ne constituait pas une menace pour l'intimité et la vie privée de la personne – objet du traitement.

À la lumière de la jurisprudence de la Cour européenne, la protection des données personnelles s'est progressivement imposée comme une composante du droit à la vie privée. En adoptant une interprétation large de la notion de vie privée, tel qu'il a été précédemment vu, et en se fondant sur l'article 8 de la Convention, à défaut d'avoir un article protégeant les données personnelles en particulier, la Cour fait découler la protection et le traitement des données personnelles du droit à la vie privée. Ce qui lui a permis d'affirmer, à l'occasion d'une affaire en 2008, que les « *catégories d'informations personnelles conservées par les autorités […], à savoir des empreintes digitales, des profils ADN et des échantillons cellulaires, constituent toutes des données à caractère personnel […] car elles se rapportent à des individus identifiés ou identifiables* »[258] et font donc parties des attributs de leurs identités.

L'ère de la révolution numérique a provoqué l'extension du droit à la vie privée engendrant deux droits autonomes : le droit au respect de la vie privée et le droit à la protection des données

[257] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, JO Année 1977-1978 – N° 79 A.N., 5 octobre 1977, p. 5782.
[258] CEDH, Cour (Grande Chambre), Affaire S. et Marper c. Royaume-Uni du 4 décembre 2008, Requête N° 30562/04 et 30566/04, Recueil des arrêts et décisions 2008, §68.

à caractère personnel ; les deux étant certes autonomes, distingués théoriquement l'un de l'autre, mais se retrouvent en interdépendance et en interaction continue. La Charte des droits fondamentaux leurs consacrent deux articles distincts : l'un relatif au respect de la vie privée[259] et l'autre à la protection des données à caractère personnel[260]. Selon une jurisprudence constante de la Cour de Justice de l'Union, ces droits fondamentaux « *font partie intégrante des principes généraux du droit dont la Cour assure le respect* »[261]. En outre, elle rajoute que « *les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux [...]* »[262]. Ce sont donc des droits fondamentaux interconnectés qui sont garantis et protégés par les législations et les institutions juridiques en Europe.

En dépit des apparences observées et des pratiques numériques actuelles, la plupart des utilisateurs du web continuent à être attachés au respect de leurs vies privées. Il est vrai que l'exposition accrue de soi ne désigne pas une volonté moindre de contrôle des informations divulguées, ni de la grandeur du public auprès duquel elles sont visibles. De plus en plus, les réseaux sociaux, espace principal de partage d'éléments de la vie privée, n'inspirent plus confiance. Ces réseaux représentent d'ailleurs les acteurs numériques qui inspirent le moins de confiance chez les français en ce qui concerne la protection de leurs informations personnelles. En effet, il existe un paradoxe entre l'usage et la confiance puisque, selon une enquête menée fin 2017, seuls 40% des français ont confiance dans le numérique malgré un usage important qui s'élève à 80%[263]. D'après les législateurs de 1977, « *l'informatique, a-t-on dit, présente des dangers pour la liberté, des dangers beaucoup plus grands que les anciens fichiers manuels ou*

[259] Charte des droits fondamentaux de l'UE du 7 décembre 2000, Art. 7 – Respect de la vie privée et familiale.
[260] Charte des droits fondamentaux de l'UE, Art. 8 – Protection des données à caractère personnel : « *1. Toute personne a droit à la protection des données à caractère personnel la concernant.*
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »
[261] CJCE, Arrêt Bernard Connolly c. Commission des Communautés européennes, du 6 mars 2001, n° C-274/99, Recueil de jurisprudence 2001, p. I-01611, point 37.
[262] CJCE, Arrêt de la Cour, Österreichischer Rundfunk et autres, du 20 mai 2003, nos C-465/00, C-138/01 et C-139/01, Recueil de jurisprudence 2003 p. I-04989, point 68.
[263] Harris-Interactive, Baromètre 2017 « La confiance des Français dans le numérique », 6ème vague, 18 décembre 2017 : http://harris-interactive.fr/opinion_polls/barometre-la-confiance-des-francais-dans-le-numerique-6e-vague/

mécanographiques. Il est des cas, en effet, dans lesquels la différence de degré se transforme en différence de nature »[264]. L'informatique devrait donc être au service de chaque citoyen[265].

Depuis 1978, la loi « Informatique et Libertés » régit le traitement des données personnelles afin que celui-ci ne porte atteinte « *ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* »[266]. Néanmoins, malgré toutes les garanties offertes par les rédacteurs de ladite loi, la vie privée restait principalement conçue comme un espace fermé, assez délimité, devant être particulièrement protégée contre les intrusions des autorités publiques. Les ingérences des entités privées n'étaient pas une problématique en cause lors de la conception de cette loi alors même que le président de la commission, rapporteur du projet de loi annonçait, dès cette époque, qu'en « *renforçant les moyens pour l'État — et pour bien d'autres que l'État, peut-être plus dangereux que ce dernier — de suivre et de confronter les diverses activités humaines, l'informatique agit dans le sens de l'efficacité technique ; elle n'agit pas toujours dans celui de la liberté* »[267]. La loi de 1978 ne pouvait bien évidemment pas anticiper les nouvelles extensions de la notion de vie privée, notamment en termes de droit à l'autonomie personnelle et de liberté d'établir et d'entretenir des relations avec ses semblables, qui tendent de nos jours à s'élargir de plus en plus tout en sollicitant un nouveau type de protection sur le web. La loi portait en son sein une sorte de pacte social prévoyant le contrôle de l'État en échange du respect de la vie privée.

Or aujourd'hui, indique E. Peres, « *les technologies sont telles qu'elles ont vite fait de remettre en cause cet équilibre en s'immisçant dans notre sphère intime via le prélèvement et la collecte des données personnelles* »[268]. L'objectif de la loi de 1978 était principalement d'éviter une informatisation incontrôlée des administrations publiques pouvant entraîner des atteintes à la vie privée et à la liberté individuelle des individus, et visait ainsi à rassurer l'opinion générale. Tout ordinateur a une mémoire, et à la différence de celles des êtres humains, la mémoire informatique n'a pas la faculté d'oublier. En effet, un ordinateur a la capacité de sélectionner et de trier en l'espace de quelques instants des données dont le recensement aurait demandé des heures, des jours voire des mois à un homme. Dans ce contexte, il s'avère que « *par des*

[264] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *Id.*, p. 5782.
[265] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés – Art. 1.
[266] Loi Informatique et Libertés, Art.1.
[267] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Id.*, p. 5782.
[268] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.*, p. 46.

interconnexions entre ordinateurs, il devient possible de rassembler sur une question ou sur une personne une moisson énorme d'informations »[269].

Les problèmes de l'informatique dans ses rapports avec les libertés ont commencé en France, suite à la demande en 1973 du Ministère de l'Intérieur de bâtir un fichier informatisé *« dénommé fort maladroitement, et comme une provocation, projet Safari dont il a été-dit, naturellement, qu'il constituait une chasse à l'homme* »[270]. Ce système automatisé pour les fichiers administratifs et le répertoire des individus (SAFARI) avait pour but de créer une base de données centralisée en se fondant, spécifiquement, sur le numéro de sécurité sociale comme identifiant commun à tous les fichiers administratifs. Il a été par conséquent baptisé l' « identifiant unique » par les informaticiens de l'époque. Ce projet d'instaurer des fichiers interconnectés à l'aide du numéro Insee a entraîné de vives réactions et débats à la suite de sa révélation par le journal Le monde en 1974. Ce système a été qualifié de « *mauvais calembour qui désigne à la fois un sigle barbare - [...] - et un mot du vocabulaire moderne qui donne à penser que l'on s'apprête à chasser le pauvre citoyen comme une bête traquée* »[271]. Le projet a donc été retiré et une Commission dite « informatique et liberté » a été instaurée, chargée de proposer une réglementation des usages et des moyens informatiques, notamment « *des mesures tendant à garantir que le développement de l'informatique dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques* »[272].

Déjà à l'époque, les députés ont fait perception de modernité en affirmant subtilement qu'il faut limiter strictement les traitements informatiques pour exclure totalement la possibilité de voir les personnes transformées en simples numéros. C'était là l'aspiration principale du projet de loi de 1978 : « *concilier la protection des libertés avec cette liberté nouvelle que représente le recours à l'informatique* »[273]. Le gouvernement français s'est depuis longtemps penché sur les questions de respect et de protection de la vie privée mais aussi des libertés, d'où plusieurs législations en la matière qui en ont découlé : la loi de 1970 renforçant la garantie des droits individuels et dont la troisième partie est particulièrement consacrée à la protection de la vie

[269] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Id.*, p. 5782.
[270] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Id.*, p. 5783.
[271] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Ibid.*, p. 5789.
[272] Demande du Gouvernement en 1974 vis-à-vis d'une Commission dites « Informatique et libertés » placée sous la présidence de M. Chenot, vice-président du Conseil d'État de l'époque : Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Ibid.*, p. 5783.
[273] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Ibidem*, p. 5788, et Rapport N° 199 de M. Jacques Thyraud sur le projet de loi relatif à l'informatique et aux libertés déposé le 19 décembre 1977, Sénat ; Disponible en ligne : https://www.senat.fr/rap/l77-199/l77-199.html

privée[274] ; le décret de 1977[275] ainsi que la loi de 1978 précitée visant à améliorer les relations entre l'administration et le public[276] en ouvrant l'accès à certains documents administratifs, ou encore les diverses lois sur le secret professionnel[277]. Toutes ces mesures ont pour objectif principal de promouvoir une société libre et ouverte. Depuis cette période, les risques constitués par l'utilisation informatique de données personnelles, nominatives, « *c'est-à-dire qui visent un individu ou un groupement* »[278], étaient donc remarquablement envisagées.

L'idée qu'une société juste est une société qui est fondée sur la liberté des citoyens est bien répandue depuis Rousseau. Ce dernier affirme que « *renoncer à sa liberté, c'est renoncer à sa qualité d'homme, aux droits de l'humanité, même à ses devoirs* »[279]. Dans cette perspective, *l'homo numericus* se retrouve face à plusieurs droits distincts mais interconnectés, dont certains peuvent éventuellement porter atteinte à d'autres : le droit à son intimité et à sa vie privée, le droit à la protection de ses données face à sa liberté de se développer, d'être soi-même et de partager, y compris sur les réseaux numériques, par exemple. Comme l'a si bien formulé A. Peyrefitte, « *on ne s'occupe jamais trop de la liberté. La liberté est toujours un sujet neuf. La liberté est toujours fragile* »[280]. Elle constitue le moteur d'une société et le fondement de la démocratie. La liberté, comme l'ont également souligné les juridictions européennes (CEDH et CJCE), implique que tout individu vit la liberté qu'il ressent au fond de lui-même, la capacité à être soi et à se construire et s'épanouir librement ; ce qui inclut, en outre, les libertés accordées à l'heure actuelle par les outils et les moyens informatiques. Or, indiquent, à ce titre, les anciens

---

[274] Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

[275] Décret du 11 février 1977 mettant en place une « Commission chargée de favoriser la communication au public des documents administratifs » : voir A. de Laubadère, A.J.D.A., 1977, p. 204.

[276] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal ; la plupart de ses dispositions ont été depuis abrogées.

[277] Loi 1810-02-19 promulguée le 1er mars 1810 ; Loi n° 56-1327 du 29 décembre 1956 de finances pour 1957 ; Ordonnance n° 58-1298 du 23 décembre 1958 modifiant notamment certains articles du code pénal ; Loi n° 77-1468 du 30 décembre 1977 instaurant la gratuité des actes de justice devant les juridictions civiles et administratives.

[278] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Id.*, p. 5788 et A. Peyrefitte rajoute plus loin : « *En effet, une des révélations qu'apporte le rapport de la commission Chenot-Tricot, c'est que certaines administrations avaient développé des systèmes informatiques sans même que leur ministre en fût au courant. La création des fichiers se déroulait dans un certain désordre juridique. Certains fichiers étaient créés par la loi, d'autres par décrets, d'autres encore, sans aucun acte juridique, par des initiatives spontanées de services administratifs obéissant, en quelque sorte, à leur propre impulsion.* »

[279] J.-J. ROUSSEAU, *Du Contrat social ou Principes du droit politique*, Livre I, Chapitre IV : "De l'esclavage", Amsterdam, Chez Marc Michel Rey (1762), Ed. Félix Alcan, 1896, p. 21, où l'auteur rajoute qu' « *il n'y a nul dédommagement possible pour quiconque renonce à tout. Une telle renonciation est incompatible avec la nature de l'homme ; et c'est ôter toute moralité à ses actions que d'ôter toute liberté à sa volonté.* » ; disponible en ligne : https://gallica.bnf.fr/ark:/12148/bpt6k61325137/f2.item.r=renoncer

[280] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Id.*, p. 5787, et M. A. Peyrefitte rajoute « *Une société libre, qu'est-ce que cela signifie ? Cela signifie que la liberté n'est pas un cadeau de luxe que la société ferait à ses citoyens quand tout va bien. La liberté est ce sans quoi les mécanismes mêmes de la société ne pourraient plus fonctionner. Elle est le moteur de notre société.* »

députés, « *la liberté demande un certain respect de l'intimité de la personne. Un homme n'est plus vraiment libre s'il est transparent à autrui, si son for intérieur devient une sorte de forum public qui serait ouvert à toutes les curiosités* »[281]. L'usage actuel du numérique semble pourtant tendre vers la création d'un forum public où les données, permettant de reconnaître et de cibler les personnes, directement identifiées ou identifiables, sont collectées et traitées en masse, comme il sera vu plus loin.

Pour renforcer la dimension de l'individu-acteur dans le droit à la protection des données, il faudrait envisager celui-ci comme englobant un droit à « l'autodétermination informationnelle » (« *Informationelle Selbstbestimmung* »). Ce droit, dégagé par la Cour Constitutionnelle allemande en 1983[282] sur le fondement des articles 1 (dignité de l'homme) et 2 (droit au libre développement de la personnalité et à la liberté d'agir) de la Loi fondamentale[283], constitue un droit attaché à la personne qui tend à *« garantir en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* »[284]. Dans ce cadre, ce droit ne doit pas être perçu comme un droit supplémentaire qui vient s'ajouter aux droits, tels que les droits à l'information, les droits d'accès ou d'opposition, mais plutôt, précise le Conseil d'État, « *comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et devant être interprétés et mis en œuvre à la lumière de cette finalité* »[285].

---

[281] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Ibid.*, p. 5787.
[282] Cour Constitutionnelle fédérale de l'Allemagne, arrêt du 13 décembre 1983 relatif à la loi de Recensement : BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats Vom 15 Dezember 1983 auf die mündliche Verhandlung Vom 18 und 19 Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden.
[283] Loi fondamentale pour la République fédérale d'Allemagne du 23 mai 1949 – Art. 1 [Dignité de l'être humain, caractère obligatoire des droits fondamentaux pour la puissance publique] « *(1) La dignité de l'être humain est intangible. Tous les pouvoirs publics ont l'obligation de la respecter et de la protéger.*
(2) En conséquence, le peuple allemand reconnait à l'être humain des droits inviolables et inaliénables comme fondement de toute communauté humaine, de la paix et de la justice dans le monde.
(3) Les droits fondamentaux énoncés ci-après lient les pouvoirs législatif, exécutif et judiciaire à titre de droit directement applicable ».
Art. 2 [Liberté d'agir, liberté de la personne] « *(1) Chacun a droit au libre épanouissement de sa personnalité pourvu qu'il ne viole pas les droits d'autrui ni n'enfreigne l'ordre constitutionnel ou la loi morale.*
(2) Chacun a droit à la vie et à l'intégrité physique. La liberté de la personne est inviolable. Des atteintes ne peuvent être apportées à ces droits qu'en vertu d'une loi », Traduction en français par C. Autexier, M. Fromont, C. Grewe & O. Jouanjan, novembre 2012, Partie I. Les droits fondamentaux, p. 18.
[284] Trad. en français de Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *In État de droit et virtualité*, K. Benyekhlef & P. Trudel (dir.), Montréal, Ed. Thémis, 2009, p. 159.
[285] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, La documentation française, Les rapports du Conseil d'État n° 65, adopté le 17 juillet 2014, p. 26.

Ce droit à l'autodétermination informationnelle comporte, également, le droit de partager et d'exposer ses données publiquement ou d'en restreindre le partage et l'exposition. C'est un pouvoir accordé à l'individu de choisir et de décider quand et comment une information qui relève de sa vie privée peut être communiquée à un tiers. Conséquemment, c'est le droit à l'autonomie personnelle, le droit de demeurer libre de conduire sa propre existence dans une société où le numérique a de plus en plus une place prépondérante ; ce qui équivaut, en ce sens, à une consécration numérique de ce droit. Ainsi, en s'inspirant de la démarche entreprise par la Cour constitutionnelle allemande, le droit à la protection des données personnelles se fonde sur le principe de la dignité humaine et celui du respect dû à l'autodétermination informationnelle, droit également envisagé et vivement recommandé par le Conseil d'État qui précise : « *alors que le droit à la protection des données peut être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif : il ne s'agit plus seulement de protéger le droit au respect de la vie privée mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté. En ce sens, le droit à l'autodétermination répond davantage à l'aspiration croissante des individus à l'autonomie de la décision* »[286].

Cette aspiration qui tend vers un contrôle des données est celle que leur patrimonialisation et le droit de propriété essaient de saisir à l'heure actuelle. Toutefois, les notions d'autonomie informationnelle et d'autonomie personnelle apporteraient une réponse plus efficace, plus concrète et plus respectueuse de la logique qui a toujours prévalu en Europe vis-à-vis de la protection des données : une logique personnaliste et non patrimoniale. En se référant au droit de propriété qui prétend accorder aux individus un meilleur moyen de gérer leurs patrimoines – constitués de leurs données personnelles, il y'a par ailleurs le risque de marchandisation des données. Quant au droit à l'autodétermination, celui-ci suggère que tout individu doit rester en mesure de décider librement de son existence ; « *l'un se situe sur le plan de l'avoir, l'autre sur celui de l'être* »[287]. Le droit d'un individu sur ses données relève donc des droits de la personnalité et non du droit de propriété. À cet égard, la CNCDH, qui se fonde sur le postulat « *selon lequel les données produites et communiquées par une personne lors de son utilisation des outils numériques constituent le prolongement de cette personne* »[288], critique avec sévérité toute patrimonialisation des données personnelles, même au nom d'une vie privée active.

[286] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, Id.,* p. 267-268.
[287] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *Id.,* p. 268.
[288] CNCDH, *Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique*, Texte n° 63, JORF n° 0126 du 3 juin 2018, p. 3, point 7.

De plus, la Commission considère que le droit au respect de la vie privée dans l'espace numérique désigne un droit positif à l'autonomie personnelle et au développement de la personne et, précise qu' « *à travers la maîtrise de ses données personnelles, l'homo numericus doit conserver sa "capacité à être lui-même" : sa vie privée ne doit pas être façonnée par un traitement incontrôlé de ses données aboutissant à un profilage limitant le droit à son développement personnel* »[289]. La CNCDH soutient également la consécration en droit français du droit à l'autodétermination informationnelle, tel que reconnu par le Conseil d'État, et affirme qu'il fait pleinement partie des droits de la personnalité. Ce principe d'autonomie est, à l'heure actuelle, timidement consacré par l'article 54 de la loi pour une République numérique qui affirme que « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, [...]*. »[290].

En effet, « *le traçage par les réseaux, la biométrie, la géolocalisation, les nanotechnologies, la vidéosurveillance participent d'une mise en visibilité publique d'informations qui relèvent du domaine privé. Cette évolution technologique conduit à replacer la protection de la vie privée au cœur des réflexions de la défense des libertés à l'ère du numérique* »[291].

B. Le concept large de « données à caractère personnel »

Les législations relatives à la protection des données personnelles, ainsi que les juridictions, définissent largement le concept de « données à caractère personnel ». Celle qui figure dans la loi de 1978 précise que « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* »[292]. La Convention 108 pour la protection des données personnelles inclut une définition courte mais identique[293] et l'ancienne directive

[289] CNCDH, *Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique*, *Id.,* p. 5-6, point 18.
[290] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, Chapitre II : Protection de la vie privée en ligne, Section I : Protection des données personnelles, Art. 54 modifiant l'article 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 0235 du 8 octobre 2016.
[291] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *Id.,* p. 47.
[292] Loi Informatique et Libertés, Art. 2 al. 2 (modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel)
[293] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – STE n° 108 du Conseil de l'Europe – Convention 108, du 28 janvier 1981, Art. 2, point a) –

européenne relative à la protection des données de 1995 comprend également la même définition large des données à caractère personnel[294]. De même, le nouveau Règlement sur la protection des données, dit RGPD, définit les données à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »[295]. Cela reflète bien la volonté des législateurs européens de définir le concept de données personnelle de manière large, volonté qui s'est manifestée tout au long des divers processus législatifs, des plus anciens aux plus récents. Ainsi, la Commission des Communautés européennes indiquait dans sa proposition initiale que « *comme dans la Convention 108, une définition large est adoptée afin de couvrir toutes les informations qui peuvent être reliées à une personne* »[296]. Sa proposition modifiée donna également satisfaction à l'objectif du Parlement qui est celle « *d'adopter la définition la plus globale possible de la notion de « donnée à caractère personnel », afin de couvrir toutes les informations qui peuvent être reliées à une personne physique* »[297].

Définitions « *« données à caractère personnel » signifie : toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ;* »

[294] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée depuis le 24/05/2018, Art. 2, point a) – Définitions « *a) « Données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*; ».

[295] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données – RGPD, Art. 4, point 1) – Définitions, p. 33.

[296] Commission des Communautés européennes, "Commission Communication on the protection of Individuals in relation to the processing of personal data in the Community and Information security", COM(90) 314 final ~ SYN 287 and 288, Bruxelles, 13 Septembre 1990, p. 19: Commentaire sur l'article 2 "*As in Convention 108, a broad definition is adopted in ardor to cover all Information which may be linked to an Individual. Depending on the use to which it is put, any item of data relating to an Individual, harmless though it may seem, may be sensitive (e.g. a mere postal address). In order to avoid a situation in which means of Indirect Identification make it possible to circumvent this definition, it is stated that an Identifiable Individual is an Individual who can be identified by reference to a number or a similar identifying particular.*"

[297] Commission des Communautés européennes, "Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", COM(92) 422 final - SYN 287, 15 octobre 1992, p. 9: Commentaire relatif à l'article 2 *"'"Personal data". The amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual (amendment No 12).*"

Les règles contenues dans ces textes visent donc à protéger autant que possible les personnes physiques. Leurs dispositions soulignent clairement que la finalité principale de ces règles est la protection des libertés et des droits fondamentaux des individus, notamment leurs vies privées, à l'égard des traitements de leurs données à caractère personnel[298]. À cet égard, le groupe de travail européen « Article 29 » sur la protection des données (G29) rappelle que « *la promulgation des premières lois sur la protection des données dans les années 70 est due aux nouvelles technologies de traitement électronique des données, qui permettaient un accès plus facile et plus étendu aux données à caractère personnel que les formes traditionnelles de traitement des données* »[299]. Il souligne la nécessité d'adopter une définition qui soit large afin d'anticiper les évolutions et d'incorporer toutes les « zones d'ombre » dans son champ d'application. De toutes les définitions susvisées de la notion de donnée à caractère personnel, il ressort principalement quatre éléments constitutifs interdépendants, quoiqu'étroitement liés. La donnée en soi n'est certes qu'un matériel brut, mais qui évoque « *une information numérique ou alphanumérique, codée, lisible par la seule machine, en vue de son enregistrement, traitement, conservation et communication* »[300].

Le choix de l'expression « toute information » sous-tend une interprétation large et est porteur de nombreuses conceptions. En ce qui concerne la nature de l'information, la notion de données personnelles semble ainsi englober toutes sortes de renseignements relatives à une personne. Ces informations peuvent être objectives, le groupe sanguin de l'individu concerné par exemple, tout comme elles peuvent être subjectives, telles que des avis ou des appréciations. Les informations subjectives constituent une grande partie des traitements de données à caractère personnel comme celui effectué par les banques, indique le G29, et ce « *pour l'évaluation de la fiabilité des emprunteurs (« X est un emprunteur fiable »), des assurances (« X ne devrait pas mourir dans un proche avenir ») ou de l'emploi (« X est un bon travailleur et mérite d'être promu »)* »[301]. Ces informations n'ont pas besoin d'être vraies ou prouvées pour être considérées comme des données à caractère personnel et peuvent être récoltées ou partagées par de nombreuses entités. Les droits d'accès, de rectification ou encore d'opposition

[298] Par ex., les articles 1er des directives 95/46/CE précitée et 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) qui précisent, l'une et l'autre, que les États membres doivent prendre les dispositions nécessaires « *pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel* ».

[299] Groupe de travail « Article 29 » sur la protection des données – G29, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, 01248/07/FR WP 136, p. 5 ; Disponible en ligne : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp136_fr.pdf

[300] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 9.

[301] G29, Avis 4/2007 sur le concept de données à caractère personnel, *Id.*, p. 7.

semblent effectivement prévoir ces hypothèses, il n'empêche que les informations restent de nature personnelle.

Quant au contenu de l'information, celui-ci se réfère à toute sorte d'information relevant de la vie privée et familiale d'une personne physique, quelle que soit sa situation, qualité ou statut, celles relatives à ses activités, à ses relations de travail, à son comportement économique et social, à son comportement sur les réseaux sociaux tout comme celles relatives à sa santé ou à sa sexualité ou encore à sa vie sexuelle. Cette interprétation coïncide avec la jurisprudence européenne prévoyant une conception large de la notion de vie privée et familiale[302] mais aussi, de façon équivalente, avec les législations en matière de protection des données ayant une conception également large, quant à la protection et à la définition de leur objet, englobant ainsi le respect de la vie privée, parmi d'autres droits et libertés. Comme il a été précédemment vu, la Charte des droits fondamentaux consacre deux droits autonomes : le droit au respect de la vie privée à son article 7 et le droit à la protection des données à caractère personnel à son article 8. Cette consécration respecte les dispositions des articles 1er de la directive de 1995 et du RGPD qui visent à assurer la protection des droits et libertés fondamentaux, et notamment la protection des données à caractère personnel dans n'importe quel contexte, tel que celui du travail, des condamnations pénales, des sanctions et jugements[303]. Cette notion « *comprend assurément le nom d'une personne joint à ses coordonnées téléphoniques ou à des informations relatives à ses conditions de travail ou à ses passe-temps* » précise la Cour de justice[304].

Quant au format ou au support utilisé pour les informations, le concept des données à caractère personnel comprend toute information disponible sous n'importe quelle forme, qu'elle soit alphabétique, numérique, graphique, acoustique, photographique ou visuelle. Celles-ci peuvent

---

[302] CEDH (Grande ch.), Affaire Amann *c.* Suisse du 16 février 2000, requête N° 27798/95, Recueil des arrêts et décisions 2000-II, point 65 « *À cet égard, elle souligne que le terme « vie privée » ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables ; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de « vie privée » (arrêts Niemietz §29 et Halford §42, précités).Cette interprétation extensive concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, entrée en vigueur le 1er octobre 1985, dont le but est « de garantir, sur le territoire de chaque Partie, à toute personne physique (…) le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1), ces dernières étant définies comme « toute information concernant une personne physique identifiée ou identifiable » (article 2).* »

[303] Directive 95/46/CE, Art. 1 « *Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.* » & RGPD, Art. 1 « *Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.* »

[304] CJCE, Affaire C-101/01 Lindqvist, du 6 novembre 2003, Recueil des arrêts et décisions 2003-I, p. 13008, point 24.

être conservées sur papier, sur un registre, stockées dans un cookie ou une application, sur un échantillon biologique, ou encore sur des étiquettes d'identification par radiofréquence[305]. L'objectif est donc d'englober tout type de données personnelles collectées et traitées, objectif également présent dans l'ancienne directive sur la protection des données qui soulignait, entres autres, que « *compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, [...]* »[306], ses dispositions s'appliquaient à tout traitement portant sur celles-ci. De plus, pour qualifier ces renseignements de données à caractère personnel, il n'est pas nécessaire qu'ils soient conservés dans une base de données ou dans un fichier structuré. Des informations sous forme de texte libre présentes dans un document électronique peuvent être considérées comme des données à caractère personnel, à l'image des courriels électroniques. Dans cette perspective, les données biométriques, qui sont des « *données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique* »[307], méritent d'être citées. Précisément, ces données sont « *par nature particulièrement sensibles du point de vue des libertés et des droits fondamentaux [...]* »[308] puisqu'elles correspondent à des caractéristiques biologiques, physiologiques, vivantes, à des actions qui peuvent être reproduites quand ces actions et/ou ces caractéristiques sont propres à la personne physique et mesurable à la fois, et ce « *même si les méthodes utilisées dans la pratique pour les mesurer techniquement impliquent un certain degré de probabilité* »[309]. Par conséquent, les images faciales, la structure faciale, les empreintes digitales, la structure de la rétine, les données dactyloscopiques, la voix ou encore la forme de la main constituent des exemples de données biométriques, portant et révélant aussi les caractéristiques comportementales ou celles profondément ancrées chez une personne, telles que la signature manuscrite, la démarche particulière, le langage choisi ou même la dynamique de frappe sur le clavier. Une des caractéristiques principales de ces données en question est qu'elles constituent, à la fois, un contenu d'informations personnelles ainsi qu'un élément permettant d'établir un lien indéniable

[305] Pour citer un exemple, RGPD, Cons. 30 « *Les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. [...]* »
[306] Directive 95/46/CE, Cons. 14.
[307] RGPD, Art. 4 point 14).
[308] RGPD, Cons. 51.
[309] G29, Avis 4/2007 sur le concept de données à caractère personnel, *Id.*, p. 9.

entre l'information et la personne, l'identifiant et l'authentifiant, par conséquent, de manière unique et spécifique[310].

Cette dualité information-identification portée par les données biométriques se retrouvent également dans les données génétiques, données résultant de l'analyse, notamment, de chromosomes, d'ADN ou d'ARN, fournissant ainsi des informations précises sur le corps de la personne et permettant une identification unique et sans aucune ambiguïté[311]. À cet égard, les prélèvements de tissus humains, tels que les prélèvements sanguins, ne sont pas en soi des données biométriques, mais constituent une source d'informations facilitant l'extraction de données biométriques et, « *lors de leur obtention, de leur conservation ou de leur utilisation, ils peuvent être accompagnés de données à caractère personnel associées* »[312]. En ce sens, la Cour européenne, sur le fondement de l'article 8, a eu l'occasion d'affirmer qu'elle « *doit aussi avoir égard au lien existant entre la personne qui a eu recours à une fécondation in vitro et les embryons ainsi conçus, et qui tient au fait que ceux-ci renferment le patrimoine génétique de la personne en question et représentent à ce titre une partie constitutive de celle-ci et de son identité biologique* »[313].

Par ailleurs, pour que les données soient à caractère personnel, elles doivent "concerner" une personne, ce que suggère les expressions adoptées par les législations et les juridictions susmentionnées « toute information concernant une personne » ou « personne concernée » par exemple. De façon générale, une information concerne une personne physique lorsqu'elle a trait à cette personne, qu'elle la touche, qu'elle est à son sujet. C'est le cas, par exemple, d'une personne filmée lors d'un entretien. Néanmoins, avec les avancées technologiques, il existe certains cas où il est difficile de déterminer si la donnée a trait à la personne ou pas, la marge de distinction étant bien fine. En effet, nombreuses informations peuvent de nos jours découler d'objets et non de personnes physiques ; ces informations concernant donc indirectement la

[310] À ce titre, le G29, dans son Avis 4/2007 sur le concept de données à caractère personnel, *Id.*, p. 9, fournit un ex. intéressant : « *[...] X a ces empreintes digitales, d'une part, et, d'autre part, [...] cet objet a été touché par quelqu'un qui présente ces empreintes digitales et celles-ci correspondent à X ; par conséquent, X a touché l'objet. Elles peuvent ainsi servir d'« identificateurs ». En effet, en raison du lien unique qui les relie à une personne physique spécifique, les données biométriques peuvent être utilisées pour identifier la personne physique.* »

[311] RGPD, Cons. 34 « *les données génétiques devraient être définies comme les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique, résultant de l'analyse d'un échantillon biologique de la personne physique en question, notamment une analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou de l'analyse d'un autre élément permettant d'obtenir des informations équivalentes.* »

[312] Recommandation CM/Rec(2016)6 du Comité des Ministres aux États membres sur la recherche utilisant du matériel biologique d'origine humaine, adoptée le 11 mai 2016, Chap. I – Objet et champ d'application, Art. 2, Al. 3.

[313] CEDH (Grande Chambre), Affaire Parrillo *c*. Italie du 27 août 2015, Requête n° 46470/11, §158.

personne. Habituellement, ces objets appartiennent à un individu, mais ils peuvent également subir une influence particulière de tierces personnes ou exercer une influence sur des individus ou se situer de n'importe quelle manière à proximité physique ou géographique d'un individu ou d'un autre objet, produisant ainsi des informations. À ce titre, en examinant les questions de protection des données soulevées par les marqueurs RFID, le G29 a eu l'occasion de préciser que « *les données concernent une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée* »[314]. Il semble donc que pour qu'une information soit considérée comme « concernant » une personne, trois éléments doivent être pris en compte, de manière alternative et non cumulative : le contenu, la finalité et le résultat. De manière évidente, le contenu se manifeste lorsque l'information a trait à une personne, à l'image des codes-barres intégrés dans les documents d'identité qui, manifestement, concernent la personne. L'élément de finalité, qui ressort quand les données sont utilisées dans un but d'évaluer ou d'influencer le statut ou le comportement d'un individu, permet également de déterminer si une information concerne une personne. Et en ce qui concerne le résultat, le lien avec les personnes physiques s'établit quand l'utilisation des données est susceptible d'avoir un impact, même léger, sur leurs droits et intérêts. Les informations ne doivent donc pas être nécessairement « axées » sur une personne pour qu'elles la concernent.

De même, les informations qui concernent une personne doivent viser une personne physique « identifiée ou identifiable ». L'identification s'opère normalement à travers des « identifiants » étroitement liés à la personne physique. Aux termes du nouveau RGPD, « *est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne [...]* »[315]. Cela peut être sa taille, la couleur de ses yeux ou une caractéristique propre à lui mais indirectement perceptible tel que son nom ou son adresse IP. De plus, « *ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes* »[316].

[314] Groupe de travail protection des données « Article 29 », Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification) N° WP 105, du 19 janvier 2005, 10107/05/FR, p. 9 ; Disponible en ligne : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp105_fr.pdf
[315] RGPD, Art. 4, point 1) « données à caractère personnel ».
[316] RGPD, Cons. 30.

Il semble alors évident que le contexte du cas d'espèce déterminera si les identifiants permettent ou non l'identification. Comme il est précisé dans la proposition modifiée de la Commission concernant la directive 95/46/CE, une personne peut être identifiée soit directement par un nom soit indirectement par un numéro de téléphone, un numéro d'immatriculation de véhicule, un numéro de sécurité sociale, un numéro de passeport ou par un croisement, une combinaison de critères significatifs permettant de la reconnaître au point de déterminer le groupe auquel elle appartient (l'âge, la fonction, le lieu de résidence, etc.). Ceci couvre également des données relatives à l'apparence, la voix, les empreintes ou caractéristiques génétiques[317].

Avec l'avancée des outils et des moyens informatiques, connaître l'identité d'une personne n'est plus véritablement requis pour l'identifier. Il est possible de reconstituer la personnalité d'une personne pour lui attribuer certaines décisions, indique ainsi le G29, « *sans même s'enquérir du nom et de l'adresse de la personne, on peut la caractériser en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui attribuer certaines décisions dans la mesure où le point de contact de la personne (l'ordinateur) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme* »[318]. À ce titre, les données pseudonymisées combinées avec d'autres informations sont susceptibles de constituer des informations concernant une personne physique identifiable. Suivant la même logique, la Cour de justice a ainsi affirmé que « *l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un traitement de données à caractère personnel [...]* »[319].

Pour déterminer si une personne est identifiable, le RGPD précise qu'il faut « *prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage* »[320]. L'ensemble des facteurs objectifs doivent donc être pris en considération, comme le coût de l'identification et le temps nécessaire pour l'effectuer, tout en tenant compte des technologies disponibles et des évolutions de celles-ci.

---

[317] Commission des Communautés européennes, "Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", COM(92) 422 final, *Id.*, Traduction du Commentaire relatif à l'article 2 *'"Personal data"[...] A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.). The definition would also cover data such as appearance, voice, fingerprints or genetic characteristics*", p. 9.

[318] G29, Avis 4/2007 sur le concept de données à caractère personnel, *Id.*, p. 15.

[319] CJCE, Affaire C-101/01 Lindqvist, *Id.,* p. 13008-13009, point 27.

[320] RGPD, Cons. 26.

De même, l'élément de finalité visé par un traitement de données doit être pris en compte puisque les moyens susceptibles d'être raisonnablement mis en œuvre mènent, *in concreto*, à l'identification des personnes. Ce qui a permis au groupe de travail précité de considérer les adresses IP comme des données qui concernent des personnes identifiables[321].

Enfin, les règles de protection des données à caractère personnel s'appliquent aux personnes physiques, à des êtres humains. Entendu ainsi, cela reflète un droit universel qui ne se limite pas à la nationalité ou au lieu de résidence d'une personne. L'article 6 de la Déclaration universelle des droits de l'homme évoque le concept de personne physique en disposant que « chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique »[322]. Le droit civil en général décrit la notion de personnalité juridique des êtres humains comme la capacité à être un sujet de droit ayant des responsabilités et des obligations, de la naissance jusqu'au décès.

In fine, il semble bien que dès qu'une information a un lien même faible ou résiduel avec une personne, elle constitue une donnée à caractère personnel faisant éventuellement référence à son identité physique et numérique.

§2. Le rôle de la révolution numérique et des avancées technologiques

Le rôle de la révolution numérique et des avancées technologiques dans la mise en œuvre du concept d'identité numérique s'est manifesté, notamment, par le biais d'une tendance croissante à l'unification du faisceau d'identité multiforme relatif aux personnes (A), mais aussi du développement simultané des activités d'identification, d'authentification et de traçabilité (B).

A. Un faisceau d'identités multiforme tendant à l'unification

La numérisation progressive de la vie quotidienne est porteuse d'un impact indéniable modifiant le processus de construction de l'identité des individus ; ce processus s'opérant de plus en plus dans et avec l'aide de l'environnement numérique.

---

[321] Dans un document de travail intitulé « Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne », WP 37, du 21 novembre 2000, le G29 a ainsi précisé que « *les fournisseurs d'accès Internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP donnée à l'utilisateur Internet. Il en va de même pour les fournisseurs de services internet qui conservent un fichier-registre sur le serveur HTTP. Dans ces cas, on peut parler, sans l'ombre d'un doute, de données à caractère personnel […]* ».

[322] Déclaration universelle des droits de l'Homme du 10 décembre 1948 : http://www.un.org/fr/universal-declaration-human-rights/

L'*homo numericus* évolue de nos jours à l'intérieur de multiples contextes sociaux différents. Ceux-ci engendrent un partage d'informations différentes en fonction du contexte dans lequel l'individu se trouve : familial, professionnel, médical, etc. Les relations se construisent par conséquent différemment en suivant les diverses frontières érigées selon les différents contextes en cours. Néanmoins, ces frontières ne paraissent pas être fixes, figées en ce sens qu'elles peuvent évoluer ou être renégociées en fonction des relations, des situations, ou même des acteurs en cause. La Professeure H. Nissenbaum[323] a thématisé cette approche en se fondant sur la notion de « vie privée en contexte », « *Privacy in context* ». Selon son analyse, les informations doivent être partagées et protégées conformément aux normes en vigueur régissant des contextes sociaux distincts et spécifiques. Le concept de « *privacy in context* » joue alors un rôle central pour toutes les questions entourant le partage inapproprié, abusif, d'informations en y répondant grâce au concept du flux d'information en « contexte approprié », « *context-appropriate* », en accord avec la situation, indispensable à la vie privée et politique[324]. Sa vision de la notion de vie privée est celle d'une prise en considération des flux d'informations respectant le contexte approprié, d'usage, lui permettant d'en déduire qu'une compréhension réelle et concrète de la structure sociale des contextes prévient des atteintes et des dérapages. La Professeure affirme ainsi que « c'est la robustesse de la structure sociale des contextes et l'efficacité de leurs normes informationnelles respectives qui freinent les dérives et permettent d'éviter que la société ne perde sa vie privée par petits fragments »[325]. D'après cette perspective, les différents flux d'informations doivent respecter les différents contextes d'usages puisque chaque contexte relationnel, qu'il soit familial, professionnel, médical ou autre, a ses propres normes, qu'elles soient explicites ou non, conformément aux attentes des utilisateurs quant à la manière dont l'information va circuler. Suivant cette logique, en cas de dérogation, l'intégrité contextuelle se trouve alors rompue. En réalité, « ce qui importe ce n'est pas l'information en soi qui doit être appropriée ou non dans un contexte donné, mais plutôt si son partage et sa diffusion respectent les normes d'usages, appropriées en matière de flux d'informations »[326].
En pratique, cela reflète la nécessité de mettre en place une séparation de contexte en créant plusieurs identités numériques pour un seul et même individu. Leurs choix et gestions seront à

[323] Pr. Helen NISSENBAUM : https://nissenbaum.tech.cornell.edu/main_cv.html
[324] H. NISSENBAUM, *Privacy in Context*, *op. cit.,* p. 187.
[325] H. NISSENBAUM, *Privacy in Context*, *Id.*, p. 243: *"It is the robustness of the social structure of contexts and the efficacy of their respective informational norms that stop the slide down the slope and prevent a society from throwing away* [its] *privacy in tiny bits."*
[326] H. NISSENBAUM, "Privacy as contextual integrity", *In* Washington Law Review, Vol. 79, 2004, p. 123: "*What matters is not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or flow, respects contextual norms of information flow.*"

l'initiative de ceux-ci suivant le droit à l'autodétermination informationnelle, qui, selon une jurisprudence constante, est un droit compris dans la notion large de vie privée. La Cour européenne des droits de l'homme annonce en ce sens que la possibilité pour une personne « *d'exercer un choix conscient et réfléchi [...] touche un aspect intime de sa vie personnelle et relève à ce titre de son droit à l'autodétermination* »[327].

Toutefois, il faut noter que la tendance actuelle s'avère être celle d'aller à l'encontre de cette nécessité qui, pourtant, est centrale pour une construction de Soi libre et autonome. Le courant manifesté à l'ère de la révolution numérique est plutôt celui de l'unification des identités numériques. En effet, une même identité, telle que celle dont dispose une personne auprès d'un réseau social, est employée dans d'autres contextes différents tels qu'une identification auprès d'un site de commerce en ligne en passant par une identification sur un forum social, par exemple. Plus précisément, à un autre degré, la tendance est plus forte comportant une unification et une centralisation, voire une confusion, de l'identité numérique régalienne (civile, judicaire), appelée aussi identité 'forte', et de l'identité numérique dite 'souple', la « Soft eID ». Comme c'est le cas dans certains pays, l'identité régalienne peut être utilisée pour accéder à des services privés ; et d'un autre côté, des fournisseurs de « Soft eID » comme Google ou Facebook, semblent mettre en place une politique des « noms réels » qui consiste à demander à l'utilisateur de leurs services de fournir la preuve de son identité judiciaire, civile. Il y a donc le risque que ces acteurs se positionnent comme des opérateurs privés délivrant une identité qualifiée de « forte », ce qui rend alors possible des utilisations ultérieures de ce type d'identité dans d'autres contextes, *a priori* différents et étrangers de leurs buts initiaux, se démarquant *de facto* du concept de « *privacy in context* ». À cet égard, le G29 précise que les services de réseaux sociaux « *devraient donc pouvoir justifier le fait de contraindre leurs utilisateurs à agir sous leur véritable identité plutôt que sous un pseudonyme* »[328].

Cette confusion de contextes et de genre, qui s'avère être plus au service des logiques marchandes et de surveillance, est facilitée par le recours de plus en plus grand à un identifiant unique. Elle ne contribue d'aucune façon à la construction de l'identité suivant la conception de l'ipséité, alors même que l'identité prend sens par la singularité affirmée à travers l'*ipse* de la personne[329]. Une des solutions à cette situation est de concrétiser une démarche consistant à

[327] CEDH, Affaire Parrillo *c*. Italie, *loc. cit.,* §159.
[328] Groupe de travail « Article 29 » sur la protection des données, Avis 5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009, WP n° 63, 01189/09/FR, p. 12.
[329] P. RICŒUR, *Soi-même comme un autre*, *op. cit.,* p. 137-198.

cloisonner les « contextes appropriés », les contextes d'usages, tout en développant la pratique de création d'identités numériques, d'identités de réseaux, multiples. Les dispositions légales encourageant les techniques de pseudonymisation vont, par exemple, dans ce sens puisque « *la pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées [...]* »[330], à condition que toute information supplémentaire soit conservée séparément[331], facilitant indirectement une séparation de contexte.

Par ailleurs, la dématérialisation et l'absence de frontières, engendrée par la révolution numérique, transforment la manière dont l'identité est capturée et perçue ; certains auteurs estimant dans ce cadre que « *l'identité numérique est à rapprocher de la notion de donnée personnelle* »[332]. En d'autres termes, celle-ci doit être associée à toute information, qu'elle soit numérisée ou non, qui est susceptible d'identifier directement ou indirectement la personne concernée. Tel qu'il a été précédemment vu, la notion de donnée personnelle s'entend largement englobant l'état civil d'une personne mais aussi son image, ses données médicales et de géolocalisation, ses habitudes et comportements, etc.

Par définition, une donnée, notion ancienne en soi, est « *une information codée, figée et transmissible* »[333]. Elle requiert une codification, ce qui facilite sa collecte et son rapprochement avec d'autres données formulées avec les mêmes références (un même format par exemple) et elle doit être figée, égale à elle-même. Elle a aussi la caractéristique d'être transmissible en ce sens qu'elle peut être mémorisée, enregistrée dans un système (papier ou numérique), pour un traitement instantané ou ultérieur. D'ailleurs, « *le terme français de « donnée » est trompeur : il sous-entend que cette information est donnée volontairement* »[334]. Néanmoins, une grande partie des données générées ne sont pas perçues comme étant des données personnelles par leurs propres créateurs. Les données de navigation sur internet et l'historique de recherche par exemple, représentent aujourd'hui des données personnelles ayant une valeur marchande précieuse, mais qui, souvent, ne sont pas envisagées comme telles par ceux et celles qui les produisent. De plus, certaines données qui peuvent en elles-mêmes paraître anodines, rapprochées ou corrélées avec d'autres ont la possibilité de fournir des informations personnelles intimes, que l'utilisateur aimerait pourtant garder secrètes. Envisagée sous cet

---

[330] RGPD, Cons. 28.

[331] RGPD, Art. 4 - point 5) « *«pseudonymisation», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément [...]».*

[332] E. A. CAPRIOLI, F. MATTATIA, S. VULLIET-TAVERNIER, *L'identité numérique*, Cahiers de droit de l'entreprise n° 3, entretien 3, LexisNexis, Mai 2011.

[333] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 10.

[334] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *Id.,* p. 10.

angle, la donnée ne se réfère pas alors à un don de la part de la personne concernée, elle peut être collectée et construite par un traitement. Il est intéressant de souligner que, à la différence de la langue française, ce terme en anglais, à savoir « data », ne porte pas à confusion en l'occurrence.

En outre, une donnée personnelle constitue « *à la fois une information déclarative sur la personne et un ensemble d'informations non déclarées, mais recueillies automatiquement notamment lors de la navigation sur les sites web* »[335].

En pratique, lorsqu'une personne s'inscrit sur un site, que ce soit pour accéder à un produit ou à un service, elle fournit son adresse mail et, dans certains cas, ses nom, prénom, coordonnées bancaires et autres renseignements, manifestant ainsi un ensemble de ses données personnelles, non aisément envisagé par la personne concernée : ses coordonnées, les traces laissées sur les sites, les moteurs de recherches et les réseaux sociaux, mais aussi les traces laissées dans le monde physique, réel (si le service était un hôtel par exemple, ou un musée). Or, affirmait déjà L. Villa lors des débats parlementaires de 1977, « *la combinaison de données non sensibles permet de dégager des informations très indiscrètes* »[336]. De surcroît, les traces laissées par les individus ont, à l'heure actuelle, tendances à se multiplier avec la numérisation progressive de toutes les sphères de la vie quotidienne (services administratifs, banques, assurances, renouvellements d'abonnements etc.), mais surtout avec l'avènement rapide de l'internet des objets, appelés également « les objets connectés ». Et les moteurs de recherche permettent d'avoir également un aperçu structuré d'informations relatives à une personne sous formes de listes des résultats de leurs recherches, qui touchent potentiellement à une multitude d'aspects de la vie privée des personnes concernées[337].

Ainsi, laissées volontairement ou involontairement, ces traces contribuent à reconnaître et à distinguer une personne des autres, à la cibler, à la profiler ou encore à la discriminer, la stigmatiser. Il est vrai que la numérisation des activités multiplie, de manière radicale, les traces que chaque personne laisse sur les systèmes et les réseaux. De plus, les informations physiologiques et biologiques participent également à la singularité de l'individu concerné et à son individualisation. En effet, le corps humain fournit des éléments d'identification infaillibles : que ce soit l'ADN, l'ARN, la voix, les empreintes, l'iris ou autre, ils représentent

---

[335] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *Ibid.,* p. 11.

[336] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *op. cit.,* p. 5786.

[337] CJUE, Grande Chambre, Google Spain SL et Google Inc. *c.* l'Agencia Española de Protección de Datos et Mario Costeja Gonzalez, 13 mai 2014, Aff. C-131/12, points 27-28 : « *[…] parmi les données trouvées, indexées, stockées par les moteurs de recherche et mises à la disposition de leurs utilisateurs figurent également des informations concernant des personnes physiques identifiées ou identifiables et donc des «données à caractère personnel*». »

des sources illimitées permettant d'extraire des renseignements importants sur l'individu. Percevant ces risques, le nouveau RGPD prévoit des dispositions interdisant tout traitement qui « *révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques [...], des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique [...]* »[338], sous réserve de certaines exceptions expressément prévues par le règlement. D'autre part, la numérisation des données personnelles procède également des documents administratifs officiels : que ce soit avec la généralisation du passeport biométrique pour l'ensemble des citoyens européens, ou à travers la carte d'identité électronique déployée dans plusieurs pays du monde. Cela conduit également à la création de nouvelles bases de données comme le Fichier national des empreintes génétiques (FNAEG)[339] qui, au 1er septembre 2013, contenait les profils génétiques de 2 547 499 individus dont : 1 911 675 personnes mises en causes et 430 298 personnes condamnées ainsi que 149 097 traces non identifiées[340], ou le Fichier automatisé des empreintes digitales (FAED)[341] qui archive les données biométriques et/ou génétiques des individus condamnés et

[338] RGPD, Art. 9 - Traitement portant sur des catégories particulières de données à caractère personnel, Al. 1.

[339] Créé par la loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions de nature sexuelle ainsi qu'à la protection des mineurs, « *le fichier national automatisé des empreintes génétiques, placé sous le contrôle d'un magistrat, est destiné à centraliser les empreintes génétiques issues des traces biologiques ainsi que les empreintes génétiques des personnes déclarées coupables de l'une des infractions mentionnées à l'article 706-55 en vue de faciliter l'identification et la recherche des auteurs de ces infractions. Sont conservées dans les mêmes conditions les empreintes génétiques des personnes poursuivies pour l'une des infractions mentionnées à l'article 706-55 ayant fait l'objet d'une décision d'irresponsabilité pénale en application des articles 706-120, 706-125, 706-129, 706-133 ou 706-134.*
Les empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 sont également conservées dans ce fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction [...]» : Art. 706-54 Code de procédure pénale.

[340] CNIL, « FNAEG : Fichier national des empreintes génétiques », du 14 avril 2014 : https://www.cnil.fr/fr/fnaeg-fichier-national-des-empreintes-genetiques

[341] Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'Intérieur, Art. 1 « *I.- Est autorisé, dans les conditions prévues au présent décret, le traitement automatisé de traces et empreintes digitales et palmaires :*
-en vue de faciliter la recherche et l'identification, par les services de la police nationale et les unités de la gendarmerie nationale ainsi que par le service national de la douane judiciaire, des auteurs de crimes et de délits et de faciliter la poursuite, l'instruction et le jugement des affaires criminelles et délictuelles dont l'autorité judiciaire est saisie ;
-en vue de faciliter la recherche et la découverte des mineurs et majeurs protégés disparus ainsi que celles des majeurs dont la disparition présente un caractère inquiétant ou suspect eu égard aux circonstances, à l'âge de l'intéressé ou à son état de santé ;
-en vue de faciliter l'identification dans un cadre judiciaire des personnes décédées ainsi que l'identification des personnes découvertes grièvement blessées dont l'identité n'a pu être établie ;
-en vue de faciliter l'identification dans un cadre extrajudiciaire des personnes décédées.
II.- Est également autorisée, dans les conditions prévues au présent décret, la consultation du traitement automatisé des empreintes digitales :
-en vue de permettre l'identification d'un étranger dans les conditions prévues à l'article L. 611-4 du code de l'entrée et du séjour des étrangers et du droit d'asile ;

suspectés, ou encore le bureau d'ordre national automatisé des procédures judiciaires[342] qui répertorie toutes les informations relatives aux procédures et instructions judiciaires, aux plaintes, dénonciations ou autres. Il semble ainsi que la révolution numérique et les avancées technologiques tendent à faire de l'être humain un objet statique, numérique au sens *stricto sensu*, qui est décomposé en traces puis recomposé en données personnelles. Cette décomposition procède d'une démultiplication des attributs d'une personne concernée alors que la recomposition de son profil, de ses éléments identitaires, est facilitée par la prolifération massive, à l'ère du Big data, des traitements de ces données à caractère personnel et de l'interconnexion et du recoupement de ceux-ci. Autrement dit, c'est donc une tendance à la réification d'une personne physique qui découle d'une décomposition de ses attributs identitaires et/ou des éléments contribuant à sa personnalité, à la construction et au développement de son identité.

La question de la commercialisation de ces divers éléments se pose à ce niveau, puisque traditionnellement le droit les considère comme étant hors commerce. Ceci dit, les données personnelles ne représentent pas en elles-mêmes des objets statiques, figés, puisque l'Homme n'est pas réductible aux seules données le concernant, à son identité numérique. Percevant ces risques, Peyrefitte disait ainsi que c'est à juste titre que « *M. Forni a rappelé que George Orwell, dans 1984, avait évoqué de façon magistrale cette angoisse de se voir réduit à des données simplifiées. C'est l'angoisse de l'individu écrasé par une société devenue une machine sans tête ni cœur, une société absurde, où tout est renversé, où, comme dit Orwell, « la guerre*

-en vue de permettre l'identification des personnes dans le cadre de la procédure de vérification d'identité de l'article 78-3 du code de procédure pénal ».

[342] Art. 48-1 Code de procédure pénale : « *Le bureau d'ordre national automatisé des procédures judiciaires constitue une application automatisée, placée sous le contrôle d'un magistrat, contenant les informations nominatives relatives aux plaintes et dénonciations reçues par les procureurs de la République ou les juges d'instruction et aux suites qui leur ont été réservées, et qui est destinée à faciliter la gestion et le suivi des procédures judiciaires par les juridictions compétentes, l'information des victimes et la connaissance réciproque entre les juridictions des procédures concernant les mêmes faits ou mettant en cause les mêmes personnes, afin notamment d'éviter les doubles poursuites.*

Cette application a également pour objet l'exploitation des informations recueillies à des fins de recherches statistiques.

Les données enregistrées dans le bureau d'ordre national automatisé portent notamment sur :

1° Les date, lieu et qualification juridique des faits ;

2° Lorsqu'ils sont connus, les nom, prénoms, date et lieu de naissance ou la raison sociale des personnes mises en cause et des victimes ;

3° Les informations relatives aux décisions sur l'action publique, au déroulement de l'instruction, à la procédure de jugement et aux modalités d'exécution des peines ;

4° Les informations relatives à la situation judiciaire, au cours de la procédure, de la personne mise en cause, poursuivie ou condamnée.

Les informations contenues dans le bureau d'ordre national automatisé sont conservées, à compter de leur dernière mise à jour enregistrée, pendant une durée de dix ans ou, si elle est supérieure, pendant une durée égale au délai de la prescription de l'action publique ou, lorsqu'une condamnation a été prononcée, au délai de la prescription de la peine. […] ».

c'est la paix », « la liberté c'est l'esclavage ». C'est cela que nous refusons […] »[343]. De même, les nouvelles lois en la matière affirment la primauté de l'être humain[344], aspirant à vouloir protéger toutes ses facettes identitaires à travers le régime de protection des données désormais mis en place.

B. Identification, authentification et traçabilité

Une 'seule' identité numérique n'existe pas, annonce D. Forest, « *on confond trop souvent dans le discours courant identité, identité numérique et identifiant. L'identité numérique est un agrégat, aux contours assez flous, de notions éparses : pseudo, identifiant, log, donnée à caractère personnel et/ou technique, IP... si l'on demeure au plan du droit, ce concept d'identité, invoqué à tout crin, n'existe pas. On parle de nom, prénom, sexe et tout le reste échappe pour l'essentiel au droit, ou est présent de manière parcellaire via des dispositions ponctuelles. Le délit d'usurpation d'identité a été inséré en droit positif par le législateur, mais on ne sait toujours pas ce qu'il recouvre précisément ! la loi récente sur la protection de l'identité tente de la réduire à des caractéristiques invariables, comme des données biométriques. C'est trop réducteur pour une notion si complexe, il faudrait idéalement pouvoir intégrer la notion d'identité au sens psychologique et sociologique dans le Code Civil. […]* »[345]. Le recours à une variété de données de toute nature permet d'identifier une personne : « *au-delà des noms et prénoms d'une personne, il peut donc s'agir d'une adresse électronique, du numéro de sécurité sociale, d'un numéro de téléphone, d'un numéro de compte bancaire, d'un pseudonyme ...* »[346]. Il est évident que cette liste n'est pas exhaustive, l'image, les cookies, l'adresse IP, les logins et mots de passe, l'historique des recherches et ainsi de suite peuvent y figurer, caractérisant ainsi la massification des données et l'avènement du Big data.

Même si l'établissement de la preuve de l'identité reste une compétence nationale, une tendance à la mise en place d'une identité numérique au niveau européen s'est déjà manifestée. Ainsi, en 2014 un règlement sur l'identification électronique et les services de confiance, dit règlement eIDAS (Electronic IDentification And trust Services), fut adopté visant « *à susciter une*

[343] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Id.*, p. 5788-5789.
[344] Pour illustration : Loi « informatique et libertés », Art. 1er « *L'informatique doit être au service de chaque citoyen.* » ; RGPD, Cons. 4 « *Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité* ».
[345] D. FOREST, « Identité(s) Numérique(s) : Tous authentifiés ? », *In* CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », 2012, p. 38.
[346] Circulaire du 28 juillet 2011 relative à la présentation des dispositions de droit pénal général et de procédure pénale générale de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, BOMJL n° 2011-08 du 31 août 2011, 1. Dispositions de droit pénal, *1.1. Créations de nouvelles incriminations*, 1.1.1. Usurpation d'identité ou usage de données personnelles en vue de porter atteinte à la tranquillité, à l'honneur ou à la considération d'autrui.

confiance accrue dans les transactions électroniques au sein du marché intérieur en fournissant un socle commun pour des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques et en accroissant ainsi l'efficacité des services en ligne publics et privés, ainsi que de l'activité économique et du commerce électronique dans l'Union »[347]. Abrogeant la directive « signature électronique »[348] avec une entrée en vigueur prévue pour le 1er juillet 2016, ce règlement s'inscrit dans la lignée de la stratégie numérique mise en œuvre pour l'Europe.

À l'échelle nationale, les États membres de l'Union ont commencé à prévoir l'instauration d'une carte d'identité électronique unifiée. Ainsi, le 15 février 1999 l'Estonie adopta une loi sur les documents d'identité qui prévoit la création d'une carte d'identité électronique comportant le nom, la date de naissance ou le numéro personnel d'identification, une photographie ou une image faciale ainsi que la signature ou l'image de la signature du détenteur de ladite carte[349]. En mars 2004, ce fut au tour de l'Autriche qui créa et fixa les conditions de mise en place de la « carte citoyenne », "*Citizen Card* ", servant à valider « l'identité unique » de son détenteur[350]. En France, le Ministère de l'Intérieur a lancé en 1999 un programme public d'identité nationale électronique sécurisée, appelé aussi INES, pour une meilleure identification des citoyens comprenant deux volets principaux : d'une part, un passeport muni d'une puce électronique comportant des données biométriques et, d'autre part, une carte nationale d'identité électronique (CNIe) accordant l'accès à des services numériques, notamment aux services d'administration électroniques. À la suite des attentats de 2001 aux États-Unis et depuis l'adoption en 2004 du Règlement européen visant l'intégration d'éléments biométriques

[347] Règlement (UE) N° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE du 28/08/2014, Cons. 2.

[348] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999, portant sur un cadre communautaire pour les signatures électroniques, Date de vin de validité : 30.06.2016, JOUE L 13 du 19.01.2000, p. 12-20.

[349] Identity Documents Act, *Riigikogu*, Passed 15.02.1999, RT I 1999, 25, 365 Entry into force 01.01.2000, Chapter I. General Provisions, §2. Identity documents "*(1) An identity document (hereinafter document) is a document issued by a state authority in which the name, date of birth or personal identification code, and a photograph or facial image and the signature or image of signature of the holder are entered, unless otherwise provided by law or legislation established on the basis thereof*", p. 2/24.
https://www.riigiteataja.ee/en/tolge/pdf/504112013003

[350] The Austrian E-Government Act – Federal Act on Provisions Facilitating Electronic Communications with Public Bodies, entered into force on 1 March 2004, Austrian Federal Law Gazette (BGBl), part I, Nr. 10/2004, Part II. Identification and Authentication in Electronic Communications with Public Bodies, "*The "Citizen Card" Function: 4. (1) The citizen card serves to validate the unique identity of a person making a submission and of the authenticity of a submission made electronically in procedures for which a controller in the public sector has set up a technical environment in which the citizen card can be used."*
http://archiv.digitales.oesterreich.gv.at/DocView.axd?CobId=31191

dans les passeports et les documents de voyage[351], les États membres sont tenus d'établir une nouvelle génération de documents de voyage, à savoir un passeport biométrique muni d'une puce électronique sans contact, lisible à distance. Le projet INES s'inscrivait dans cette lignée et aspirait à être une véritable révolution en termes d'identification et d'authentification des citoyens. Principalement, ce projet prévoyait de mettre en place une nouvelle carte d'identité (payante et certainement obligatoire) destinée à être articulée avec plusieurs fichiers centraux de données nominatives : le fichier d'état civil constitué à partir du Répertoire national d'identification des personnes physiques contenant le numéro NIR susmentionné, le fichier d'empreintes digitales des porteurs de titres d'identité, le fichier comprenant l'image faciale numérisée de ceux-ci et enfin, un fichier des titulaires de passeports. En outre, la nouvelle CNIe comprendrait des éléments biométriques, propres à son détenteur, stockés dans une puce électronique. Il était donc prévu que « *comme le « passe Navigo » mis en place en région parisienne par la RATP, les données personnelles contenues dans cette puce puissent être interrogeables sans contact lors de procédures de contrôles automatisées* »[352]. Et les informations contenues dans celles-ci seraient divisées en « cinq blocs » distincts[353] : un « bloc identité », contenant principalement les empreintes digitales et la photo numérisée du titulaire ; un « bloc authentification de la carte » permettant de prouver que la carte est authentique ; un « bloc identification du porteur » facilitant l'accès du détenteur à des services électroniques publics ou privés ; un « bloc signature électronique » offrant la possibilité de signer électroniquement des documents d'administration publique (e-administration) ; et un « bloc portfolio personnel » permettant la conservation d'informations personnelles supplémentaires le concernant.

Néanmoins, ce projet a fait l'objet de nombreuses contestations, débats et critiques et fut, dans ce contexte et à la suite du changement de gouvernement, abandonné pour être remplacé par le projet dit de « protection de l'identité ».

---

[351] Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, JO L 385 du 29.12.2004, p. 1–6.

[352] P. PIAZZA, « Les résistances au Projet INES », *In* Cultures & Conflits n°64, 2006, p. 65-75, § 4.

[353] Rapport d'information n° 439 (2004-2005) de J.-R. LECERF, fait au nom de la mission d'information de la commission des lois sur la nouvelle génération de documents d'identité et la fraude documentaire, déposé le 29 juin 2005, *Identité intelligente et respect des libertés*, Sénat, Coll. Les Rapports du Sénat, II. A- Un titre d'identité biométrique : quels avantages pour la sécurité, point 2) d. Le projet INES http://www.senat.fr/rap/r04-439/r04-439.html & Note de synthèse « Projet Identité Nationale Électronique Sécurisée », R. YUNG, sénateur, 2005, http://claudinelepage.eu/S-FDM/ryung/note-ines.pdf

Entre-temps, un décret de 2005 institue les passeports électroniques portant des puces électroniques sécurisées et des zones de lecture optique[354] qui « *a pour objectif, conformément aux textes européens, de prévenir et de lutter contre la fraude documentaire portant sur ces titres grâce à de nouvelles modalités de production, à l'insertion dans ce passeport de la photographie numérisée de son détenteur et d'un composant électronique (puce sans contact) contenant des données relatives à son détenteur et à sa délivrance, ainsi qu'à la mise en place de transmissions de données relatives aux passeports volés ou perdus vers le Système d'information Schengen et Interpol. […]. Enfin, le projet de décret vise à conférer au passeport la valeur d'un titre d'identité équivalent à la carte nationale d'identité qui devra permettre "la simplification de la vie quotidienne des administrés"* »[355]. En outre, la loi de finances de 2006[356], complétée par un décret de 2007, crée l'Agence nationale des titres sécurisés (ANTS) qui a pour mission principale de répondre aux besoins des administrations en ce qui concerne les titres sécurisés, à savoir les documents officiels délivrés par l'État[357].

Puis, le second projet de carte d'identité électronique, prévu initialement en 2009, a donné lieu à la loi du 27 mars 2012 sur la protection de l'identité[358] qui généralise l'insertion du composant électronique sécurisé, y compris pour les cartes d'identité. Celle-ci contiendrait une première puce, obligatoire, qui peut être qualifiée de « régalienne », portant les différentes données d'identification et données biométriques, y compris les empreintes digitales, mais aussi une deuxième puce, « facultative », contenant « *des données, conservées séparément, lui permettant de s'identifier sur les réseaux de communications électroniques et de mettre en œuvre sa signature électronique* »[359], que ce soit pour des services administratifs, publics ou commerciaux, privés. Il était prévu par conséquent de créer un « traitement de données à

[354] Décret n°2005-1726 du 30 décembre 2005 relatif aux passeports, Art. 1 à 3, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000018763666

[355] Délibération n° 2005-279 du 22 novembre 2005 portant avis sur le projet de décret instituant le passeport électronique et sur les modifications apportées au traitement DELPHINE permettant l'établissement, la délivrance et la gestion des passeports, CNIL, Légifrance, 14.10.2015, https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017652180

[356] Loi n° 2006-1666 du 21 décembre de Finances pour 2007, JORF 27 décembre 2006, Version en vigueur du 27 décembre 2006 au 28 décembre 2007, Art. 46.

[357] Décret n° 2007-240 du 22 février 2007 portant création de l'Agence nationale des titres sécurisés, JO n° 0047 du 24.02.2007, texte n° 8, Art. 2.

[358] Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, JORF n° 0075 du 28 mars 2012 p. 5604, texte n° 2, Art. 2 « *La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes : 1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ; 2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ; 3° Son domicile ; 4° Sa taille et la couleur de ses yeux ; 5° Ses empreintes digitales ; 6° Sa photographie.* »

[359] Texte adopté n° 883 « Proposition de loi relative à la protection de l'identité » (Texte définitif), du 6 mars 2012, Assemblée nationale, Session ordinaire de 2011-2012, Art. 3 : http://www.assemblee-nationale.fr/13/ta/ta0883.asp

caractère personnel facilitant leur recueil et leur conservation »[360], et l'ensemble de ces informations seraient stockées dans la base centrale des titres sécurisés gérée par l'ANTS[361]. Toutefois, cette loi sur la protection de l'identité a fait l'objet d'une censure partielle par le Conseil Constitutionnel qui a déclaré contraire à la Constitution certaines de ces dispositions au motif qu'elles portent une atteinte au droit à la vie privée disproportionnée par rapport au but poursuivi par le législateur[362]. Précisément, le Conseil juge « *qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ; [...] »*[363]. Par ailleurs, il dénonce les imprécisions entourant les conditions de mise en place de la puce facultative, conservée séparément, en soulignant que les dispositions « *ne précisent ni la nature des « données » au moyen desquelles ces fonctions peuvent être mises en œuvre ni les garanties assurant l'intégrité et la confidentialité de ces données ; qu'elles ne définissent pas davantage les conditions dans lesquelles s'opère l'authentification des personnes mettant en œuvre ces fonctions, [...]* »[364]. En conséquence, ces dispositions furent jugées contraires à la Constitution.

---

[360] Texte adopté n° 883 « Proposition de loi relative à la protection de l'identité », Art. 5 « *I. – Afin de préserver l'intégrité des données requises pour la délivrance du passeport français et de la carte nationale d'identité, l'État crée, dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un traitement de données à caractère personnel facilitant leur recueil et leur conservation. Ce traitement de données, mis en œuvre par le ministère de l'intérieur, permet l'établissement et la vérification des titres d'identité ou de voyage dans des conditions garantissant l'intégrité et la confidentialité des données à caractère personnel ainsi que la traçabilité des consultations et des modifications effectuées par les personnes y ayant accès.* »

[361] Décret du 2 décembre 2011 modifiant le décret n° 2007-255 du 27 février 2007 fixant la liste des titres sécurisés relevant de l'Agence nationale des titres sécurisés, ayant pour objet l'élargissement de la liste des titres relevant de la compétence de l'ANTS rajoutant par conséquent la carte nationale d'identité, JORF n° 0280 du 3 décembre 2011 p. 20474, texte n° 26.

[362] Conseil Constitutionnel, Décision n° 2012-652 DC du 22 mars 2012 sur la Loi relative à la protection de l'identité, JORF n° 0075 du 28 mars 2012 p. 5607, texte n° 6.

[363] Conseil Constitutionnel, décision du 22 mars 2012 sur la Loi relative à la protection de l'identité, *Id.*, Cons. 11, p. 5-6. Ainsi, le Conseil relève, que « *ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française; que les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne ; que les dispositions de la loi déférée autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire ;* », Cons. 10, p. 5.

[364] Conseil Constitutionnel, décision du 22 mars 2012 sur la Loi relative à la protection de l'identité, *Ibid.*, Cons. 14, p. 6-7.

Parallèlement, un projet de mise en place d'une identité numérique nommé IDENUM[365] a été lancé en 2010-2011, suspendu pendant une certaine période, puis relancé en 2013. Il expérimentait sur des formes de collaboration entre les secteurs privé et public pour la fourniture de labels et de certifications. Inscrit dans le cadre du programme des Investissements d'Avenir[366], ce projet a été cofinancé par l'État *via* la Caisse des dépôts ainsi que par des acteurs privés tels que SFR, La Poste[367], le Crédit Mutuel-CIC ou encore Solocal Group[368]. L'objectif principal de ce projet n'était pas de créer « *des identifiants numériques mais un label qui certifiera que cet identifiant permet bien de récupérer des données qualifiées suffisantes pour s'identifier à un autre service. Un peu comme on le fait aujourd'hui avec Facebook, [...]* »[369]. Après une phase d'expérimentation pendant laquelle SFR agissait comme fournisseur d'identité, le projet a été suspendu courant 2015. IDENUM s'est alors rejoint au projet FranceConnect, lancé en 2014, qui s'inscrit dans le courant de l'État plateforme visant la transformation publique et numérique de l'État sous l'impulsion du Secrétariat général pour la modernisation de l'action publique (SGMAP)[370].

Créé par un arrêté de 2014[371], le télé-service FranceConnect est un « *dispositif qui garantit l'identité d'un usager en se reposant sur des comptes certifiés existants* »[372] et représente une sorte d'invitation ouverte aux fournisseurs de services, tels que les services d'impôt ou de mairie, aux fournisseurs d'identité comme les comptes AMELI ou ceux de La Poste, et aux fournisseurs de données, par exemple la Direction générale des finances publiques. Ainsi, un même acteur peut jouer plusieurs rôles à la fois, en fournissant à la fois des services et des données par exemple. En pratique, quand un utilisateur européen se connecte en ligne *via* le bouton (ou le portail) FranceConnect, il sera authentifié par le fournisseur d'identité de son choix qui confirmera à son tour l'identité de l'utilisateur au fournisseur de service en question,

---

[365] Le portail de l'économie, des finances, de l'action et des comptes publics, « Mise en place de l'identité numérique IDENUM », du 30 mai 2011 : https://www.economie.gouv.fr/mise-place-lidentite-numerique-idenum

[366] Le portail de l'économie, des finances, de l'action et des comptes publics, « Faire du numérique un espace de confiance », du 21 juin 2013 : https://www.economie.gouv.fr/le-numerique-espace-de-confiance

[367] https://legroupe.laposte.fr/espace-presse/liste-des-communiques/creation-d-une-societe-commune-idenum

[368] A. BARBAUX, « Identifiant numérique unique Idenum : NKM en a rêvé, Fleur Pellerin l'a fait », L'usine digitale, publié le 10 avril 2013 : https://www.usine-digitale.fr/article/identifiant-numerique-unique-idenum-nkm-en-a-reve-fleur-pellerin-l-a-fait.N194954

[369] A. BARBAUX, « Identifiant numérique unique Idenum », *Id.*

[370] Le portail de la transformation de l'action publique, « Une nouvelle organisation pour la transformation publique et numérique de l'État - Décrets du 20 novembre 2017 », du 21 novembre 2017 : http://www.modernisation.gouv.fr/etudes-et-referentiels/decrets/une-nouvelle-organisation-pour-la-transformation-publique-et-numerique-de-letat-decrets-du-20-novembre-2017

[371] Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », JORF n° 0180 du 6 août 2015 p. 13487, texte n° 4.

[372] https://api.gouv.fr/api/franceconnect.html

qui ouvrira en conséquence l'accès à ses services en ligne. Sa vocation est celle d'une reconnaissance rapide, d'une navigation simplifiée et la suppression du besoin de « *jongler avec une multitude d'identités numériques* »[373]. Ainsi, quel que soit le moyen de communication, la traçabilité, le suivi et la transparence des données transmises et manipulées lors des démarches en ligne (assortie de l'identification certifiée) sont assurés à l'encontre des utilisateurs, des autorités administratives et des autres fournisseurs de télé-services. Il semble donc qu'existe un mouvement s'orientant de plus en plus vers une unification des identités numériques à des fins, entre autres, d'identification, d'authentification, de traçabilité et de suivi.

L'identité numérique peut être perçue comme une « représentation informatique » d'une entité, d'une personne physique[374]. Cela correspond à l'ensemble des outils et moyens technologiques permettant à cette personne de se projeter et de se manifester, sous plusieurs formes et dans différents contextes, dans le monde du web. Cette représentation vise à associer à une personne un ensemble de données numériques, d'attributs, qui peuvent être figés, statiques à l'image du nom ou de l'empreinte, ou, au contraire, dynamiques tels que le nom, l'heure de démarrage et la durée d'utilisation d'un service utilisé, les données de localisation, les centres d'intérêts, les historiques de recherche, etc. Ce qui fait écho au texte adopté par l'Assemblée proposant une carte d'identité comportant deux puces : l'une figée, régalienne, l'autre dynamique et changeante.

Il apparaît alors que l'objectif principal poursuivi est celui d'identifier ou d'authentifier une personne. Une distinction devrait cependant être opérée entre identification et authentification, procédant du degré de confiance établi entre l'identité déclarée de la personne et l'identité numérique qu'elle détient. Ainsi, le processus d'identification électronique qui consiste à utiliser des données d'identification personnelles numériques, à savoir « *un ensemble de données permettant d'établir l'identité d'une personne [...]* »[375], représente de manière univoque une personne physique ou morale. Alors que l'authentification, qui est un « *processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique* »[376], quémande une preuve et un niveau de confiance plus élevé. En informatique, ceux-ci se traduisent par ce qui est nommé les « *credentials* » qui peuvent prendre la forme d'une signature électronique, d'une

[373] Pourquoi se connecter avec FranceConnect : https://franceconnect.gouv.fr
[374] M. LAURENT et S. BOUZEFRANE (dir.), *La gestion des identité numériques*, Ed. iSTE, Coll. Systèmes d'information, web et informatique ubiquitaire, janvier 2015, 284 p.
[375] Règlement eIDAS du 23 juillet 2014, *loc. cit.,* Art. 3 – Définitions « données d'identification personnelle ».
[376] Règlement eIDAS du 23 juillet 2014, *Id.,* Art. 3 – Définitions « authentification ».

empreinte biométrique ou d'un mot de passe à caractère spécifique. Certaines techniques récentes renforcent encore plus le niveau d'authentification en opérant des analyses comportementales[377] permettant d'authentifier, avec confiance, une personne.

Que ce soit pour identifier, authentifier une personne ou tracer son parcours ou ses activités, une sorte de relation d'interdépendance semble se tisser entre l'identité physique, perçue et vécue par les individus, et l'identité numérique, virtuelle, perçue et retracée par différentes entités. Cette nature dépendante de la relation qui se forme est critiquée par plusieurs auteurs et professeurs, dont S. Turkle : « *Turkle further criticizes the dependent nature of our relationships with technology ; she sees the potential of this dependency to critically influence our formation of identity. According to Turkle, through our relationships with computers, we become a tethered self: a self wired into social existence through technology* »[378].

[377] *Cf.* p. 380 et 577.

[378] A. BRINGS, "Identity Construction Online: An Analysis of Sherry Turkle's Ideas on the Influence of Technology on Identity", Gonzaga University, COML 509, p. 11: http://web02.gonzaga.edu/comlstudentresources/Brings_FinalPaper_COML509_doc.pdf

Chapitre II. La valorisation de l'identité au XXIe Siècle : Une influence interactive

« *Manipuler les données, c'est faire émerger du sens, et faire émerger des actions, cela avait un rapport très étroit avec le pouvoir.* »[379]

Une étude de la notion d'identité et de l'étendue de ses implications, y compris ses composantes numériques, induit une étude sur sa valorisation à l'ère numérique et sur la valeur, continuellement croissante, qui lui est accordée.

En effet, la notion de valorisation suppose une « *mise en valeur de quelque chose pour en tirer davantage de ressources* », ou, dans un sens plus philosophique, le « *fait d'accorder une importance plus grande, davantage de valeur à quelqu'un ou à quelque chose* » ; et en matière économique, elle indique une « hausse de la valeur marchande d'un produit ou d'un service, provoquée soit par une mesure législative soit par une intervention sur le marché »[380]. Quant au concept de valeur, il désigne le « *caractère mesurable prêté à un objet en fonction de sa capacité à être échangé ou vendu* ; [le] *prix correspondant à l'estimation faite d'un objet* », ou la « *mesure d'une grandeur, d'une quantité variable* », ou encore la « *qualité objective correspondant à un effet souhaité, à un but donné ;* [l'] *efficacité,* [la] *portée d'une chose* »[381]. Et, en économie, domaine qui exploite grandement les outils et les capacités numériques développés, ce concept se réfère particulièrement à l' « *évaluation d'une chose en fonction de son utilité sociale, de la quantité de travail nécessaire à sa production, du rapport de l'offre et de la demande* »[382]. Il ressort des développements suivants que, à l'heure de la révolution numérique, les données produites en masse présentent une valeur non négligeable, inimaginable par le passé, et s'avèrent être, continuellement et progressivement, valorisantes à titre personnel et/ou collectif.

À ce stade, il est donc utile de s'interroger sur la valeur rattachée aux données à caractère personnel, composantes de l'identité numérique, et la valorisation qui en découle, rappelant par conséquent le concept d'interactivité et l'influence doublement interactive opérée par l'ère du numérique et des avancées technologiques. Précisément, la notion d'interactive, qui « *se dit de*

[379] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 12.
[380] CNRTL, « Valorisation » : https://www.cnrtl.fr/definition/valorisation
[381] CNRTL, « Valeur » : https://www.cnrtl.fr/lexicographie/valeur ; Voir également, Dictionnaire Larousse, « Valeur » : https://www.larousse.fr/dictionnaires/francais/valeur/80972
[382] CNRTL, « Valeur », *Id*.

choses ou de phénomènes qui agissent les uns sur les autres »[383], désigne, en informatique, « *les matériels, les programmes ou les conditions d'exploitations qui permettent des actions réciproques avec des utilisateurs ou avec des appareils* »[384], conçus « *de manière à susciter certaines réponses de la part du public* »[385]. Ce chapitre permet ainsi d'observer l'influence réciproque, interactive, de la révolution numérique portée par la société du XXI^e^ Siècle sur la valeur et la valorisation des données personnelles, et, subséquemment, des identités numériques résultant de cette même révolution.

Comment se manifeste donc la valorisation des identités à notre époque ? Plus concrètement, quelle est la valeur portée par les masses de données à caractère personnel générées et collectées continuellement et quotidiennement ?

Il s'avère que l'influence de l'ère numérique est double, faisant écho à la définition de la notion d'interactivité susmentionnée, dans le sens où elle invoque un aspect interactif technique entre les données, les objets et les technologies, ainsi qu'un aspect interactif social entre l'intégralité des technologies et des données générées et les individus générant lesdites données et utilisant lesdites technologies. Autrement dit, les identités et les données y rattachées semblent avoir une valeur horizontale, se traduisant par la production des masses de données (Section 1), ainsi qu'une valeur verticale, se manifestant par la parole accordée aux masses de données produites et collectées (Section 2).

Section 1 – Une valeur horizontale : la production des masses de données

La valeur horizontale de l'identité numérique se traduit, principalement, par l'émergence synchrone du concept et des pratiques de documentation numérique, dite e-documentation (§1), ainsi que du concept et des pratiques de réputation numérique, dite e-réputation (§2), caractérisant simultanément la production des masses de données observées au XXI^e^ Siècle.

[383] CNRTL, « Interactif » : https://www.cnrtl.fr/definition/academie9/interactif
[384] La Langue Française, « Interactif : définition du Wiktionnaire » : https://www.lalanguefrancaise.com/dictionnaire/definition/interactif
[385] CNRTL, « Interactif » : *Id.*

§1. L'identité numérique : une e-documentation

La e-documentation de soi fut possible et facilitée grâce à l'avènement, d'une part, d'un web de l'interaction et de l'interopérabilité (A), et, d'autre part, d'un web de traces et d'informations numériques (B), simplifiant de ce fait la production et la circulation intenses des traces et données documentaires.

A. L'avènement d'un Web de l'interaction et de l'interopérabilité

Dans la vie de tous les jours, la construction de l'identité d'une personne se caractérise par une démarche constante d'évolution et d'interaction. À l'ère du numérique, la notion d'identité s'associe à une double perception, « la perception de sa construction personnelle et celle qui est perçue et reconnue par les autres »[386], rappelant ainsi les perceptions de l'identité telles que conçues par Goffman et Erikson notamment. Les perceptions découlent ainsi de la psychologie et du lien social renvoyant à l'idée de reconnaissance et de performance de soi, en d'autres termes, à l'identité pour soi. Celle-ci représente le reflet des actes d'une personne, qu'ils soient intentionnels ou non, *via* les messages diffusés et le sens qui en est dégagé. Comme il a été vu avec les théories de Goffman, l'identité d'une personne qui se construit par le jeu de l'interaction résulte de l'opposition entre l'identité pour autrui (celle définie par autrui) et l'identité pour soi[387].

À la fin des années 80, Tim Berners-Lee[388], un ingénieur informatique anglais pour le CERN[389] (Conseil européen pour la recherche nucléaire), a commencé ses travaux sur un système d'hypertexte, permettant d'opérer une liaison entre des documents électroniques, et sur le protocole d'application, permettant de les transférer et de les communiquer entre les ordinateurs. Il introduit son système au CERN en 1990, connu depuis sous le nom de World Wide Web : un moyen de communication rapide et efficace transformant *de facto* les normes et les communautés scientifiques et sociales. L'origine de la notion « hypertexte » peut remonter à la conception, au XVIII^{e} Siècle, de celle d'encyclopédie à savoir une large base de données et d'organisation aspirant à l'exhaustivité du savoir. Ainsi, en 1936, H.G. Wells avance l'idée d'une encyclopédie universelle qui serait le fondement idéologique d'un monde unifié, « *une base intellectuelle de tout homme intelligent au monde. Elle vivrait, croîtrait, évoluerait,*

[386] G. DESGENS-PASANAU, E. FREYSSINET, *L'identité à l'ère numérique*, Ed. Dalloz-Sirey, Coll. Présaje, 2009, p. 63-72.
[387] *Cf.* p. 42 et s.
[388] https://www.w3.org/People/Berners-Lee/
[389] https://home.cern/fr

serait révisée, enrichie, modifiée par tous les penseurs originaux, partout dans le monde. [...]»[390]. Mais l'histoire de l'hypertexte coïncide, concrètement, avec les développements technologiques et les avancées en informatique. Sa problématique se manifeste en 1945 avec V. Bush qui propose un système, nommé *Memex*, permettant d'automatiser la collecte et le stockage de documents et d'informations. Suivant son idée, un individu pourrait stocker des documents et des textes de toute nature ainsi que des notes et des idées personnelles moyennant un mode mécanique, permettant une consultation rapide et facile, en associant lesdites informations en fonction des besoins. Selon Bush, le cerveau des humains fonctionne par association, et, en s'appuyant sur cette logique, il souligne que « lorsqu'un "item", un élément, est saisi, il se colle instantanément au prochain item tel que suggéré par l'association de pensées, en accord avec le réseau complexe de pistes porté par les cellules nerveuses du cerveau. Ainsi, dès qu'un document parviendrait à la machine *Memex*, une multitude de voies associatives le mettrait en relation avec le trésor d'informations déjà collecté. De nouvelles formes d'encyclopédies apparaîtraient alors, préparés à travers un maillage de pistes associatives qui les traversent, prêtes à être inscrites dans le Memex et, à partir de là, amplifiées »[391]. Toutefois la réalisation de ce projet s'est avérée impossible face aux obstacles et aux lacunes technologiques de l'époque. D. Engelbart, principalement connu pour le développement d'interfaces, notamment la souris (accompagnant les ordinateurs), reprend dès 1963 les travaux de Bush à l'Institut de recherche de Stanford. Ses travaux aboutirent en 1968 donnant lieu au premier système mis en œuvre sous forme d'hypertexte : le NLS, pour oNLine System, une base de données facilitant le travail en collaboration[392] dans la mesure où tous les intervenants et les acteurs sont reliés en réseau à l'ordinateur.

---

[390] J.P. VERNIER, *H.G. Wells et son temps*, Presses Universitaires de Rouen et du Havre, 1971, p. 484.

[391] V. BUSH, « As we may think », The Atlantic Monthly, July 1945, Section 6 & 8, p. 108-110 "*The human mind does not work that way. It operates by association. With one item in its grasp, it snaps instantly to the next that is suggested by the association of thoughts, in accordance with some intricate web of trails carried by the cells of the brain. It has other characteristics, of course; trails that are not frequently followed are prone to fade, items are not fully permanent, memory is transitory. Yet the speed of action, the intricacy of trails, the detail of mental pictures, is awe-inspiring beyond all else in nature. [...] Wholly new forms of encyclopedias will appear, ready-made with a mesh of associative trails running through them, ready to be dropped into the memex and there amplified*"

[392] Engelbart voulait amplifier l'intelligence humaine, tel que suggère le titre de son deuxième projet : *Augment*, développé au sein de son laboratoire SRI (Stanford Research Institute devenu SRI International) qu'il a fondé à Stanford. *NLS/Augment*, commercialisé en 1984 par McDonnell-Douglas, est un environnement en réseau, de traitement de textes et de gestion d'idées permettant la collecte de documents, notes et rapports de recherche tout en fournissant des moyens de planification, d'analyse et de communication. Engelbart fournit donc les premiers outils et les premières pratiques de l'hypertexte, qui, selon sa vision, ne limitent ni ne contraignent les gens les plus habiles. Il souhaite ainsi encourager la performance et l'excellence : D.ENGELBART, « Authorship Provisions in Augment », From COMPCON '84 Digest: Proceedings of the COMPCON Conference, San Francisco, CA, February 27 - March 1, 1984 (OAD,2250,): https://www.dougengelbart.org/pubs/oad-2250.html & https://www.dougengelbart.org/about/augment.html

Cela dit, l'invention du terme « hypertexte » et la conceptualisation qui y est associée sont dues à T. Nelson[393] qui conçoit un projet hypertextuel qu'il nomme « *Xanadu* »[394] dont le but était la mise en place d'une structure qui permet de relier l'ensemble de la littérature existante dans un grand dépôt unique, où chaque texte pourra être également accessible[395]. La notion d'hypertexte désigne les informations lisibles par l'homme reliées ensemble et libérées de la contrainte d'être linéaires[396]. C'est donc une écriture non séquentielle, un texte électronique qui contient des liens vers d'autres textes, d'autres informations, tel que le web (diminutif du World Wide Web) par exemple. L'histoire de l'hypertexte se décline ensuite en divers projets et logiciels, valorisant chacun un aspect ou un autre de ce système : gIBIS[397] (pour *graphical Issue Based Information Systems*), le logiciel *HyperCard*[398] ou encore le logiciel *KnowledgePro*[399] (pour *Knowledge Processing System*) pour n'en citer que quelques-uns. Les différentes applications qui en ont découlé avaient pour but, premièrement, de gérer des masses de données et, ensuite, d'aider à marquer et à indexer des navigations capables de transformer ces données en informations structurées et, enfin, en connaissances significatives, rendues significatives pour la compréhension et le savoir humain.

---

[393] Dès 1965, Ted Nelson inventa les termes « *hypertext* » et « *hypermedia* » pour désigner des caractéristiques d'un système d'information électronique, d'une base de données informatisée dans son article « Complex information processing: a file structure for the complex, the changing and the indeterminate », ACM '65 Proceedings of the 1965 20th national conference, Cleveland, Ohio, USA, August 24 - 26, 1965, p. 84-100.

[394] Du nom du temple de plaisir dans le poème *« Kubla Khan : Or, a vision in a dream. A Fragment*. » de S.T. Coleridge : https://www.poetryfoundation.org/poems/43991/kubla-khan

[395] T. H. NELSON, *Literary Machines: The report on, and of, Project Xanadu concerning word processing, electronic publishing, hypertext, thinkertoys, tomorrow's intellectual revolution, and certain other topics including knowledge, education and freedom*, Mindful Press, Sausalito, California, 1981 (Les Nouvelles éditions ultérieures datent de: 1981, 1982, 1983, 1984, 1987, 1990, 1991, 1992 &1993)

[396] Ted Nelson publia en 1974 *Computer Lib/Dream Machines* – deux ouvrages inter-mêlés, « *intertwingled* », par nature (republié en 1987 par Microsoft Press, US) dans lequel se trouvent définis pour la première fois tous les concepts des hypertextes connus aujourd'hui. Les termes d'hypertexte et d'hypermédia sont ainsi employés pour la première fois dans cet ouvrage.

[397] J. CONKLIN & M. L. BEGEMAN, "gIBIS: a hypertext tool for exploratory policy discussion", CSCW '88 Proceedings of the 1988 ACM conference on Computer-supported cooperative work, Portland, Oregon-USA, September 26 - 28, 1988, p. 140-152; Abstract: "*This paper describes an application specific hypertext system designed to facilitate the capture of early design deliberations. It implements a specific method, called Issue Based Information Systems (IBIS), which has been developed for use on large, complex design problems. The hypertext system described here, gIBIS (for graphical IBIS), makes use of color and a high-speed relational database server to facilitate building and browsing typed IBIS networks. [...]*"

[398] "*On August 11, 1987, Bill Atkinson announced a new product from Apple for the Macintosh; a multimedia, easily programmed system called HyperCard. HyperCard brought into one sharp package the ability for a Macintosh to do interactive documents with calculation, sound, music and graphics. It was a popular package, and thousands of HyperCard "stacks" were created using the software*":
https://blog.archive.org/2017/08/11/hypercard-on-the-archive-celebrating-30-years-of-hypercard/

[399] C. PATTON, "Electronic Investment Tools Highlight Conference", InfoWorld du 25 juillet 1988, Info World Media Group Inc., p. 23 *"[...] Knowledge Garden Inc. also unveiled the Knowledgepro Graphics Toolkit, an add-in for software developers working with the Knowledgepro expert system shell. Graphics Toolkit links graphic images with hypertext for situations that require more than written text. [...]".*

L'hypertexte se réfère donc à une base de données au sein de laquelle un usager peut naviguer d'une information à l'autre par un jeu d'interaction et d'association entre les différents blocs d'informations existants.

Le projet *Xanadu* de Nelson est souvent perçu comme l'ancêtre du World Wide Web, voire comme une tentative de le créer. Là où le premier avait une ambition plus vaste, le second l'a d'une certaine façon vulgarisée. Le but initial du projet baptisé World Wide Web (W3) était de permettre à des scientifiques, travaillant dans des universités et des instituts partout dans le monde, d'échanger des informations de manière instantanée. En avril 1993, le CERN a élevé le logiciel du W3 dans le domaine public et a, par la suite, mis la version ultérieure de l'application sous licence libre. Ceci a conséquemment accéléré sa diffusion permettant, à terme, à la Toile mondiale de se tisser progressivement[400]. Cette Toile est considérablement large, autant dans sa dimension que dans ses contenus, contenus qui au fur et à mesure n'ont cessé d'augmenter quitte à exploser dans leurs quantités. Ce qui a induit la mise en place et le recours à des moteurs de recherche tâchant de mettre un semblant d'ordre dans ce chaos d'information productif, prolifique, inépuisable et intarissable, en se basant sur un classement selon le principe de pertinence[401]. Ce principe désigne une « *méthode de classement, désormais abandonnée au profit du principe de respect des fonds, selon laquelle les archives sont regroupées par sujet, sans tenir compte ni de leur producteur et de leur provenance, ni de leur ordre primitif* »[402]. Ce mouvement concrétisa ainsi le premier âge documentaire du Web, un lieu de relations asymétriques où l'individu est passif accédant simplement aux contenus des

[400] CERN, « La naissance du web » : où il est précisé que « *Le premier site web créé au CERN – et dans le monde – était destiné au projet World Wide Web lui-même. Il était hébergé sur l'ordinateur NeXT de Tim Berners-Lee. Le site décrivait les principales caractéristiques du web et expliquait comment accéder aux documents d'autres personnes et comment configurer son propre serveur. L'ordinateur NeXT – le serveur web d'origine – est encore au CERN. En 2013, le CERN a entrepris de remettre en service le premier site web, et a même rétabli le site web à son adresse d'origine* » : https://home.cern/fr/topics/birth-web

[401] V. PROZOROVA-THOMAS, « Le classement selon le principe de pertinence comme reflet de la commande d'État : les archives soviétiques », Matériaux pour l'histoire de notre temps, *L'historien face à l'ordre informatique*, 2006/2 (N° 82), La contemporaine, 2006, p. 58-64 : « *Les deux principes de classement des documents — selon leur « provenance » (auteur-concepteur) et selon leur « pertinence » (celle de l'information qu'ils contiennent) — ont, suivant les différentes époques, servi de fondement à l'organisation des archives, en Russie comme en France. Leur légitimité respective a fait couler beaucoup d'encre sans que personne ne s'interroge d'une part, sur le contexte idéologique et politique de leur apparition, d'autre part, sur leur répercussion sur l'usage scientifique du patrimoine archivistique. [...]. Dans le contexte actuel, les principes de pertinence thématique et du respect des fonds semblent enfin devenir complémentaires : il est en effet possible de classer et de décrire les documents en respectant leur provenance et de décliner ensuite l'instrument de recherche dans plusieurs thématiques via les diverses balises de codage en XML. Grâce aux inventaires informatisés, chaque principe peut donc trouver son champ d'application légitime.* »

[402] Dictionnaire de terminologie archivistique, « principe de pertinence », Direction des archives de France, 2002, Mise en forme par les Archives départementales du Nord, 2007, p. 28.

sites mais sans pouvoir véritablement agir, le but étant de connecter les informations, les documents, à travers internet.

Ensuite, vint le web instantané qui fournit en temps réel l'état des toutes dernières informations publiées, et dans lequel l'individu est actif, nommé le Web 2.0 ou World Live Web pour caractériser l'aspect direct, instantané de l'information et de la documentation. L'expression « Web 2.0 » de Tim O'Reilly, reprise par le Conseil d'État dans son étude annuelle sur le numérique et communément employée aujourd'hui, caractérise un tournant produit par « *l'augmentation des débits de connexion* [qui] *a permis au début des années 2000 l'émergence de nouveaux services reposant sur l'interaction, la collaboration et le partage entre des utilisateurs qui ne sont plus passifs, mais qui contribuent au contenu ; [...]* »[403]. Ce fut là l'avènement d'un deuxième âge documentaire où la logique d'interaction prévaut, se traduisant par l'émergence de l'ère des services de partage de pair à pair (comme eMule ou BiTorrent), des plateformes de partage de contenus (comme Instagram, YouTube, Flickr ou Dailymotion), des services et dispositifs en ligne (tel que BlaBlaCar ou le Couchsurfing), des podcasts, groupwares, weblogs, wikis et ainsi de suite ; sans oublier les réseaux sociaux qui représentent, à l'époque du Web 2.0, le service le plus emblématique. Le tout contribue, *de facto,* à cet âge de documentation qui permet un regroupement instantané et direct de contenus, à l'image d'autant de fragments, de strates documentaires aussitôt publiés, sitôt indexés et immédiatement accessibles. L'éclosion du Web 2.0 marque, dans ce contexte, « *le passage de l'interactivité à l'interaction et contribue ainsi à la construction de réseaux qui ne se basent plus sur l'échange d'informations, mais sur le partage du savoir* »[404]. Il se caractérise par le développement de nouveaux services et dispositifs sociotechniques liés à l'accroissement de l'importante place de l'internaute sur le web. Ce dernier devient alors une plateforme d'échange entre les utilisateurs, les applications et les services en ligne plutôt qu'un simple écran-vitrine.

La place de l'utilisateur de ce web se trouve bouleversée en ce sens qu'il devient le principal diffuseur d'informations à travers les réseaux sociaux, les blogs, les wikis, les tags, etc. En effet, là où le Web 1.0, première application du World Wide Web, reproduisait un modèle de communication qualifié de « *one-to-many* » employé par les médias traditionnels comme la télé ou la presse, le Web 2.0, en innovant les usages numériques, repose sur un modèle de communication dit « *many-to-many* » : chaque individu a la capacité d'être à la fois émetteur

[403] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, op. cit.,* p. 63.
[404] L. QUONIAM et A. LUCIEN, « Du web 2.0 à l'intelligence compétitive 2.0 », 7ème colloque du chapitre français de l'ISKO, *Intelligence collective et organisation des connaissances*, Juin 2009, France (p.15-24), p. 15.

et récepteur de l'information. Ainsi, « *plus qu'un phénomène technique, il s'agit d'un changement de mode de fonctionnement, d'organisation, d'apprentissage, de prise de décision. Celui-ci met en jeu une architecture de participation, une architecture sociale et une architecture d'applications informatiques partagées, collaboratives et réparties* »[405]. Les utilisateurs ont la possibilité de collaborer à l'écriture des contenus, de les modifier, de les partager ; *in fine* de contribuer activement au tissage de la Toile grandissante que représente le web. Dans cette perspective, les différentes applications du Web 2.0 mettent en réseau les mots-clés mais aussi leurs rapports et liens, tout en classant l'information, en la commentant, en l'annotant et ainsi de suite. De même, la technologie RSS (pour *Really Simple Syndication*) facilite l'abonnement à des listes d'informations collectées en permettant à l'utilisateur de visualiser rapidement et efficacement les nouvelles informations ajoutées.

S'est ainsi formée l'architecture d'internet qui a l'originalité d'être une « architecture en couche », présentant un caractère ouvert, décentralisé et innovant l'ayant habilité à se développer, à s'adapter et à s'intégrer, et d'aboutir aux évolutions qui ont été observées depuis lors. Cette architecture en couche, traduisant la structure en couches superposées d'internet, est porteuse de quatre couches principales la caractérisant : une couche physique, l'ensemble des matériels, des câbles etc., représentant l'infrastructure physique de l'internet ; une couche logique, comprenant l'ensemble des services, tels que le routage, le nommage ou l'adressage, permettant d'assurer la transmission des données, de faire donc voyager les informations, découpées en petits paquets de données, entre l'expéditeur et le destinataire, caractérisant ainsi l'infrastructure logique du réseau (le Protocole Internet TCP/IP) ; une couche composée des applications, qui constituent les programmes informatiques permettant à tout un chacun d'utiliser internet sans en être spécialiste, comme les e-mails, les réseaux sociaux ou encore les moteurs de recherche ; et, une couche constituée de l'information et de l'interaction sociale, nommée parfois cognitive ou sémantique, qui est celle des utilisateurs, des discussions et des échanges en temps réel, à travers le monde[406].

Sollicité par le CESE pour son Avis sur les données numériques, l'UNSA affirme que « *l'accroissement des données produites par tous - entreprises, particuliers, scientifiques, institutions publiques - et des objets connectés qui débouchera sur le web 3.0 d'ici à 2020, ainsi que le perfectionnement des outils d'analyse sont comparés aujourd'hui à un phénomène de*

[405] L. QUONIAM et A. LUCIEN, « Du web 2.0 à l'intelligence compétitive 2.0 », *Id.*, p. 16.
[406] F. DOUZET, « La géopolitique pour comprendre le cyberespace », In Hérodote N° 152-153, *Cyberespace : Enjeux géopolitiques*, La Découverte, 1er-2ème trimestre 2014, p. 6-7.

révolution aussi importante que l'imprimerie en son temps. »[407]. Cette nouvelle révolution numérique induite par le Web 2.0 semble entraîner deux effets principaux : d'un côté, une interconnexion réelle et instantanée des informations *via* les métadonnées[408] et l'interopérabilité du langage informatique utilisé et, de l'autre, une mise en réseau accrue des acteurs-consommateurs incités à développer, à la fois, une activité éditoriale et des rapports sociaux.

En effet, ces dernières années, sous l'impulsion des développements croissants des intelligences artificielles et des objets connectés, le passage du Web 2.0 au Web 3.0, appelé parfois le web sémantique, commence à se manifester[409]. Le web sémantique, qui, d'une certaine façon, accompagne toutes les phases d'évolution du web, désigne l'information qui est mise en réseau de manière intelligente. Il se nourrit et se complète du Web 2.0 tout en fournissant un modèle cohérent, une procédure type, ainsi que des outils appropriés pour la définition et l'utilisation des relations pertinentes entre les données disponibles sur le web. Autrement dit, « *the Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation* »[410]. Le web sémantique s'entend alors comme un ensemble de technologies et d'outils en ligne dont "l'interopérabilité"[411] permet des interactions entre elles grâce aux métadonnées. De plus, « *le Web sémantique, qui propose de poser des métadonnées sur l'ensemble des ressources du Web, est un allié de taille pour le Big Data, dès lors que les deux mouvements poursuivent le même objectif : faire parler les masses de données* »[412].

---

[407] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 131.

[408] Ce sont des données de description de données : « *Il s'agit donc de données sur les données, à propos des données, qui définissent, décrivent des données. Le terme est récent. Néanmoins, il y a toujours eu des métadonnées. Selon l'activité, cela s'appelle cataloguer, indexer, classifier, décrire, élaborer un instrument de recherche, que l'on soit bibliothécaire, documentaliste, archiviste, scientifique. [...] Les métadonnées sont un vaste sujet à la mesure du rôle qu'elles jouent dans le processus de pérennisation. Étymologiquement, « méta » provient du grec signifiant « après, au-delà de, avec » :« méta » données signifie « au-delà des données », « qui dépasse les données », « qui englobe les données ».* » F. Banat-Berger & C. huc, PIAF, Section 9 – Métadonnées, 22 novembre 2011 : http://www.piaf-archives.org/sites/default/files/bulk_media/m07s09/section09_papier.pdf

[409] Pour illustration : https://semantic-web.com/semantic-data-management/

[410] T. BERNERS-LEE, J. HENDLER & O. LASSILA, "The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities", Scientific American, May 2001, p. 1. https://www-sop.inria.fr/acacia/cours/essi2006/Scientific%20American_%20Feature%20Article_%20The%20Semantic%20Web_%20May%202001.pdf

[411] L'AFUL (Association Francophone des Utilisateurs de Logiciels Libres) et le RGI (Référentiel Général d'Interopérabilité officialisé par l'arrêté en date du 20 avril 2016 (JORF n°0095 du 22 avril 2016 texte n° 1)) proposent la définition suivante : « *L'interopérabilité est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre.* » http://references.modernisation.gouv.fr/sites/default/files/Referentiel_General_Interoperabilite_V2.pdf

[412] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *Id.,* p. 17.

Que ce soit la version 2.0 ou la 3.0, les deux se ressemblent en ce sens qu'elles collectent et indexent toutes les informations mises en ligne par les individus utilisateurs-acteurs. Avec l'accroissement du rôle de l'internaute en tant que contributeur au web, se manifeste parallèlement un accroissement du rôle de l'intimité des internautes, du rôle de leurs vies privées dans le jeu des données ainsi produites et gérées[413]. Une sorte de *continuum* stable semble, par conséquent, se mettre en place entre les identités, les documents et les comportements qu'ils soient en ligne ou hors ligne. Précisément, émergent de plus en plus des applications visant à supprimer la frontière entre le monde connecté et celui déconnecté[414]. Grâce aux nouvelles pratiques et technologies qui se développent, tout sur le web est en permanence collecté, traité, analysé, agrégé, indexé, documenté, sauvegardé ; et la plupart des informations faisant l'objet de ces divers traitements se rapportent aux relations virtuelles des individus, qu'elles soient sociales, professionnelles, personnelles, médicales, administratives. Dans ce cadre, « *la dichotomie réel/virtuel fut graduellement abandonnée au profit d'une vision plus complexe des interactions entre ces deux dimensions, de plus en plus imbriquées l'une dans l'autre. L'accent est aujourd'hui mis sur les stratégies, toujours plus sophistiquées et différenciées, d'exposition sur le réseau et tiennent compte du fait que le plus célèbre des sites dits de « réseau social », Facebook, fonctionne à partir de l'identité réelle des utilisateurs – et limite donc le jeu « libre » et « émancipateur » sur l'identité, initialement associée au cyberespace* »[415].

Tous les domaines en relation avec le numérique sont donc visés et, conséquemment, toutes les identités numériques. Il en ressort alors que « *l'homme est devenu un document comme les autres, disposant d'une identité dont il n'est plus « propriétaire », dont il ne contrôle que peu la visibilité (ouverture des profils à l'indexation par les moteurs de recherche), et dont il sous-estime la finalité marchande* »[416].

---

[413] *Cf.* p. 198 et s.

[414] Par ex., les outils de cache « cash features », d'API (Application Programming Interfaces) ou de Cache API employés par Google : "*The Cache API is a system for storing and retrieving network requests and corresponding responses. These might be regular requests and responses created in the course of running your application, or they could be created solely for the purpose of storing some data in the cache. The Cache API was created to enable Service Workers to cache network requests so that they can provide appropriate responses even while offline."* https://developers.google.com/web/fundamentals/instant-and-offline/web-storage/cache-api & https://support.google.com/websearch/answer/1687222?hl=en

[415] B. LOVELUCK, *Réseaux, Libertés et Contrôle : Une généalogie politique d'internet*, Ed. Armand Colin, Coll. Le temps des idées, 2015, p. 101 ; et l'auteur indique ainsi que « *Comme le note Josiane Jouët : « Avec la massification de ces espaces, l'endossement d'une identité numérique se banalise tandis que les pratiques de "reliance" à distance, de conversations triviales, mais aussi de partage d'écrits multimédias avec des internautes connus ou inconnus, proches ou lointains, est en voie de devenir une pratique de la vie quotidienne qui reconfigure le lien aux autres ».* »

[416] O. ERTZSCHEID, « L'homme, un document comme les autres », Hermès, La Revue 2009/1 (n° 53), p. 38.

B. L'avènement d'un Web de traces et d'informations numériques

À mesure que les utilisateurs contribuent de manière active à de nouveaux contenus, ainsi qu'à de nouveaux sites web, une mise en liaison nécessaire et simultanée dans la structure du web se trouve alors incorporée par d'autres utilisateurs qui découvrent le contenu puis le relient à d'autres. À l'image des synapses qui se forment et se tissent dans un cerveau[417], avec des associations se renforçant *via* un processus de répétition ou d'intensité, le web des connections, des interactions et des relations se cultivera naturellement en tant que résultat « *output* » de l'activité collective de tous les utilisateurs. L'architecture actuelle du web et du réseau internet entraîne la production d'une large variété de traces numériques documentaires, qualifiées de *Big data*.

Les individus occupent dorénavant le centre de la Toile mondiale ainsi tissée, place tenue précédemment par les documents et leur simple actualisation. Le processus permettant d'indexer les documents mis sur le web se déplace et se transmute pour englober l'indexation des individus par le biais des traces numériques laissées, consciemment ou inconsciemment, sur le réseau ; c'est donc vouloir englober leur identité numérique. Toute personne a une omniprésence particulière dans l'univers du web actuel, et développe et renouvelle des situations communicationnelles à travers les réseaux sociaux, les plateformes collaboratives, les sites communautaires, les forums, les applications de messageries instantanées ; le tout pouvant désormais être indexé. Dans ce cadre, « *c'est à une nouvelle dérive des continents documentaires que nous assistons, mais une dérive inverse de celle que nous enseignent la géologie et sa tectonique des plaques : aujourd'hui ne subsiste qu'une même pangée, qu'un même territoire uniformément indexable par quelques-uns, au nom de tous les autres* »[418]. L'information circule, se morcelle et finit par s'éparpiller, générant diverses traces numériques rendant possible une documentation des identités numériques en temps réel.

Au XXI[e] Siècle, une course vers une existence numérique et la construction d'une identité numérique semble régner et se pérenniser, devenant de plus en plus un « *trend* », une mode. La panoplie d'outils et d'applications disponibles facilite et contribue à la création de cette identité

---

[417] « *Le cerveau des mammifères est composé de plusieurs centaines de types neuronaux différents qui présentent des fonctions spécifiques. Chaque type de neurones est relié à d'autres types via des connections particulières appelées synapses. Chaque type de synapse a une localisation subcellulaire bien définie et des propriétés fonctionnelles particulières, permettant ainsi la formation d'un réseau neuronal fonctionnel* » : F. Selimi, I.M. Cristea, E. Heller, B.T. Chait & N. Heintz, « Comprendre la connectique du cerveau en disséquant chaque type de synapse », PLoS Biology (2009), 14 avril 2009, La recherche en sciences du vivant, Institut des sciences biologiques – CNRS, https://www.cnrs.fr/insb/recherche/parutions/articles09/F-Selimi.htm

[418] O. ERTZSCHEID, *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies*, Marseille, OpenEdition Press, Coll. « Encyclopédie numérique 1 », 25 mars 2013, p. 16, point 29 ; Disponible en ligne : https://books.openedition.org/oep/332?lang=en

et à son développement tout au long de la vie de l'individu[419]. En construisant sa présence numérique, l'individu exprime son « désir de liberté »[420] tout en révélant également ses capacités et ses performances par l'acquisition de différentes compétences : stratégiques, techniques, communicationnelles, managériales et parfois même de marketing. L'identité numérique qui se construit se décline en de nombreuses représentations numériques créées et développées à travers les technologies interactives. Ces représentations ne correspondent pas à la présence physique des individus mais se fondent plutôt sur les contenus créés et les traces laissées, ainsi que sur le mode d'interaction et de connexion qui définissent la représentation de l'individu influencée par la lecture et la perception des représentations des tiers. Le concept, vu précédemment, de Oyserman et Markus selon lequel les représentations sont des « *blocs sur lequel le soi se construit* »[421] trouve son écho dans ce cadre. Le mouvement lancé par les dernières révolutions technologiques et l'émergence de nouveaux outils et dispositifs impactent et modifient, de manière continue, les représentations faites. Et, rappelons-le, l'identité est le produit des processus interactifs entre l'individu et la société qui, continuellement, s'actualisent dans une représentation de soi[422].

L'ensemble de ces informations et représentations laissent des traces numériques qui passent d'un stock vers un flux. Les premières traces de l'identité numérique ont vu le jour avec le projet SAFARI précité[423] qui a conduit à la mise en place de la loi Informatique et libertés. Depuis, le débat sur les données et le partage ou l'accès aux données est récurrent. Tout comme l'identité, au sens traditionnel, ne peut être unique, parallèlement, transposée sur le web et mise en réseau, l'identité numérique ne peut l'être non plus, ce qui transparaît à travers la multitude de traces numériques laissées, des traces aussi disparates que nombreuses. En effet, jusqu'aux années 90, l'identité numérique s'assimilait à un identifiant numérique où il était question d'identification, d'authentification et de traçabilité, principalement pour la sécurisation des données et le partage entre les administrations. Puis, à partir des années 2000, les questions entourant la vie privée commencent à être soulevées face au développement massif du web de l'interaction et de la communication avec l'irruption, au tout début, de MiGente (2000),

[419] Par ex., en 2015, Facebook a introduit une application, nommée « Life », permettant de donner vie aux photos et vidéos postées sur Facebook : "*Now you can bring the photos and videos you share on Facebook to life with live video and collages, to help friends and family feel like they're in the moment with you*", https://newsroom.fb.com/news/2015/12/introducing-live-video-and-collages/

[420] G. DESGENS-PASANAU, E. FREYSSINET, *L'identité à l'ère numérique*, *op. cit.,* p. 69-71.

[421] D. OYSERMAN & H. R. MARKUS, "Self as social representation", *loc. cit.*, p. 118.

[422] *Cf.* p. 42 et s.

[423] *Cf.* p. 72 et s.

Friendster (2002), LinkedIn (2003), Hi5 (2003) et MySpace (2003)[424]. En même temps, Google se développait pour devenir peu à peu l'outil incontournable le plus utilisé aujourd'hui, dépassant en 2013 le cap des 30 mille milliards de pages indexées[425] et celui des 130 mille milliards en 2016[426].

Avec la massification et la banalisation de la production des données et informations mises en ligne, s'accompagnent une massification et une banalisation des traces numériques générées, qu'elles soient sociétales ou techniques, récoltées, partagées ou indexées, intégralement et indifféremment, dans un objectif de documentation, de renseignement, sur les individus. Ce qui rappelle l'analyse de Dubar sur l'identité narrative vis-à-vis de laquelle il indique que « *la quatrième forme identitaire, au croisement du « sociétaire » et de l'identité pour soi, est appelée forme narrative, elle renvoie à des Nous contingents et à des Je poursuivant leurs intérêts de réussite économique, sociale, personnelle. Cette configuration, qui inclut une mise en question ou à distance des identités attribuées, renvoie à un projet de vie, un style de vie individualisés. Dans cette forme biographique, pour soi, il y a besoin, par l'action dans le monde, de se faire reconnaître par des autruis significatifs. La réflexivité n'est plus tournée, comme précédemment, sur l'intimité d'un moi intérieur, mais sur un projet, à soi, d'être et de faire dans le monde* »[427].

Dans ce contexte, l'identité numérique se constitue par la somme des traces numériques se référant à un individu ou une collectivité. Celles-ci peuvent être des traces de profils qui correspondent à ce que la personne dit de soi (l'image voulue, l'identité déclarée), des traces de navigations fournissant des renseignements sur les pages web fréquentées et les comportements effectués (achat, commentaire, publication etc.) mais aussi des traces déclaratives se rapportant aux opinions, publications et réflexions de la personne. En d'autres termes, « *l'identité numérique peut être définie comme la collection des traces (écrits, contenus audio ou vidéos, messages sur des forums, identifiants de connexion, etc.) que nous laissons derrière nous, consciemment ou inconsciemment, au fil de nos navigations sur le réseau et le reflet de cet ensemble de traces, tel qu'il apparaît « remixé » par les moteurs de recherche* »[428]. Il en résulte

---

[424] Source : http://controverses.mines-paristech.fr/public/promo10/promo10_G20/historique-des-reseaux-sociaux/index.html

[425] Billions of times a day in the blink of an eye- March 1, 2013 – Google Search Blog : https://search.googleblog.com/2013/03/billions-of-times-day-in-blink-of-eye.html

[426] B. SCHWARTZ, "Google's search knows about over 130 trillion pages", November 14, 2016: https://searchengineland.com/googles-search-indexes-hits-130-trillion-pages-documents-263378

[427] C. DUBAR, *La Crise des identités, op. cit.,* p. 207.

[428] O. ERTZSCHEID, *Qu'est-ce que l'identité numérique ?, Id.,* p. 13, et l'auteur rajoute : « *Mon identité numérique c'est : adresse IP, cookies, courrier électronique, nom, prénom, pseudos, coordonnées (personnelles, administratives, bancaires, professionnelles, sociales), photos, avatars, logos, tags, liens, vidéos, articles, commentaires de forums, données géolocalisées, etc.* ».

une diversification intense des sources mais aussi de la nature des données et des informations qui circulent sur le web.

Au cours des premières années suivant l'adoption de la loi Informatique et libertés, les données étaient principalement collectées par des entités structurées qui constituaient des fichiers et documents sur des individus dont elles avaient à connaître dans les limites de leurs activités. Ainsi, les différentes administrations publiques recueillaient des données dans le cadre de leurs missions afin d'alimenter les fichiers de sécurité sociale, de police, ou encore des impôts. De leur côté, les entreprises collectaient et traitaient les données les concernant, telles que celles de leurs clients, salariés ou fournisseurs, et les associations celles de leurs adhérents par exemple. Ces diverses sources de données correspondaient donc à des contextes particuliers rappelant les concepts de « *privacy in context* » et de « *contextual integrity* » tels que conçus par Nissenbaum[429]. Néanmoins, à l'époque de la conception de la loi pour une République numérique, son allié le RGPD, et la nouvelle loi Informatique et libertés conséquemment modifiée, plusieurs nouvelles sources de données se sont développées, générant de ce fait une sensation d'obsolescence.

Déjà, il est important de noter la quantité de données publiées par les individus eux-mêmes sur les réseaux sociaux ou sur les sites de partage de contenus : les personnes livrent volontairement une masse d'information se rapportant à leurs situations familiales ou amoureuses, leurs activités ou relations professionnelles ou personnelles, leurs opinions et centres d'intérêts, leurs préférences littéraires, musicales ou audiovisuelles, et donc à leurs quotidiens. Suivant la même logique, les personnes communiquent, de nos jours, des informations concernant des personnes tierces. L'illustration la plus typique est celle de la photo partagée sur un réseau social attestant que telle personne était à tel endroit, à tel moment, dans telle situation, contribuant à la construction de sa présence numérique. De plus, l'accès et l'utilisation de ces photos sont facilités par la possibilité de « *taguer* » la personne en indiquant son nom, ce qui simplifie par conséquent l'opération de rapprochement et de croisement que peut entreprendre un moteur de recherche, par exemple, entre la personne taguée et les photos où elle figure ou toute autre information où elle est mentionnée. Suivant le même processus, des logiciels permettant d'opérer une reconnaissance faciale automatique d'un individu, en comparant une photo à d'autres où il est déjà identifié, se développent de plus en plus[430]. Par ailleurs, les nombreux

[429] *Cf.* p. 87 et s.

[430] Par ex., la technologie développée par Facebook dans cette optique, appelée « Tag Suggest », qui sert à la reconnaissance faciale : « *Notre technologie analyse les pixels dans les photos et les vidéos, comme votre photo de profil et les photos et vidéos dans lesquelles vous avez été identifié(e), afin de calculer un chiffre unique que nous appelons un modèle. Nous comparons d'autres photos et vidéos sur Facebook à ce modèle et si une*

outils et procédés en développement continu recueillent, de plus en plus fréquemment et automatiquement, les données personnelles que ce soit par le biais d'installation de cookies sur le terminal d'un individu, l'envoi d'un signal de localisation à l'opérateur (de télécommunications) par les smartphones ou les tablettes, la collecte d'images par les caméras de surveillance et de vidéoprotection ou encore la collecte des données d'achats extraites des cartes de fidélité ; sans oublier la masse de données dorénavant produites, en parallèle, par les objets connectés.

Cette diversification des sources de collectes s'accompagne d'une hétérogénéité croissante des données collectées. Lors de la collecte des données par les institutions, celles-ci étaient structurées en fonction, notamment, des caractéristiques objectives et stables de la personne, son âge, ses revenus ou les infractions commises par exemple. Alors que les données disponibles actuellement sur une personne sont « *disséminées, disparates et actualisables en permanence : il peut s'agir aussi bien de l'observation des goûts, des opinions, des relations, des lieux visités, des historiques de navigation sur Internet, de photographies, de mentions de la personne sur un site Internet, de messages échangés, de la vitesse d'une course à pied ou de tremblements corporels suggérant l'existence d'une maladie neurologique* »[431].

Depuis le début des traces numériques et jusqu'en 2003, les humains ont produit 5 exaoctets de données numériques, soit 5 milliards de milliards d'octets[432]. Dans son étude annuelle, le Conseil d'État indique qu'en 2012, « *le trafic mensuel a été de 43 exaoctets par mois, c'est-à-dire 43 milliards d'octets (10^{18}) ; c'est 20 000 fois plus qu'en 1996* »[433]. La croissance du nombre des internautes, des objets connectés ainsi que des débits de connexion a mené à une croissance exponentielle du nombre, du volume, de la variété, de la vitesse d'exploitation, de la valeur et de la véracité des données à collecter et à traiter, concrétisant ainsi l'assise du Big data. En effet, le taux de croissance du volume, du trafic et du flux de données ne cesse d'augmenter, et ce de manière encore plus accrue ces dernières années : 90% de la totalité des données disponibles aujourd'hui ont été créées ces dernières années[434]. Ce qui a également

correspondance est trouvée, nous vous reconnaîtrons. », « Comment fonctionne la reconnaissance faciale de Facebook ? », https://www.facebook.com/help/122175507864081

[431] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, op. cit.,* p. 155, et le Conseil rajoute à cet égard que « *les accéléromètres et les gyroscopes présents aujourd'hui sur les smartphones permettent en effet de recueillir de telles informations.* »

[432] S. LUPIERI, « Big data : devant nous le déluge », Enjeux, Les Échos, du 1er octobre 2012 : http://archives.lesechos.fr/archives/2012/Enjeux/00294-036-ENJ.htm#

[433] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, Id.,* p. 48.

[434] C. BRASSEUR, *Enjeux et usages du Big Data : Technologies, méthodes et mises en œuvre*, Paris, Ed. Hermès - Lavoisier, Coll. Management et Informatique, 2013, p. 30.

induit la croissance de la mémoire informatique, les « bytes » ou bits, qui est passée du gigaoctet (10^9 octets) au téraoctet (10^{12} octets), au pétaoctet (10^{15} octets), au exaoctet (10^{18} octets) et même au zettaoctet (10^{21} octets). Google traite ainsi plus de 27 pétaoctets de données par jour, un volume qui correspond à des milliers de fois la quantité de l'ensemble des documents imprimés dans la bibliothèque du Congrès américain[435]. Quant à Facebook, 10 millions de nouvelles photos sont postées, téléchargées, toutes les heures et le nombre de messages sur Twitter augmente d'environ 200% annuellement dépassant, fin 2012, les 400 millions de *tweets* par jour[436]. Depuis le début du World Wide Web (1990) et jusqu'en 2015, le pourcentage mondial des utilisateurs d'internet est passé de 0,05 % à 44 %[437] et le nombre d'abonnements au service de téléphonie mobile de moins 2 pour 1 000 personnes à, approximativement, un abonnement par personne[438].

Au niveau mondial, il existe, au moment de la rédaction, plus d'1,5 milliards de sites web[439] et toutes les minutes plus de 400 000 tweets, 20 millions de SMS et 250 millions de mails sont envoyés et reçus. Dans ce contexte, « *si l'on tient compte de toutes les sources de données, il faut, en 2013, dix minutes pour produire 5 exaoctets d'informations. Il fallait deux jours en 2011 pour générer une volumétrie comparable, (selon Eric Schmidt, l'ancien PDG de Google)* »[440]. Cette explosion massive de données résulte principalement de l'accroissement continu des microprocesseurs, de la mémoire numérique, de la généralisation du haut débit, de la réduction des frais de collecte, de stockage et de traitement des données, des réseaux sociaux, de l'ensemble du web 2.0 et 3.0, des smartphones, des appareils numériques, des objets connectés, du *cloud computing*[441]. Ce dernier, appelé en français l'informatique en nuage, correspond à des prestations à distance, le stockage de données par exemple, qui sont réparties physiquement dans des *Data centers* et non pas sur le poste (terminal) de l'utilisateur. Cette forme de prestation particulière permet de nos jours de stocker des données à un prix maigre,

---

[435] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data: A revolution that will transform how we live, work and think*, Great-Britain, John Murray (Publishers), 2013, p. 8.

[436] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data, Id.,* p. 8.

[437] World Bank Group, 2017 World Development Indicators, International Bank for Reconstruction and Development/The World Bank, 2017, p 86; Disponible en ligne: https://data.worldbank.org/products/wdi & https://datacatalog.worldbank.org/dataset/world-development-indicators

[438] World Bank Group, 2017 World Development Indicators, *Id.,* p. 6: "*Demand for mobile cellular subscriptions continues to grow, while fixed-line connections fall.*"

[439] http://www.internetlivestats.com/total-number-of-websites/

[440] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 11.

[441] « *Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire.*
Note : L'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients. » Commission Générale de terminologie et de néologie, Vocabulaire de l'informatique et de l'internet, JORF du 6 juin 2010, Texte n° 42.

quasi-inexistant, provoquant par conséquent l'effondrement quasi-total du coût de la mémoire numérique : là où il était évalué à 300 dollars dans les années 80, il vaut aujourd'hui à peu près 0,00022 dollar[442]. La quantité et le volume de données désormais créées est si astronomique et si hétéroclite qu'il est désormais possible de les qualifier et de les analyser en termes de Big data, caractérisé par des éléments composant la formule dite des « 5V ». Selon le Conseil d'État, « *ce n'est qu'au cours de cette période que des solutions permettant d'exploiter des données hétérogènes (textes, images, données de connexion, données de localisation, etc.) et non structurées sous forme de base de données ont été développées* »[443].

Dans cette perspective, plusieurs critères servent également à la collecte, le stockage et l'analyse du Big data et sa capacité à être utilisé. Ainsi, la Vélocité ou la Vitesse correspond aux délais d'actualisation et d'analyse des données mais aussi à leurs traitements en temps réel et non plus en différé permettant, en conséquence, de les analyser en flux (*streaming*) sans devoir les stocker. La Dr. McGregor accompagnée d'une équipe de chercheurs de l'Université d'Ontario et d'IBM travaillent avec un certain nombre d'hôpitaux sur un logiciel assistant les médecins dans leurs diagnostics en les aidant à prendre de meilleures décisions lors de la prise en charge de bébés prématurés. Le logiciel capture et traite les données des patients en temps réel, repérant et traquant 16 différents flux de données, tels que la fréquence cardiaque, la fréquence respiratoire, la tension artérielle et le taux d'oxygène sanguin, correspondant ensemble à approximativement 1 260 saisies de points de données (*data points*) par seconde. Ce logiciel a la capacité, en suivant une méthode fondée sur la corrélation (et non la causalité), de détecter des changements subtils, légèrement perceptibles, dans la condition des prématurés et de signaler l'apparition d'une infection 24 heures avant la manifestation de symptômes patents, visibles. Dr. McGregor explique, en effet, que « *you can't see it with the naked eye, but a computer can* »[444]. Deux autres éléments, déjà traités, correspondent à la Variété et au Volume des données numériques du fait de leur production et leur hétérogénéité grandissantes[445]. La

[442] A history of storage cost (update) : http://www.mkomo.com/cost-per-gigabyte-update
[443] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, Id.,* p. 48.
[444] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data, Id.*, p. 60.
[445] Il est, par exemple, possible aujourd'hui d'étudier les sentiments et opinions des individus *via* la grande variété des tweets publiés ou des reviews postés sur un produit grâce au « Social Media Data for Sentiment Analysis » : *"We introduce a novel approach for automatically classifying the sentiment of Twitter messages. These messages are classified as either positive or negative with respect to a query term. This is useful for consumers who want to research the sentiment of products before purchase, or companies that want to monitor the public sentiment of their brands. There is no previous research on classifying sentiment of messages on microblogging services like Twitter. We present the results of machine learning algorithms for classifying the sentiment of Twitter messages using distant supervision. Our training data consists of Twitter messages with emoticons, which are used as noisy labels. This type of training data is abundantly available and can be obtained through automated means. We show that machine learning algorithms (Naive Bayes, Maximum Entropy, and SVM) have accuracy above 80% when trained with emoticon data*", A. Go, R. Bhayani & L.

qualité des données, leur Véracité, représente également une autre caractéristique en raison de l'absence de fiabilité des données exploitées pouvant induire une remise en cause des conclusions tirées du processus de traitement. Le mouvement engendré par les « *fake news* », pratique récente émergente, en constitue une illustration adéquate, notamment à l'heure actuelle où des tweets ou des microblogs publiés peuvent affecter, en l'espace de quelques minutes, la cotation en bourse d'une entreprise (cas de Snapchat, Chipotle Mexican grill ou Tesla) en la faisant drastiquement chuter ou augmenter[446]. À ces quatre éléments, s'ajoute un dernier dans la formule dite des « 5 V » servant à caractériser le Big data[447], celui de la Valeur[448], de la Valorisation des données, attendue de leurs exploitations.

À travers cette masse de données désormais disponible, il semble alors que se forme pragmatiquement une documentation, de plus en plus complète, détaillée et transparente, des identités et empreintes numériques. Autrement dit, le processus de documentation s'opère à travers la collecte des traces et données numériques produites et partagées par les internautes, mais aussi par tout ce que celles-ci révèlent finalement sur les individus en question, une fois captées et traitées par les moteurs de recherche ou les réseaux sociaux. L'un des défis actuels auquel se trouve confrontée la société de l'information est celui de permettre à tout individu d'inverser la tendance entre l'identité numérique vécue et celle perçue, en lui accordant les moyens de reprendre le contrôle et pouvoir mesurer l'étendue de la masse des traces numériques produite et d'en délimiter le périmètre.

Un nouvel âge documentaire, dynamique et innovant, paraît alors se dessiner, « *celui qui systématise l'instrumentalisation de nos sociabilités numériques ainsi que le caractère indexable d'une identité constituée par nos traces sur le réseau, indistinctement publiques, privées ou intimes. Documents et mots-clés ont acquis une dimension marchande* »[449].

Huang, "Twitter Sentiment Classification using Distant Supervision", technical report: https://cs.stanford.edu/people/alecmgo/papers/TwitterDistantSupervision09.pdf

[446] Par ex., G. Clément, « Bourse : tous ces tweets qui ont affolé les marchés financiers », Le Revenu 14/03/2018 : https://www.lerevenu.com/bourse/bourse-tous-ces-tweets-qui-ont-affole-les-marches-financiers & N. Ingraham, « False tweet sent a company's stock plummeting more than 25 percent », The Verge, 29/01/2013 : https://www.theverge.com/2013/1/29/3930010/false-tweet-sent-a-companys-stock-plummeting-25-percent

[447] *Cf.* Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, Id.,* p. 48 ; CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *Id.,* p. 16, et M.-P. HAMEL et D. MARGUERIT (département Questions sociales), « Analyse des big data : Quels usages, quels défis ? », Commissariat Général à la stratégie et à la prospective, La Note d'analyse N° 08- Novembre 2013, p. 2-3.

[448] *Cf.* p. 135 et s.

[449] O. ERTZSCHEID, « L'homme, un document comme les autres », *Id.,* p. 38.

§2. L'identité numérique : une e-réputation

Complément de l'identité numérique, la e-réputation représente à l'heure actuelle, concomitamment, un vecteur personnel (A) ainsi qu'un vecteur économique (B), participant de conserve à l'édification de l'identité numérique.

A. Un vecteur personnel

À l'ère du tout numérique, l'e-réputation serait le complément de l'identité numérique en ce sens qu'elle participe à la construction de soi sur l'espace du web, et représente l'image et la notoriété numériques de l'individu. Une e-réputation se cultive principalement par la présence sur les réseaux sociaux reliée aux traces et données numériques laissées volontairement et se concrétise, de manière dynamique, lors du traitement et de l'analyse dont l'ensemble fait l'objet. Elle correspond, par conséquent, à la combinaison entre une 'image voulue' et une 'image perçue'.

Dans cette perspective, l'identité numérique évoque la notion de « pulsions scopiques »[450], nommée également « scopophilie » ou « scoptophilie », développée en psychanalyse, désignant un désir de se « faire » voir, un plaisir de regarder. Initiée par Freud, il fonde la pulsion sur des éléments corporels, biologiques, en passant par le désir sexuel, là où pour Lacan il est langagier, linguistique. Or, il y a autre chose que le désir, « *il y a la jouissance et à ce niveau-là justement, on ne peut pas se reconnaître soi-même. À ce niveau-là on n'a pas de partenaire humain que ce soit de l'autre sexe ou du même sexe. Là, il y a une exigence qui est sans relâche, qu'on appelle dans les termes de Freud, la pulsion* »[451]. Cette exigence insatiable sans relâche nécessaire à la pulsion, et ce sans quoi c'est l'angoisse, peut être de nature abstraite se composant de leurres et de semblants. Et ce leurre peut être « *l'objet artistique le plus élaboré ou l'objet technologique le plus récent, et ça c'est pour chacun un partenaire essentiel. Mais il n'est pas humain* »[452]. Ce désir de se « faire » voir comporte un double sens se référant, d'une part, au désir de voir sans être vu ou, inversement, à celui d'être vu pour exister, desquels

---

[450] S. FREUD, *Trois essais sur la théorie sexuelle*, Paris, Ed. Gallimard, 1987, p. 65-68.

[451] J.-A. MILLER, « L'invention du partenaire », École de la cause freudienne, Orientations lacanienne ; et l'auteur rajoute « *Une exigence qui ne s'étanche pas comme la soif, qui ne s'assouvit pas comme la faim, une demande impérative, absolue, qui ne se formule pas en mots mais qui est insatiable, qui en veut toujours plus, qui ne connaît pas de limites ni de temps mort. Elle n'a pas de visage, elle n'a pas de tête, elle est acéphale. Elle n'est pas non plus accrochée à la personne de l'autre, elle ne cherche qu'à s'accomplir, qu'à boucler sa boucle sur elle-même par le moyen de quelque chose qui permette au corps de jouir de lui-même* » : http://www.causefreudienne.net/linvention-du-partenaire/

[452] J.-A. MILLER, « L'invention du partenaire », *Id.*

découlent les traces et données numériques désormais laissées sur le réseau. Ces pulsions trouvent, à l'époque de la révolution numérique, un lieu idéal dans la panoplie de réseaux sociaux disponibles qui instrumentalisent ces parts pulsionnelles en permettant à toute personne de voir et d'être vu, mais aussi de voir sans être vu. La réputation numérique se situe au juste milieu, touchant l'image perçue (le désir de voir) ainsi que l'image voulue (le désir d'être vu). Celle-ci se réfère à la marque, le « *personal branding* », qui est nécessairement subjective et fluctuante. De ce fait, une e-réputation peut s'effondrer aussi rapidement qu'elle est longue à construire et à gérer, à protéger. Ainsi, l'*homo numericus* se trouve confronté à la nécessité d'adopter une démarche managériale en vue de construire son image tout en protégeant son identité.

La technique du *personal branding* vise à mettre en œuvre des stratégies et des pratiques numériques afin de gérer sa marque personnelle en poursuivant un objectif particulier. L'individu adopte alors des techniques de marketing et de communication stratégique pour une promotion personnelle, « *tout comme les entreprises cultivent leur marque, une personne – qu'elle soit étudiante, salariée, entrepreneuse, cadre ou consultante… – a tout intérêt à mettre en place une stratégie de « Personal Branding » adaptée à ses ambitions pour créer sa propre marque, asseoir sa notoriété, gérer sa e-réputation et protéger son identité numérique* »[453]. À l'image de la notion d'identité, le concept d'image revêt une importance grandissante. De ce point de vue, l'image se forme à travers le résultat des informations, volontairement ou involontairement, transmises et perçues.

Selon l'analyse de Kapferer, le concept de l'image est lié à celui de la réception de la communication puisqu'elle traduit la manière dont les individus décodent les signes émis[454]. L'image déclarée, voulue, résulte d'une construction stratégique moyennant des positionnements de marketing, tandis que l'image perçue découle d'une « combinaison entre le réel et le symbolique ». L'aspect réel de celle-ci se compose de facteurs et de paramètres, de fragments figuratifs concrets, alors que le côté symbolique de cette image perçue est rattaché au concept de représentations. L'image est externe correspondant simultanément à une représentation de soi et des autres, mais elle est également interne, propre à chaque personne ou organisation.

[453] « Le Personal Branding, la solution pour construire sa e-réputation », entreprise reputation VIP : https://www.reputationvip.com/fr/blog/le-personal-branding-la-solution-pour-construire-sa-e-reputation

[454] J.-N. KAPFERER, « Maîtriser l'image de l'entreprise : le prisme d'identité », Revue Française de Gestion N° 71 (novembre-décembre 1988), Lavoisier, 1988, p.76-83.

Tout comme le concept de l'identité, elle ne constitue pas une finalité en soi, elle est en mouvance et en fluctuation continue et, comme l'ont souligné Zavalloni et Baugnet, l'identité se manifeste comme une structure organisée des représentations de soi et des autres[455]. Autrement dit, c'est l'ensemble des représentations vécues du rapport entre individu et société, soulignant ainsi l'importance des processus d'inclusion et d'exclusion qui caractérisent les constructions identitaires à partir de l'opposition « Nous-Eux ». Il semble alors qu'existe une unicité entre les notions d'identité et d'image qui, toutes deux, requièrent une gestion et une protection plus pointue, notamment avec les pratiques technologiques qui se manifestent. Les dernières législations en matière de numérique prévoient des dispositions destinées à protéger la réputation et l'identité numériques. En effet, le nouveau RGPD prévoit la question de la réputation en termes de risques pour les droits et libertés des personnes, ou lors d'une violation des données personnelles visant à prévenir, entre autres, d'un traitement « *susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier : lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, [...]* »[456]. L'image et la réputation font partie des éléments composant la notion de vie privée, notion large qui fait l'objet de nombreuses protections par des dispositions « *du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal, qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes* »[457].

Il est évident que les questions entourant l'image et la réputation sont récurrentes dans le monde numérique et la société de l'information actuels qui ont non seulement les capacités de collecter et de traiter toute trace numérique disponible, mais également la capacité de ne jamais oublier alors qu'un individu oublie facilement ; sans compter la capacité de reconstruire et de retracer toutes les traces numériques menant à l'identification et à la connaissance assez détaillée d'une personne physique. Déjà en 1977, les parlementaires avançaient qu'il « *y a le risque énorme, en croyant appréhender un individu par une foule de données disparates, d'avoir de lui une image stéréotypée et contraire à ce qu'il est réellement et à ce qu'il peut devenir* »[458], ce qui peut éventuellement nuire à son image, à sa e-réputation, à sa personne.

---

[455] *Cf.* p. 42 et s.

[456] RGPD, Cons. 75 ; La même formulation se retrouve également au Cons. 85 pour le cas de violation de données à caractère personnel.

[457] Loi Informatique et libertés, Art. 67 modifié par l'article 34 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF n°0141 du 21 juin 2018, texte n° 1.

[458] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *op. cit.*, p. 5786.

Confectionner une image repose sur la reproduction des attitudes observées en s'appropriant les tendances et frustrations du moment vécues. Elle évolue donc en suivant un positionnement marketing soumis aux mutations de l'environnement et aux comportements des tiers. Il s'agit dans ce cadre d'observer et de scruter les différents modes de vie, les idées, les opinions, les pratiques, les comportements, dans le but de produire un nouveau sens en fonction de la personnalité de l'individu et sa manière d'analyser les situations. Un changement de paradigme s'opère dépassant la simple aspiration à une vie privée pour aboutir à un mouvement de « *publicisation de soi* » : il n'est plus simplement question « *d'être « laissé en paix », à l'abri des intrusions, mais aussi de maîtriser son image de soi et sa réputation* »[459].

De nouveaux outils contribuant au façonnement d'une bonne e-réputation voient le jour aux côtés de ceux existants permettant de construire l'image, la réputation à protéger. Twitter[460] constitue ainsi l'outil de diffusion immédiate le plus utilisé aujourd'hui ayant la capacité, en l'espace de quelques secondes, de faire et de défaire une réputation. Google Analytics[461], une branche du courant « Google Marketing Platform »[462], et Google Trends[463] représentent des outils d'analyse des tendances numériques permettant de se faire une opinion sur une personne, un produit ou un service. Quant aux outils propres à l'e-réputation, tels que SocialMention[464], buffer[465], drumUp[466] ou Pipl[467], ceux-ci proposent notamment de rechercher, trouver et analyser, à travers le monde, les traces numériques d'une personne sur le web social et affichent des résultats accompagnés d'analyse par thèmes et par catégories. SocialMention, par exemple, propose des statistiques sur différentes thématiques touchant à la réputation et à la marque personnelle[468] : « *Strength* », la force de probabilité que la marque personnelle d'un individu soit mentionnée sur les réseaux sociaux ; « *Sentiment* » qui est la proportion, le ratio entre les mentions qui sont généralement positives face à celles négatives ou neutres ; « *Passion* » désignant le degré de probabilité que les personnes mentionnant la marque personnelle vont le faire à plusieurs reprises ; et, « *Reach* » qui représente le niveau de l'étendue de l'influence, la portée de l'influence. Ces divers outils contribuent grandement à la construction de l'image voulue, en surveillant et en guidant les individus à travers la collecte et l'analyse des données

[459] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, op. cit.,* p. 10.
[460] https://twitter.com/?lang=fr
[461] https://analytics.google.com/analytics/web/provision/?authuser=0#provision/SignUp/
[462] https://marketingplatform.google.com/about/
[463] https://trends.google.com/trends/?geo=US
[464] http://socialmention.com
[465] https://buffer.com
[466] https://drumup.io
[467] https://pipl.com
[468] http://socialmention.com/search?t=all&q=david+icke&btnG=Search

du web et des images perçues. En effet, ces outils et techniques affermissent les pulsions, les désirs de voir et de se faire voir, tout en accordant la possibilité de voir sans être vu, à travers les résultats affichés.

Face aux avancées technologiques, l'individu semble dorénavant impliqué dans une « négociation de soi » en quête continue de protection de son image, de sa réputation, de son identité numérique. De même, indique le Conseil d'État, « *face à la multiplication des traces laissées en ligne par les individus, qui dessinent une image de la personne accessible à tous les internautes, la volonté de contrôler sa e-réputation se développe* »[469]. C'est cette volonté de contrôle qui a conduit au développement du marché de l'e-réputation et des nombreux outils dorénavant disponibles ; internet et les réseaux permettant, en effet, aux individus de s'exposer et de se mettre en scène quitte à faire spectacle, grâce à l'illusion de liberté totale que procure l'espace du web. Il semble ainsi que l'expérience de vie et la construction d'une personne s'est métamorphosée pour passer au rang de contenu éditorial faisant l'objet de suivi, de recherche, de contribution, de gestion et d'analyse de performance et de visibilité. Comme le note Dubar, « *comment étudier les constructions identitaires personnelles ? Celles-ci, réflexives, narratives, supposent une mise en mots, une mise en récit. Le recours aux sciences du langage et l'analyse du langage sont requis pour cerner les catégories pertinentes de l'expérience, approcher des « mondes vécus » verbalisés, classer, non des personnes, mais des « ordres catégoriels », des univers de croyance, des formes langagières* »[470].

À l'image du modèle de communication de crise[471] adopté par les entreprises, les divers décalages possibles aujourd'hui entre l'image et l'identité ou entre l'image voulue et celle perçue conduisent, dans certains cas, à des situations non crédibles, de crises, imposant en conséquence l'adoption de stratégies et de méthodes de communication de crise, « *crisis communication* »[472]. L'information mal traitée et/ou contradictoire ou erronée, la rumeur non

[469] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, Id.,* p. 68.
[470] C. DUBAR, *La Crise des identités, op. cit.*, p. 207-208.
[471] « *Au sens strict du terme, la communication de crise est constituée de l'ensemble des dispositifs, techniques et actions de communication entreprises pour lutter contre les effets d'un événement (accident, pollution, licenciement, rappel produit…) pouvant avoir des effets négatifs sur l'image de l'organisation concernée ou de ses produits. La communication de crise peut également souvent être entendue dans un sens plus large et comprendre aussi bien des éléments et dispositifs destinés à détecter et anticiper les crises (veille de crise) que les éléments de réponse à ces crises (cellule de crise, site web de crise, ..) relevant du domaine de la communication* », B. Bathelot, « Définition : Communication de crise », du 23/02/2018, Définitions-marketing : https://www.definitions-marketing.com/definition/communication-de-crise/
[472] "*For organizations, crises are pervasive, difficult to keep quiet in today's global multimedia environment; they are challenging, potentially catastrophic; they can even be opportunities for organizations to thrive and emerge stronger. Crises come in many shapes and sizes including media blunders, social media activism, extortion, product tampering, security issues or negligence, just to name a few. […]. Therefore, in order to*

contrôlée ou non démentie, mais aussi la nature et la qualité même de l'image constituent différents facteurs de risques pouvant porter atteinte à la réputation numérique. Sans réponse communicationnelle adéquate, la crise subie peut parfois générer des conséquences majeures et destructrices sur l'image de la personne l'affectant, souvent, dans la vie réelle, quotidienne.
Dès lors, la meilleure stratégie est celle d'intervenir avant l'arrivée de la crise, en amont, nommée aussi la « veille médiatique ou veille médias »[473]. À ce stade, qui n'est pas limité dans le temps et qui peut intervenir à tout moment, intervient alors, l'analyse des risques, appelée en matière de comptabilité le « risque d'audit »[474]. Ces dispositifs et techniques analysent les informations quantitativement et qualitativement, identifiant et évaluant, lorsque c'est le cas, les risques possibles en fonction de leurs sévérités ainsi que leurs effets potentiels sur l'image perçue par les tiers. En même temps, des stratégies et des actions sont envisagées à partir des retours d'expérience et des leçons tirées des crises précédentes. L'*homo numericus* adopte de

understand the field of crisis communication, as a public relations and management function, it is important to focus on the critical factors that affect our understanding of the concept and proliferation of research and practice in the area. There are five critical factors that drive our understanding and research in crisis communication: (1) issues and reputation management as crisis mitigation and prevention, (2) crisis types in a modern global environment, (3) organizational factors affecting crisis response, (4) stakeholder factors affecting crisis response, and (5) response factors to consider in crisis response", A. DIERS-LAWSON, Crisis Communication, *In* H. Giles et J. Harwood (Eds), *The Oxford Encyclopedia of Intergroup Communication*, Leeds Beckett University, Oxford University Press, 2017: http://communication.oxfordre.com/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-397 ; https://audralawson.com/wp-content/uploads/2019/05/DiersLawsonCrisisCommunicationOxfordUniversityPress.pdf

[473] « *L'analyse médiatique va au-delà de la simple veille presse. Aujourd'hui à l'ère de l'information, des réseaux sociaux il faut investiguer des volumes conséquents de données pour en déduire les bonnes recommandations pour action. Le succès de cette veille médiatique dépendra du périmètre de sources, de données et de recherche défini au départ, et sur lequel se baseront les critères à analyser. [...] Une veille médiatique structurée n'est pas un simple état des lieux. Elle doit être constamment enrichie de nouvelles informations issues d'une surveillance en temps réel de multiples canaux d'informations. Les décisions les plus judicieuses sont basées sur des faits et des informations récentes, permettant d'agir au bon moment, au bon endroit vers les bonnes cibles. La veille médiatique permet d'enrichir ces réflexions dans plusieurs domaines* », Veille média : étude des retombées presse sur plusieurs canaux médiatiques, LexisNexis Business Information Solutions : https://bis.lexisnexis.fr/glossaire/veille-mediatique

[474] Dans le cadre de la certification des comptes, « *le risque que le commissaire aux comptes exprime une opinion différente de celle qu'il aurait émise s'il avait identifié toutes les anomalies significatives dans les comptes est appelé « risque d'audit ». Le risque d'audit comprend deux composantes : le risque d'anomalies significatives dans les comptes et le risque de non-détection de ces anomalies. Le risque d'anomalies significatives dans les comptes est propre à l'entité ; il existe indépendamment de l'audit des comptes. Il se subdivise en risque inhérent et risque lié au contrôle. Le risque inhérent correspond à la possibilité que, sans tenir compte du contrôle interne qui pourrait exister dans l'entité, une anomalie significative se produise dans les comptes. Le risque lié au contrôle correspond au risque qu'une anomalie significative ne soit ni prévenue ni détectée par le contrôle interne de l'entité et donc non corrigée en temps voulu.*
Le risque de non-détection est propre à la mission d'audit : il correspond au risque que le commissaire aux comptes ne parvienne pas à détecter une anomalie significative. Le commissaire aux comptes réduit le risque d'audit à un niveau suffisamment faible pour obtenir l'assurance recherchée nécessaire à la certification des comptes. À cette fin, il évalue le risque d'anomalies significatives et conçoit les procédures d'audit à mettre en œuvre en réponse à cette évaluation, [...] », NEP-200. Principes applicables à l'audit des comptes mis en œuvre dans le cadre de la certification des comptes, homologuée par arrêté du 19 juillet 2006 publié au JORF n° 176 du 1er août 2006, texte n° 12, p. 11412.

plus en plus ces attitudes et techniques impactant sa construction et le développement libre de soi, en ce sens que veiller à sa réputation numérique et se préparer pour prévenir les risques de crise ou d'atteinte à son image peut conduire l'individu à adopter d'autres comportements que ceux initialement prévus, façonnant ainsi subtilement sa personnalité, son identité. De la même manière, sa réponse communicationnelle sera subjective, la plupart du temps en réaction instantanée, non-réfléchie, pouvant entraîner d'autres situations de crises.

La technique du « storytelling »[475] s'est mise en place à la suite de l'effet d'usure des réponses factuelles, juridiques ou techniques apportées lors d'une crise. Elle instrumentalise pour sa part un aspect exploité depuis longtemps, mais dont l'étendue de son applicabilité ne fait que croître avec le web social, celui de l'émotion, de l'aspect cognitif, que l'histoire suscite chez son audience. Les histoires diffusées se trouvent amplifiées, non seulement par l'affect, mais surtout par le recours au marketing viral[476], encore appelé « buzz marketing »[477], instauré sur la base du principe qu'une personne intéressée par une annonce va la partager avec son entourage qui, à leur tour, vont la véhiculer, activant ainsi un système de recommandation en amont qui fonctionne suivant le phénomène du bouche-à-oreille, désormais, numérisé.

Toutefois, il est important de relever que les individus sont rarement des professionnels de marketing et de communication stratégiques. Or, le web permet dorénavant à toute personne d'éterniser un vécu, une image, une identité, mais en restituant uniquement des moments de vies sortis de leurs contextes et dénués d'émotions, une histoire morcelée. Il tend dans cette

---

475 "*In human culture, storytelling is a long-established tradition. The reasons people tell stories are manifold: to entertain, to transfer knowledge between generations, to maintain cultural heritage, or to warn others of dangers. With the emergence of the digitisation of media, many new possibilities to tell stories in serious and non-entertainment contexts emerged. A fundamental aspect of storytelling is the emotions, thus cognitive aspects that the story evokes in its audience. One example of why this is important is outlined by Stephen Denning in his book The Leader's Guide to Storytelling, where he shows how he used storytelling to market his projects. […]. By adding storytelling, and creating a personal relationship between his audience and his ideas, he connected with his superiors, and successfully obtained funding for his initiatives [14]. To put it simply: "emotion is the fast line to the brain". […]. There are many other genres that can often contain serious storytelling, such as persuasive marketing, change management, e-learning, psychology, user profiling or serious games*", A. Lugmayr, E. Sutinen, J. Suhonen, C. Islas Sedano, H. Hlavacs & C. Suero Montero, *Serious storytelling - a first definition and review*, *In* Multimedia Tools and Applications 76 (14), January 2017, Springer Science & Business Media New York, 2016, p. 15707-15733.

476 « *Exploitation, au profit d'une marque ou d'une organisation, du bouche-à-oreille sur Internet ou les mobiles, visant à créer une réaction en chaîne* », J. Lendrevie et J. Lévy, *Dictionnaire bilingue Mercator, Tout le marketing à l'ère numérique*, 11ème édition, Dunod, Coll. Livres en or, 2014, p. 575.

477 "*Also called as "BUZZ", a buzz marketing campaign is anything which spreads like a viral among the targeted consumers creating anxiousness and excitement about the product in a positive manner which can lead to trials and generate purchases of the product. It usually involves Word Of Mouth marketing strategy which nowadays is usually done through electronic and digital media such as telephone calls, emails, SMS, Facebook messaging, etc. Research proves that this form of marketing is 10 times more efficient in initiating action than other communications because there is greater credibility of the product when someone who you know refers it rather than getting convinced by the usual television or print advertisements*", Management Dictionary, Marketing and strategy terms, https://www.mbaskool.com/business-concepts/marketing-and-strategy-terms/2030-buzz-marketing.html

perspective à devenir le lieu du faire-croire, du faire-voir et l'espace de la crise communicationnelle. En effet, « *le web est à la fois une formidable mémoire et en même temps une remarquable passoire* »[478].

Constatant ces divers problèmes, les autorités et les institutions juridiques mettent en place progressivement des dispositions destinées à protéger la réputation, au titre du droit à la vie privée, y compris un droit à la rectification ou à la suppression des données[479]. Ainsi, le Pacte international relatif aux droits civils et politiques, adopté initialement par l'Assemblée générale en 1966 et entré en vigueur en 1976, prévoit le droit de toute personne à être protégée contre des « *[…] atteintes illégales à son honneur et à sa réputation* »[480]. Depuis, de nombreuses dispositions protégeant l'honneur et la réputation des personnes ont vu le jour ayant pour but de prévenir contre « *quiconque ayant recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à la réputation ou à la considération de la personne ou à l'intimité de la vie privée […]* »[481]. De même, le Comité des droits de l'homme insistait, dès 1988, sur le fait que les États devraient « *indiquer dans leurs rapports dans quelle mesure l'honneur et la réputation des individus sont protégés par la loi et comment cette protection est assurée dans leur système juridique* »[482]. Au regard de la multiplicité des moyens techniques facilitant les atteintes à l'image, à l'e-réputation, un droit à l'oubli s'est peu à peu instauré, gagnant en légitimité et renforcé par les décisions récentes de la CJUE dans les affaires Google Spain et Schrems[483]. Les juges, dans ces décisions, se penchent sur le droit au déréférencement, à l'oubli numérique, sans le nommer, en affirmant qu'une « *protection efficace et complète des personnes concernées ne pourrait être réalisée si celles-ci devaient d'abord ou en parallèle obtenir l'effacement des informations les*

[478] S. BEN AMOR, L. GRANGET, « L'identité numérique : De la construction au suicide en 52 minutes », Lavoisier, Les Cahiers du numérique 2011/1, Vol. 7, p. 111.
[479] *Cf.* p. 120 et 214.
[480] Pacte international relatif aux droits civils et politiques, Adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale dans sa résolution 2200 A (XXI) du 16 décembre 1966 – Entrée en vigueur le 23 mars 1976, Art. 17.
[481] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *op. cit.*, p. 5793.
[482] Rapport du Comité des Droits de l'Homme, Documents officiels de l'Assemblée générale, quarante-troisième session, Supplément n° 40 (A/43/40), Annexe VI-Observations générales au titre du paragraphe 4 de l'article 40 du Pacte international relatif aux droits civils et politiques, New-York, Nations-Unies, 1er novembre 1988 (trad.), p. 189, point 11.
[483] CJUE, Grande Chambre, Maximillian Schrems c. Data Protection Commissioner, en présence de Digital Rights Ireland Ltd, 6 octobre 2015, affaire C-362/14.

concernant »[484]. Le nouveau RGPD a par la suite codifié, à son article 17, ce droit en le baptisant le droit à l'effacement[485].

In fine, la multiplication des traces numériques et la confusion des sphères privées et professionnelles, en particulier sur les réseaux sociaux, constituent des facteurs susceptibles de produire une image différente, en contraste avec celle souhaitée, nécessitant le recours à des stratégies de *brand content* constituant, *de facto*, le marché de l'e-réputation.

B. Un vecteur économique

Plus les applications et les outils numériques se développent, plus le besoin de recourir à des stratégies de *brand content*, de contenu des marques, augmente ; l'objectif principal étant de focaliser l'attention. Le *brand content* désigne « *les contenus produits plus ou moins directement par une marque dans une logique de marketing des contenus* »[486] ; ceux-ci étant généralement des contenus éditoriaux sur internet, mais qui peuvent prendre la forme de divers autres contenus. C'est donc la mise en place d'une culture de la marque visant à créer des expériences uniques et fortes à connotation positive. Pour ce faire, l'adoption d'une stratégie éditoriale pérenne, qui exprime et traduit l'identité voulue de la marque personnelle, s'avère nécessaire.

Les stratégies de *brand content* servent, entre autres, à réaliser un *storytelling*, à obtenir une visibilité et une notoriété, à affirmer un positionnement ou une expertise particulière. Avec les nouvelles pratiques numériques, les techniques de *brand content* se sont démultipliées, facilitées par la logique du *social publishing*[487] qui, comme son nom l'indique, désigne l'art de publier du contenu sur les réseaux sociaux de façon à accorder aux personnes la possibilité de répondre, de laisser un commentaire ou de donner leur avis, créant à la longue des liaisons, des relations. Des commentaires, des boutons « *like* », « *j'aime* » et leur contraire, des sondages ou encore des *émoticons* permettent, de nos jours, aux internautes d'exprimer une opinion, un avis, un positionnement ou un jugement sur les contenus. En outre, il apparaît que plus la thématique est scandaleuse, autant bénigne soit-elle[488], plus elle suscite des réactions et des réponses. Les

---

[484] CJUE, Affaire Google Spain de 2014, *op. cit.,* point 84.
[485] *Cf.* p. 214.
[486] B. BATHELOT, « Définition : Brand content », Définitions marketing, Glossaires : Publicité média, juin 2017 : https://www.definitions-marketing.com/definition/brand-content/
[487] "*The capability for the masses to accumulate their individually developed content (versus shared development via a wiki) into a usable repository and shared channel for social use and feedback*", Gartner, IT Glossary, https://www.gartner.com/it-glossary/social-publishing
[488] Pour ne citer qu'un exemple, l'histoire de la veste de Melania Trump « I really dont care, Do u ? » lors de sa visite à des migrants au Mexique massivement relayées sur les réseaux sociaux et les médias : https://www.rtl.be/people/buzz/-je-m-en-fiche-completement-la-veste-de-melania-trump-qui-suscite-la-

langues, le langage informatique, les systèmes de signes et d'hypertextes, ou encore les nombreuses institutions sociales et médiatiques, semblent progressivement imposer une vision du monde et influencent les manières de penser. Ces différents dispositifs et outils constituent de plus en plus la mémoire de l'humanité qui, à chaque utilisation, implique l'intelligence collective numérisée. Sauf que ces outils et dispositifs ne constituent pas simplement des mémoires, « *ce sont également des machines à percevoir qui peuvent fonctionner à trois niveaux différents : direct, indirect et métaphorique* », en transformant la nature de nos perceptions, « *[...] notre rapport au monde, et en particulier nos relations à l'espace et au temps, de telle sorte qu'il devient impossible de décider s'ils transforment le monde humain ou notre manière de le percevoir* »[489].

Un marché s'est ainsi mis en place ayant pour ambition principale la gestion de la réputation numérique et pour ennemi, la rumeur ou le risque non contrôlés. L'opinion fluctue et varie en fonction des évènements, utilisés par le traitement informatique et résultant en des messages publicitaires personnalisées. En suivant le processus de persuasion, la variable la plus importante est celle de la réaction, la réponse à l'exécution du message, logique qui se retrouve également dans le marketing viral à travers l'attention suscitée. Divers types de représentations prévalent ainsi dans cette « économie cognitive »[490] que constitue le marché de l'e-réputation et celui indirectement de l'identité numérique, favorisant « *[...] des modes de connaissance distincts (mythe, théorie, simulations), avec les styles, les critères d'évaluation, les "valeurs" qui leur correspondent, si bien que les changements de technologies intellectuelles ou de médias peuvent avoir indirectement de profondes répercussions sur l'intelligence collective* »[491]. Ce nouveau marché propose de nombreux outils et services, fondés suivant une logique de marketing, permettant d'améliorer et de soigner la réputation numérique d'une personne, d'une association, ou d'une entreprise. Des outils ainsi que des entreprises de gestion

stupefaction-1033573.aspx ou https://www.huffingtonpost.fr/2018/06/21/melania-trump-choque-aux-etats-unis-en-portant-cette-veste-zara-lors-dune-visite-a-des-migrants_a_23465143/ & https://www.lemonde.fr/big-browser/article/2018/06/22/provocation-ou-gaffe-la-veste-je-m-en-fiche-de-melania-trump-agite-l-amerique_5319265_4832693.html

[489] P. LÉVY, *Qu'est-ce que le virtuel ?*, Paris, La Découverte, 1998, p. 39.

[490] « *On peut en effet considérer les groupes humains comme des "milieux" écologiques ou économiques dans lesquels des espèces de représentations ou d'idées apparaissent et meurent, se répandent ou régressent, se font concurrence ou vivent en symbiose, se conservent ou mutent. Nous ne parlons pas seulement des idées, représentations, messages ou propositions individuelles, mais bel et bien de leurs espèces : genres littéraires ou artistiques, modes d'organisation des connaissances, types d'argumentations ou de "logiques" en usage, styles et supports des messages. Un* ***collectif humain est le théâtre d'une économie ou d'une écologie cognitive au sein desquels évoluent des espèces de représentations*** » : P. LÉVY, *Qu'est-ce que le virtuel ?*, *Id.,* p. 40.

[491] P. LÉVY, *Qu'est-ce que le virtuel ?, Ibid.,* p. 40.

de la réputation en ligne[492], « *online reputation management* »[493], ont vu le jour proposant leurs services et technologies pour la surveillance, la protection et le nettoyage de la réputation d'un individu ou d'un commerce. À ce titre, *ReputationDefender*, une entreprise de gestion de e-réputation, annonce qu'elle « *utilise une technologie de pointe pour vous aider à créer une communication positive et une image réaliste de qui vous êtes vraiment* »[494]. Nombreuses sociétés sont aujourd'hui spécialisées dans le nettoyage de rumeurs, la gestion et la protection de l'image, l'influence, le noyage des propos négatifs ou encore l'analyse du buzz généré par les marques[495]. L'e-réputation est bel et bien devenu un marché, et un qui devient de plus en plus concurrentiel. De ce fait, même les compagnies d'assurance pénètrent ce marché et commencent à proposer des prestations liées à la gestion et à la protection de l'e-réputation[496]. Ce marché représente, dès lors, un phénomène nouveau ayant une importance économique et des impacts sociaux en croissance.

Il est vrai que la technique de gestion des identités en ligne, adoptée ou non par un individu, a une influence majeure sur la formation et le développement des communautés en ligne, mais aussi sur la fiabilité des informations y circulant. Des communautés, telles que celles présentes sur Amazon[497] ou eBay[498], procèdent activement pour générer des contenus et des informations sur les produits, les services et les vendeurs proposés sur ces plateformes. La plupart du temps, ces informations mènent à des avis ou à des recommandations personnalisés et bien ciblés portant une grande valeur économique. En effet, sur la base des avis et des recommandations générés, les internautes peuvent prendre des décisions plus éclairées, plus informées que ce soit dans l'espace numérique ou physique. En ce sens, l'article 52 de la loi pour une République numérique a inséré un nouvel article dans le Code de la consommation prévoyant que « *toute personne physique ou morale dont l'activité consiste, à titre principal ou accessoire, à collecter, à modérer ou à diffuser des avis en ligne provenant de consommateurs est tenue de délivrer*

[492] Pour illustration : Reputation.com aide les entreprises fonctionnant par établissement à recevoir de meilleures notes et de meilleurs avis sur le web social : https://www.reputation.com/fr/
[493] "*Online reputation management (ORM) is the practice of crafting strategies that shape or influence the public perception of an organization, individual or other entity on the Internet. It helps drive public opinion about a business and its products and services*", Techopedia Dictionary: https://www.techopedia.com/definition/29591/online-reputation-management-orm
[494] https://fr.reputationdefender.com
[495] Pour un exemple d'une société proposant ces divers services pour les particuliers, les personnalités, les collectivités publiques et les entreprises et dirigeants : https://www.votre-reputation.com/particuliers/
[496] Pour illustration : La compagnie d'assurance SwissLife qui désormais propose l'assurance SwissLife e-reputation : https://www.swisslife.fr/Particuliers/Proteger-mes-proches-et-maintenir-mes-revenus/Proteger-ma-famille/E-reputation
[497] Votre Communauté Amazon : https://www.amazon.fr/gp/help/customer/display.html/?nodeId=201929990
[498] Communauté eBay : https://communaute.ebay.fr

aux utilisateurs une information loyale, claire et transparente sur les modalités de publication et de traitement des avis mis en ligne »[499]. Le législateur fixe ainsi une obligation d'information loyale relative à la qualité des avis publiés en ligne, tout en prévoyant un processus de contrôle et de vérification des avis émis. L'enjeu que revêt la fiabilité des avis en ligne est par conséquent majeur, autant du côté des consommateurs que de celui des entreprises en ligne. Les sites postant des avis doivent dorénavant indiquer explicitement si leur publication a fait l'objet de contrôle et de vérification, en affichant les caractéristiques principales de la procédure mise en œuvre. Ils sont également tenus d'informer les internautes, clairement et en toute transparence, des modalités de publication des avis publiés ainsi que des modalités de leurs traitements.

De juillet 2013 et jusqu'à septembre 2018, existait en France la norme Afnor[500], d'application volontaire, relative aux principes et aux exigences portant sur les processus de collecte, de modération et de restitution des avis en ligne des consommateurs. Première norme au monde portant sur les modalités de traitement des avis des consommateurs en ligne, elle permettait aux entreprises d'assurer la fiabilité et la transparence des processus de collecte des avis en ligne, leur modération, ainsi que leur restitution. Néanmoins, dans le corpus mis en place pour la vérification des avis, « *l'ambiguïté qui existe entre les notions d'acte d'achat et d'expérience de consommation démontre les difficultés à transcrire de manière générale un système permettant de procéder à la vérification des avis mis en ligne* »[501]. De plus, la norme ne fait que certifier le processus et non le contrôle des avis déposés. Ainsi, la DGCCRF a eu l'occasion de prononcer, en 2015, 21 avertissements et 11 injonctions, ainsi que de dresser 3 procès-verbaux sur les 261 opérations de contrôle effectuées[502]. Dans la plupart des cas, la qualification

---

[499] Loi pour une République numérique, Art. 52, « *Le livre Ier du code de la consommation est ainsi modifié : 1° Après l'article L. 111-7, il est inséré un article L. 111-7-2 ainsi rédigé :* « *Art. L. 111-7-2. - Sans préjudice des obligations d'information prévues à l'article 19 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et aux articles L. 111-7 et L. 111-7-1 du présent code, toute personne physique ou morale dont l'activité consiste, à titre principal ou accessoire, à collecter, à modérer ou à diffuser des avis en ligne provenant de consommateurs est tenue de délivrer aux utilisateurs une information loyale, claire et transparente sur les modalités de publication et de traitement des avis mis en ligne. Elle précise si ces avis font ou non l'objet d'un contrôle et, si tel est le cas, elle indique les caractéristiques principales du contrôle mis en œuvre. Elle affiche la date de l'avis et ses éventuelles mises à jour. Elle indique aux consommateurs dont l'avis en ligne n'a pas été publié les raisons qui justifient son rejet. Elle met en place une fonctionnalité gratuite qui permet aux responsables des produits ou des services faisant l'objet d'un avis en ligne de lui signaler un doute sur l'authenticité de cet avis, à condition que ce signalement soit motivé* ».

[500] AFNOR Éditions, NF Z74-501 Juillet 2013 – Annulée le 22/09/2018, Avis en ligne de consommateurs - Principes et exigences portant sur les processus de collecte, modération et restitution des avis en ligne de consommateurs : https://www.boutique.afnor.org/norme/nf-z74-501/avis-en-ligne-de-consommateurs-principes-et-exigences-portant-sur-les-processus-de-collecte-moderation-et-restitution-des-avi/article/808897/fa178349

[501] Projet de loi pour une République numérique – Étude d'impact, 9 décembre 2015, Dossiers législatifs de l'Assemblée Nationale, Section 4 Information des consommateurs, p. 91.

[502] Direction générale de la concurrence, de la consommation et de la répression des fraudes - DGCCRF, Enquête Communications électroniques : une surveillance attentive du marché, https://www.economie.gouv.fr/dgccrf/communications-electroniques-surveillance-attentive-marche

retenue était la pratique commerciale trompeuse[503]. Comme a pu le souligner Dubar, *a priori*, l'individu ne peut plus accorder sa confiance à telle ou telle organisation, il lui « *faut donc trouver en soi des raisons de choisir tel ou tel "représentant", tel ou tel programme, telle ou telle option. Mais sur quelle base ?* »[504].

Se manifeste alors d'autres enjeux complémentaires : la sécurité des données mais surtout la confiance numérique accordée qui fait aujourd'hui l'objet d'une loi en France, celle relative à la confiance dans l'économie numérique[505]. La question des avis en ligne réitère cette question de confiance et acquière une place de plus en plus dominante, hégémonique. Fin 2014, l'IFOP, en partenariat avec l'agence Reputation VIP (précitée), a effectué un sondage analysant l'impact de l'e-réputation sur le processus d'achat à travers lequel elle montre que « *l'e-réputation peut constituer une force de frappe dissuasive à l'achat* »[506].

Le web s'impose ainsi comme un vecteur d'information incontournable pour les internautes dans la mesure où, en 2014, 80% des individus ont eu recours à internet pour des avis et des renseignements concernant un produit ou un service. Préalablement à l'achat en ligne, 88% des individus consultent les avis d'autres consommateurs, les forums ou les blogs, et 73% suivent la même pratique pour un achat en boutique. Dans le cas des achats en ligne, des avis négatifs sur un site ou un forum étaient de nature à dissuader plus de 80% des individus de réaliser l'achat prévu. D'un autre côté, « *75% des français estiment que certains des avis sont faux* »[507].

Il est donc évident que les évènements se produisant en ligne ont un impact dans la vie quotidienne, physique, et ce même à l'extérieur du seul domaine de commerce électronique. Les sites de rencontre en ligne[508] par exemple, de plus en plus nombreux, permettent aux individus d'avoir un premier contact en ligne au préalable d'une rencontre physique éventuelle. D'un autre point de vue, une différence d'opinion lors d'une rencontre physique peut également

---

[503] Art. L. 121-2 Code de la consommation : « *Les agents de la concurrence, de la consommation et de la répression des fraudes, ceux de la direction générale de l'alimentation du ministère de l'agriculture et ceux du service de métrologie au ministère de l'industrie sont habilités à constater, au moyen de procès-verbaux sur l'ensemble du territoire national les pratiques commerciales trompeuses. Ils peuvent exiger du responsable d'une pratique commerciale la mise à leur disposition ou la communication de tous les éléments propres à justifier les allégations, indications ou présentations inhérentes à cette pratique, y compris lorsque ces éléments sont détenus par un fabricant implanté hors du territoire national. Ils peuvent également exiger de l'annonceur, de l'agence de publicité ou du responsable du support la mise à leur disposition des messages publicitaires diffusés* ».

[504] C. DUBAR, *La Crise des identités, op. cit.,* p. 161.

[505] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[506] Institut d'études Opinion et Marketing en France et à l'international, L'impact de l'e-réputation sur le processus d'achat – Sondage Ifop pour Réputation VIP, décembre 2014 : https://www.ifop.com/wp-content/uploads/2018/03/2968-1-study_file.pdf & https://www.reputationvip.com/fr/blog/sondage-ifop-reputation-vip-linfluence-de-le-reputation-sur-lacte-dachat

[507] Projet de loi pour une République numérique – Étude d'impact, *Id.,* p. 92.

[508] Quelques exemples : https://www.meetic.fr , https://www.edarling.fr/conseils-rencontres/site-de-rencontre ou https://www.hugavenue.com

avoir un impact négatif sur l'individu puisqu'elle aura tendance à se répercuter et ressortir dans le monde numérique. Parallèlement, des messages ou des photos échangés sur Facebook Messenger, entre autres, peuvent entraîner des conséquences, parfois majeures, sur la vie privée des personnes. En effet, malgré le fait que les atteintes à la réputation peuvent être qualifiées de « petits litiges », « *leurs enjeux sont parfois significatifs pour les personnes concernées mais les intérêts pécuniaires en cause sont le plus souvent limités* »[509]. Par ailleurs, une rencontre physique est de plus en plus fréquemment précédée d'une prise de contact virtuelle, pratique qui touche nombreux domaines tels que l'accès à l'assurance, à un crédit, ou même à l'emploi. Des avis ou caractéristiques négatifs, défavorables, peuvent conduire à restreindre l'accès voire même à l'interdire.

De nos jours, la large production et dissémination des données personnelles mène à la croissance des risques : que ce soit la masse d'informations qui apparaît dès que le nom d'une personne est inséré dans la barre de recherche, ou celles qui figurent déjà dans les bases de données des acteurs en cause, elles font toutes l'objet de traitements produisant des avis favorables ou défavorables[510]. Selon une enquête du Sénat américain, « *les assureurs et les employeurs sont ainsi parmi les premiers acquéreurs des données détenues par les data brokers ; ils peuvent aussi s'intéresser aux données en ligne sur les réseaux sociaux* »[511]. Par conséquent, un signal négatif peut être directement déduit, un épisode professionnel antérieur négatif peut déterminer l'accès ou non à l'emploi par exemple, mais l'ensemble est souvent déduit des corrélations statistiques : Derwent Capital[512] à Londres et MarketPsych[513] en Californie, deux fonds spéculatifs, ont, à ce titre, commencé à analyser des textes de tweets transformés en données, des « *datafied text* », comme signaux pour l'investissement en bourse en appliquant la technique du *Sentiment Analysis*, du *Social Media Data for Sentiment Analysis* susmentionnée ; les deux entreprises vendent aujourd'hui ces informations à des négociants et des opérateurs commerciaux[514]. Reconnaître et cibler l'identité d'un individu ainsi que sa e-réputation s'avèrent être, en outre, de plus en plus essentiels dans le cadre des recrutements ; le développement de sites de réseaux professionnels, tels que LinkedIn[515], ne fait qu'en témoigner.

[509] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, op. cit.,* p. 28-29.
[510] *Cf.* p. 380 et s., p. 430 et s.
[511] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, Id.,* p. 161.
[512] https://www.linkedin.com/company/derwent-capital-markets-ltd- & https://www.fnlondon.com/articles/twitter-derwent-capital-hedge-fund-20110815
[513] https://www.marketpsych.com
[514] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data, op. cit.,* p. 92-93.
[515] https://www.linkedin.com

L'utilisation et l'exploitation exponentielle des données par les entreprises montrent, par ailleurs, l'influence que cela peut entraîner dans la manière dont les gens gèrent leurs identités. Il est évident que, dans un environnement de confiance, les internautes seront plus prêts à céder leurs informations et données personnelles moyennant des services personnalisés et des offres adaptées à leurs besoins et envies. Ces informations caractérisent plusieurs enjeux considérables dont, dans cette perspective, un risque pour leurs réputations et leurs intérêts en cas de mauvaise protection de leurs données ou de problème de sécurité informatique. Les nouvelles réglementations en la matière, en particulier le RGPD, tentent d'apporter des solutions et préconisent vivement le recours à des « *mesures techniques et organisationnelles appropriées* »[516] pour garantir la protection et la sécurité des données personnelles et des équipements informatiques[517], tels que les principes de protection des données dès la conception et de protection des données par défaut[518].

L'e-réputation, complément de l'identité numérique, représente ainsi un vecteur économique, un marché de marketing et de gestion portant divers enjeux : la protection des données, la sécurité informatique, la confiance numérique, la loyauté informationnelle, la transparence des avis et recommandations ; tous contribuant de manière dynamique et continue à la construction et au maintien de l'e-réputation. Comme il a été précédemment noté, il existe à l'ère du tout numérique, un paradoxe entre l'usage et la confiance numérique, également aperçu par la CNCDH dans son avis de 2018 dans lequel elle relève qu'il est « *frappant de constater que l'espace emblématique du "partage" d'éléments de sa vie privée, les réseaux sociaux, n'inspire pas confiance* »[519].

---

[516] RGPD, Cons. 78 « *[…]. Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer. Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données* ».

[517] RGPD, Cons. 39 « *[…] Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement* ».

[518] Respectivement, les équivalents du concept de *Privacy by design* et celui de *Privacy by default*.

[519] CNCDH, *Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, op. cit.,* p. 4, point 14.

Les masses de données ainsi produites font, par la suite, l'objet de traitements et d'analyses afin de leur accorder une parole significative, porteuse de valeur, induisant *in fine* le développement de l'économie des données.

Section 2 – Une valeur verticale : la parole des masses de données

La valeur verticale de l'identité numérique se manifeste, pour sa part, par la parole donnée aux masses de données produites, caractérisant par conséquent la nouvelle économie des données qui voit le jour : économie qui incarne en soi une source de croissance (§1), mais aussi une source à diverses tendances (§2).

§1. L'économie des données : une source de croissance

Cette nouvelle source de croissance que représente l'économie des données procède d'une étude de la chaîne de valeurs de la donnée personnelle (A), permettant d'aboutir, entre autres, à un modèle économique personnalisé et réussi (B).

A. Une nouvelle chaîne de valeurs

Avec les nouvelles technologies de l'information et de la communication, toute donnée peut être analysée en suivant l'approche du cycle de vie du produit, dite PLC[520] (Product Life Cycle). Dans cette perspective, chaque donnée personnelle a un cycle de vie allant de son recueil, sa collecte, jusqu'à son utilisation ou sa suppression. Un examen des « *value chains* »[521] permet d'identifier le rôle des différents acteurs, et met en évidence des domaines d'activité de marché améliorant la valeur pécuniaire des données. De même, cela aide à fournir un aperçu général de l'activité de la chaîne et à localiser des domaines potentiels méritant d'être envisagés de plus

[520] "*Among the contingent theories of strategic management, the product life cycle approach (PLC) holds a leading position. According to the PLC theory (Buzzell 1966; Clifford 1977; Cox 1967; Dhalla and Yuspeh 1976; Doyle 1976; Levitt 1965; Wright 1971) different strategies are adopted at the various phases of a product life. Specifically, a leadership strategy is adopted at the introduction and growth phases and is then followed by the niche strategy at the maturity stage. Finally, when decline sets in, a harvest strategy is implemented. Over the years the PLC model as a tool for strategic planning has been modified. However, its basic premise- that a given set of strategic actions is associated with each stage-still remains. In representing the evolution of the product through time, the PLC approach can be used prescriptively for allocating efforts and resources among different activities of the multibusiness firm*", R. A. Thietart and R. Vivas, "An Empirical Investigation of Success Strategies for Businesses along the Product Life Cycle", Management Science, Vol. 30, N° 12, Décembre 1984 (p. 1405-1423), p. 1405.

[521] "*Value chains are an integral part of strategic planning for many businesses today. A value chain refers to the full life cycle of a product or process, including material sourcing, production, consumption and disposal/recycling processes*", Collaboration, innovation, transformation: Ideas and inspiration to accelerate sustainable growth - A value chain approach, World Business Council for Sustainable Development (WBCSD), Décembre 2011, p. 3.

près par les législateurs. Le concept de « chaîne de valeur » introduit par M. Porter en 1985[522], se réfère au cycle de vie complet d'un produit ou d'un service. Il désigne l'étude spécifique des activités d'une entreprise pour mettre en évidence ses activités phares, celles qui ont un impact réel en termes de profit ou de qualité lui fournissant un avantage concurrentiel. Cette étude permet ainsi de savoir où se positionner et de travailler ce positionnement pour développer de la valeur ajoutée. En effet, « *value chain analysis is a method for decomposing the firm into strategically important activities and understanding their impact on cost behavior and differentiation* »[523].

En explorant la chaîne de valeur des données personnelles, l'accent est mis sur la manière dont les données personnelles sont porteuses d'innovation qui se traduit sous forme de nouveaux produits et services, de gains d'efficacité dans l'application du processus, de nouvelles méthodes et techniques d'analyses, mais aussi de création de valeur tant pour les entreprises que pour les utilisateurs. Ces chaînes de valeurs sont mises en contexte en examinant les façons spécifiques d'utilisation des données personnelles dans divers secteurs de l'économie. L'application des règles relatives à la protection de la vie privée peut, cependant, avoir une incidence sur l'étude de la chaîne de valeur, et peut varier d'un pays à l'autre, et même entre différents secteurs d'un même pays.

La collecte des données personnelles s'opère de manière différente : elles peuvent être volontairement offertes ou cédées par les individus lors du partage explicite d'informations les concernant ou touchant des tiers, à l'exemple des informations bancaires fournies pour un achat en ligne, ou celles accordées lors de la création d'un profil sur un réseau social ; les données peuvent être également observées et saisies en enregistrant les activités des utilisateurs, contrairement aux données transmises volontairement, tels que les préférences de navigation, ou encore le comportement suivi en matière de communications téléphoniques. Par ailleurs, les données personnelles peuvent provenir des déductions et inférences articulées sur la base d'un traitement des données, à l'exemple des cotations de crédit, les *credit scores*, permettant d'accorder un avis favorable ou défavorable à une personne demandant un crédit. De plus, les

---

[522] M. E. PORTER, *Competitive Advantage: creating and sustaining superior performance*, The Free Press, New York, 1985, p. 11-15: "*The idea of the value chain is based on the process view of organisations, the idea of seeing a manufacturing (or service) organisation as a system, made up of subsystems each with inputs, transformation processes and outputs. Inputs, transformation processes, and outputs involve the acquisition and consumption of resources - money, labor, materials, equipment, buildings, land, administration and management. How value chain activities are carried out determines costs and affects profits. Most organisations engage in hundreds, even thousands, of activities in the process of converting inputs to outputs. These activities can be classified generally as either primary or support activities that all businesses must undertake in some form*".

[523] M. HERGERT et D. MORRIS, "Accounting Data for Value Chain Analysis", Strategic Management Journal, Vol. 10, N° 2, Mars - Avril 1989 (p. 175-188), p. 177.

données personnelles peuvent être déduites à travers l'analyse de plusieurs traces de données disparates qui, initialement, ne permettent pas de faire un lien direct avec la personne.

Chaque type de donnée personnelle, qu'elle soit offerte, cédée, saisie ou déduite, est initialement collecté ou consulté puis sauvegardé, agrégé, corrélé, traité et analysé et enfin utilisé. Chacune de ces étapes, nous informe l'OCDE, présente des caractéristiques particulières susceptibles de faire intervenir plusieurs acteurs différents[524]. Selon l'étude de l'OCDE sur l'économie des données personnelles, « *the personal data lifecycle can be presented as following a four-step value chain* »[525] : la collecte ou l'accès, la sauvegarde et l'agrégation, l'analyse et la distribution et enfin, l'utilisation.

Ces quatre étapes constituent ainsi le cycle de vie d'une donnée personnelle impliquant une variété d'acteurs différents, tels que des individus, des institutions publiques ou privées ou encore des ONG, jouant chacun un rôle différent. En ce sens, les courtiers en données, les « *Data brokers* », n'utilisent généralement pas les données personnelles mais les traitent et les vendent plutôt. Néanmoins, certaines parties prenantes de la chaîne de valeur peuvent être impliquées dans toutes les étapes de celle-ci leur permettant, à terme, de les utiliser pour le développement de leur propre modèle économique personnalisé[526]. Par ailleurs, l'OCDE observe que les frontières entre les données offertes, cédées, saisies et inférées ne sont pas claires, « *what is volunteered, surrendered and observed has a major impact on what is inferred, and what is volunteered and surrendered is often inaccurate* »[527].

La collecte des données à caractère personnel ou la possibilité d'y accéder, dans le respect des normes en vigueur, présente la première étape de ce processus qui couvre plusieurs secteurs de l'économie et, de façon générale, une large variété de sources. Avec l'intensification de la quantité et du volume des données mises à disposition sur le web, cette étape s'est largement transformée, permettant de collecter des informations plus variées et détaillées et ce, de manière directe ou indirecte. En effet, les opérateurs de réseaux ont, de nos jours, des données de plus en plus détaillées sur leur abonnés, y compris des données de géolocalisation ; les entreprises collectent une large quantité d'informations personnelles sur leurs employés (exemple de Zest

---

[524] OECD, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, N° 220, OECD Publishing, Paris, 2013, p. 10. http://dx.doi.org/10.1787/5k486qtxldmq-en

[525] OECD, "Exploring the Economics of Personal Data", *Id.*, p. 35; et l'organisation précise qu'il existe une dernière étape dans la chaîne de valeur, la suppression des données : "*The final step in the personal data life cycle is disposal, which is a fundamental aspect of the protections related to privacy and information security. It is not included as part of this discussion, however, because it does not offer obvious contributions to the value chain*" (Endnotes).

[526] *Cf.* p. 142.

[527] OECD, "Exploring the Economics of Personal Data", *Id.,* p. 11.

Finance), y compris les mails, logins ou les réseaux d'intérêts particuliers ou professionnels et ainsi de suite. Dans certains cas, les données personnelles sont collectées de manière indirecte, induisant *de facto* la création de nouveaux modèles économiques.

La collecte des données, en elle-même, implique dorénavant une grande variété d'activités comme les techniques de recensement et d'enregistrement des données de localisation des adresses IP, les « *Internet location information* », destinées à être utilisées dans les contenus et services de livraison en fonction de sa pertinence vis-à-vis des utilisateurs localisés à un endroit précis. Ces informations de localisation recensées repèrent la géolocalisation précise de l'adresse IP de l'internaute en fournissant le pays, la ville, la région, le numéro complet de l'adresse, ainsi que les données de localisation en longitude et en latitude[528]. Au regard du fait que les technologies de réseaux rendent la traçabilité des objets et des personnes faisables dans une large variété d'activités, de nouveaux modèles économiques se sont progressivement mis en place. Ceux-là, explique l'OCDE, ont tendance à se concentrer sur une meilleure compréhension des consommateurs individuels afin de leur fournir des services et des produits personnalisés, de réduire les recherches de consommateur et les frais de transaction, mais aussi afin d'augmenter l'efficacité des fournisseurs et prestataires de service, qu'ils soient du secteur public ou privé[529].

D'un autre côté, au lieu qu'elles soient saisies, les données peuvent être créées par le biais d'une analyse comprenant, par exemple, le développement des profils, goûts et préférences à partir des activités en ligne qui pourront être subséquemment utilisés dans les offres et ciblages publicitaires.

À partir du moment où une donnée est collectée, elle fait l'objet d'une sauvegarde et d'une agrégation, caractérisant la deuxième étape d'une chaîne de valeurs des données. Les éléments de données distincts sont organisés et stockés dans des fichiers et des séries de données pouvant être ultérieurement exploités pour des traitements et des analyses supplémentaires. Comme il a été sus-indiqué, l'agrégation des recommandations faites par les internautes peut constituer le

---

[528] C'est ce que fournit, par ex., l'entreprise IP Location, qui explique l'utilité de collecter les données de géolocalisation des adresses IP en affirmant ainsi « *Pairing of IP address to a geographical location is called geolocation. There are times when you need to identify where your web visitors are coming from. You might have an ecommerce website, and would like to know where your potential customers are, pre-populate country code on forms, display different language and reduce credit card fraud based on geographic location. Or, you might want to fight against illegal spammers and hackers, and would like to locate source of a problem* », https://www.iplocation.net . Pour un autre exemple: https://www.ip2location.com

[529] OECD, "Exploring the Economics of Personal Data", *Id.,* p. 12 – Traduction libre: "*As network technologies make the tracking of things and people across a wide range of activities feasible, new business models have emerged. These tend to focus on understanding individual consumers better in order to provide tailored products and services, to reduce consumer search and transaction costs and to increase the efficiency of suppliers and providers, be they private or public sector entities*".

fondement de nouveaux services dans la mesure où elle peut servir à établir une confiance nécessaire pour l'utilisation du service, tel que les nouveaux services de covoiturage par exemple. À ce stade, la question est de savoir comment agréger les données entre elles, « *de la manière la plus juste et la plus efficace possible et créer un Data-Frame sur lequel les algorithmes pourront « apprendre »* »[530]. Les données à regrouper étant de natures si différentes et variées, cela nécessite le recours à plusieurs procédures d'agrégation. De plus en plus, les données personnelles se situent au centre du processus d'information représentant, *in fine*, des mesures ou des observations d'attributs ou de variables économiques ou sociales. La fonction d'agrégation des données s'applique à l'intégralité de cet ensemble de variables mis en relation, suivant différentes mesures et appréciations ayant pour résultat la production d'une valeur unique synthétique, telle qu'une chaîne ou un groupe présentant des caractéristiques communes. Il est alors possible d'agréger les données par caractéristiques, par position géographique ou par temps. L'agrégation des données ou « *data aggregation* »[531], désigne le processus par lequel des données brutes sont recueillies puis traduites, de manière succincte, sous une forme synthétique pour des analyses statistiques.

En effet, de nombreuses données personnelles, comme les informations bancaires, le numéro de compte ou les informations de connexion détaillées sont stockées par un grand nombre de prestataires de services tels que les fournisseurs d'accès à internet (FAI) et opérateurs de réseaux mobiles, les commerçants, les médecins ou encore les services publics et organismes gouvernementaux. Parallèlement, les contenus générés et transmis par les utilisateurs sont également stockés par plusieurs fournisseurs de services et de contenus, y compris les réseaux sociaux et professionnels, les blogs, les plateformes de partage de contenus, mais aussi les fournisseurs de service de messagerie électronique. Il est important de noter, dans ce cadre, qu'en raison du gain potentiel d'efficacité en termes de rentabilité des dépenses, les données personnelles et structurelles, d'organisation, sont de plus en plus enregistrées à distance et accessibles en ligne. Ceci s'explique notamment par l'accroissement des services de stockage

[530] Etic Data, « Enrichissement de données : les 3 méthodes d'agrégation », France : https://etic-data.com/methodes-agregation-donnees/

[531] "*Data aggregation is a type of data and information mining process where data is searched, gathered and presented in a report-based, summarized format to achieve specific business objectives or processes and/or conduct human analysis. Data aggregation may be performed manually or through specialized software. Data aggregation is a component of business intelligence (BI) solutions. Data aggregation personnel or software search databases find relevant search query data and present data findings in a summarized format that is meaningful and useful for the end user or application. Data aggregation generally works on big data or data marts that do not provide much information value as a whole. Data aggregation's key applications are the gathering, utilization and presentation of data that is available and present on the global Internet*", Techopedia Dictionary: https://www.techopedia.com/definition/14647/data-aggregation

en ligne assorti d'une réduction du coût des bites des données, comme le service du *cloud computing*, de l'informatique en nuage[532].

Ainsi, les données sont stockées et agrégées par différents acteurs de la chaîne de valeur des données pour, ensuite, faire l'objet de combinaison avec d'autres données dans le but de mettre au point, de façon détaillée, des profils et des dossiers numériques ainsi que des macros tendances pouvant être utilisées, et servir diverses fins aussi disparates et variées que les données le sont. Un élément clé de la valeur rajoutée, à ce niveau, est la fusion des données de sources différentes avec les profils établis, et le recours à des logiques et des moyens analytiques d'analyses pour inférer et déduire des informations qui, autrement, feront défaut. Vers le XVII^{e} Siècle, un anglais du nom de J. Graunt[533] eut l'idée originale d'élaborer une approche qui, au lieu de compter chaque citoyen, lui permettait de déduire, d'inférer, le nombre de la population à Londres au moment de l'épidémie[534]. Son approche, qualifiée à notre époque de statistiques, a créé l'idée qu'il est possible d'extrapoler, à partir d'un petit échantillon, des connaissances utiles concernant la population en général.

Ces sources différentes de données comprennent, *inter alia*, des bases de données accessibles au public, des données exclusives, privées, détenues par les entreprises ou même des données de la recherche institutionnelle. Et l'OCDE relève, à ce propos, que « *the possibility of such aggregation present unprecedented opportunities for drawing unique insights, creating tremendous opportunities for new products and services* »[535]. Il faut également noter que les données peuvent faire l'objet de plusieurs cycles d'analyse et de distribution, au cours desquels des données supplémentaires vont être créées et inscrites à chaque itération. Les informations combinées pour établir des profils personnels plus raffinés, souvent revendus, représentent une importante source de données impactant, *a fortiori,* la valorisation des données personnelles.

Par ailleurs, la valeur des données constitue un des critères employés pour l'analyse des Big data. Ainsi, pour les entreprises, cette chaîne de valeur, composée de quatre étapes, a la capacité de s'intégrer dans l'analyse plus générale des masses de données constituée, pour sa part, de cinq critères d'étude. En effet, « *pour certains d'entre eux, il s'agit de valoriser les données*

---

[532] *Cf.* p. 112 et s.

[533] John Graunt (1620-1674), mercier anglais, est considéré par beaucoup d'historiens comme étant l'un des premiers démographes et le pionnier de la science des statistiques ; pour plus d'information : J.-M. Rohrbasser, « John Graunt et les bulletins de Londres : une statistique de la mortalité au XVIIe siècle », Dix-septième siècle, Vol. 243 N° 2, PUF, 2009, p. 345-368 & B. Benjamin, "John Graunt's "Observations" (reprint of the first edition), Journal of the Institute of Actuaries 90, ed. 1964, p. 1–61.

[534] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data, op. cit.,* p. 21.

[535] OECD, "Exploring the Economics of Personal Data", *Id.,* p. 13.

des utilisateurs à des fins publicitaires, et pour d'autres d'analyser ces données afin d'établir de nouveaux services à valeur ajoutée »[536].

En ce sens, l'ouverture des données publiques, l'Open data, représente un mécanisme de génération de valeur lié à l'utilisation par les secteurs public et privé de ces données afin de créer de nouveaux produits et services ; le tout en réduisant les frais de transaction. L'ouverture des données météorologiques aux Pays-Bas a, par exemple, induit le développement d'un nouvel écosystème de réutilisations professionnelles d'informations du secteur public (PSI-Public Sector Information) très dynamique, menant à une augmentation de 400% des revenus des acteurs privés, de 300% du nombre de ré-utilisateurs de ces données et même de plus de 35 millions d'euros en termes d'impôts et taxes provenant des déclarations de revenus des sociétés[537]. De même, nombreuses études européennes présentent l'intérêt d'établir une chaîne de valeur des PSI[538], et soulignent qu'une baisse de redevance, ou sa suppression intégrale, entraîne automatiquement une augmentation de la réutilisation des données en question[539]. Suivant la même logique, l'ouverture des données est génératrice de valeur grâce à une réduction de l'asymétrie d'information[540] réalisée à travers une plus grande transparence. Ainsi, « *du point de vue du développement économique, les données des SPIC ont une valeur certaine, puisqu'elles touchent à des services essentiels utilisés par l'ensemble de la population* »[541].

Plusieurs exemples démontrent que les données ont un rôle de plus en plus majeur dans la création de valeur économique et sociale. En France, poursuivant l'objectif de modernisation de l'action publique, la fonction d'administrateur général des données a été créée par décret en 2014[542]. Celui-ci « *coordonne l'action des administrations en matière d'inventaire, de gouvernance, de production, de circulation et d'exploitation des données par les administrations. Il organise, dans le respect de la protection des données personnelles et des*

---

[536] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 7.

[537] M. DE VRIES, « Re-use of public sector information – Catalogue and highlights of studies, cases and key figures on economic effects of changing policies », Report for Danish Ministry for Housing, Urban and Rural Affairs, Copenhagen, The Hague 11 août 2012, p. 18; disponible en ligne: https://gst.dk/media/2915639/reuse-of-public-sektor-information.pdf

[538] G. VICKERY, « Review of Recent Studies on PSI Re-Use and Related Market Developments », Report for the European Commission in the context of the forthcoming review of the PSI Directive, 2010, p. 13-14, disponible en ligne: https://ec.europa.eu/digital-single-market/en/news/review-recent-studies-psi-reuse-and-related-market-developments

[539] G. VICKERY, « Review of Recent Studies on PSI Re-Use and Related Market Developments », *Id.*, p. 22-28.

[540] « *Il y a asymétrie d'information quand un acteur possède une information plus complète, ou de meilleure qualité, que les autres acteurs participant à une transaction ou une communication. Cela aboutit à des situations non optimales. Les données ouvertes permettent de réduire ces asymétries à plusieurs niveaux* », Projet de loi pour une République numérique – Étude d'impact, *op. cit.,* p. 16.

[541] Projet de loi pour une République numérique – Étude d'impact, *Id.,* p. 22.

[542] Décret n° 2014-1050 du 16 septembre 2014 instituant un administrateur général des données, JORF n° 0215 du 17 septembre 2014, texte n° 2.

secrets protégés par la loi, la meilleure exploitation de ces données et leur plus large circulation, notamment aux fins d'évaluation des politiques publiques, d'amélioration et de transparence de l'action publique et de stimulation de la recherche et de l'innovation »[543].

Après que les données ont fait l'objet de collecte, d'agrégation et de stockage et d'analyse, elles sont souvent mises sur le marché pour les utilisateurs finaux, concrétisant, par conséquent, la dernière étape de la chaîne de valeur. Ceux-ci acquièrent généralement les profils des individus (certains vont jusqu'à acheter les sociétés les produisant) en vue de compléter et d'enrichir leurs propres activités commerciales. Si ces transactions pouvaient être évaluées, souligne l'OCDE, « *they can provide into how highly the market values the personal data* »[544].

B. Un modèle économique personnalisé

Les données numériques, notamment celles à caractère personnel, constituent une ressource fondamentale dans le secteur économique, les exemples de Google ou de Facebook n'étant que deux parmi tant d'entreprises démontrant l'efficacité actuelle de la valorisation systématique des données recueillies. À la suite de l'établissement des chaînes de valeurs des données et l'affinement des profils et dossiers personnels, la question fondamentale qui se pose pour les entreprises est celle de déterminer la manière d'intégrer et de valoriser cette masse de données pour créer ou renforcer leur modèle économique. Dans ce contexte, ce sont particulièrement les multiples possibilités d'analyse des informations que représentent les données, plus que les seules caractéristiques du Big data, qui deviennent progressivement l'enjeu stratégique entourant l'économie des données.

En matière de marketing, il semble que « *nous sommes en train de passer d'un modèle classique de segmentation à un modèle de caractérisation comportementale grâce aux nouvelles possibilités techniques offertes par le traitement des données massives. [...]. Le profiling des clients apporte sans aucun doute une valeur ajoutée à l'entreprise qui peut alors affiner et personnaliser ses produits et ses offres* »[545]. Le Big data, combiné avec l'analyse qu'il encourt, offre de nouveaux outils à disposition des entreprises leur permettant de développer leurs activités économiques de manière innovante. Comme a pu l'annoncer G. Dyson, « *we now live in a world where information is potentially unlimited. Information is cheap, but meaning is*

[543] Décret du 16 septembre 2014 instituant un administrateur général des données, *Id.,* Art. 2.
[544] OECD, "Exploring the Economics of Personal Data", *loc. cit.,* p. 16.
[545] C. BRASSEUR, *Enjeux et usages du Big Data, op. cit.,* p. 48.

expensive »[546] ; le but n'étant plus celui de la simple collecte, mais plutôt celui de faire parler les masses de données, de leur donner un sens. Les données sont devenues, en l'espace de peu de temps, le critère fondamental de valorisation des entreprises modernes. Il faut souligner que la valorisation du capital d'un certain nombre d'entreprises n'est pas liée à leur chiffre d'affaire actuel, courant, ou à leur rentabilité, mais plutôt aux profits tirés par la combinaison de leur capacité à générer du trafic sur leur plateforme avec leur capacité à recueillir des données à caractère personnel.

Pour une entreprise, les informations initiales fournies par les clients et utilisateurs de leurs sites web, qui forment ainsi les informations nécessaires pré-requises de leurs bases clients, constituent une première source de valeur. C'est ce qui a permis à l'entreprise Amazon, par exemple, de licencier ses employés de marketing à la suite de l'adoption de techniques d'homogénéité des pratiques des achats qui ont permis aux machines de proposer des meilleures recommandations que les employés humains, générant ainsi plus de profits.

Vers la fin de 2012, plus de 5% des petites et moyennes entreprises et plus de 90 % des 500 premières entreprises américaines, les *Fortune 500*, ont mis en œuvre, au minimum, une initiative d'expérimentation de Big data en cours[547]. Pour la seule période allant de 2012 à 2018, le chiffre d'affaire du marché mondial du Big data est passé d'une valeur de 12.5 milliards de dollars américains à 42 milliards ; des estimations lui font atteindre les 103 milliards de dollars en 2027, et réaliser ainsi un taux de croissance annuel composé, le « *Compound Annual Growth Rate - CAGR* », de 10,48%[548]. En France, le marché du Big data est évalué à 2,5 milliards d'euros en 2018[549].

Le Big data devient, *in concreto,* un avantage concurrentiel permettant d'affiner les profils et dossiers numériques et d'enrichir les activités commerciales. Il constitue des données d'un autre type, provenant de sources diverses et variées, facilitant d'autres techniques et valorisations économiques. Autrement dit, « *the wealth of user-generated content that has emerged over*

---

[546] The Europan, Conversation with George Dyson – auteur de l'ouvrage *Turing's Cathedral* (2011), du 17/10/2011 : https://www.theeuropean-magazine.com/352-dyson-george/353-evolution-and-innovation, et *Cf.* p. 390 et s.

[547] Talend, « Talend's Big Data Solutions Receive Commitment from Partner Community » : https://www.talend.com/about-us/press-releases/talends-big-data-solutions-receive-commitment-partner-community/

[548] Sources : Statista, "Forecast of Big Data market size, based on revenue, from 2011 to 2027 (in billion U.S. dollars)" (Survey period: 2011-2018), March 2018 : https://www.statista.com/statistics/254266/global-big-data-market-forecast/ & Forbes, "10 Charts That Will Change Your Perspective Of Big Data's Growth", May 2018: https://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/#c1f8ed029268

[549] Source : https://www.economie.gouv.fr/nfi-economie-des-donnees-enjeux-et-objectifs

recent years also offers opportunities to develop profiles and target specific individuals with product and service offerings likely to be of most interest to them »[550].

Dans le domaine de la publicité, cette masse de données, une fois analysée, sert à cibler, de manière assez précise, les individus. Cela permet à l'entreprise de gagner en termes de coût et d'efficacité puisque les anciens moyens, auparavant engagés pour toucher des cibles assez limitées, sont progressivement remplacés par des campagnes publicitaires ajustées aux cibles réelles visées.

Par ailleurs, ce phénomène de « datafication »[551] des utilisateurs fournit une nouvelle méthode inédite, celle d'ajuster l'offre à la demande avec exactitude, en déterminant la taille réelle de la cible ainsi que d'autres variables spécifiques. Cette pratique s'avère être de plus en plus efficace au bénéfice des grandes entreprises, mais aussi des TPE et des PME leur permettant d'optimiser leur investissement ou d'employer de nouveaux outils techniques et analytiques ou des ressources originales, non exploitées par le passé. En effet, exploiter toutes les possibilités et les caractéristiques du Big data permet aux entreprises d' « *optimiser leurs processus de production, par exemple dans la domaine de la logistique, ou pour analyser de manière systématique les comportements de leurs clients* »[552].

Il semble alors que les identités numériques des utilisateurs du web ont une position centrale dans l'économie, qu'elle soit numérique ou matérielle, physique. Les modèles économiques qui se développent collectent toutes les informations personnelles, disponibles ou rendues disponibles, sur leurs clients dans le but de croître et d'innover leurs activités commerciales, en ayant recours à des pratiques de discrimination par les prix, de ciblage publicitaire ou de recommandations personnalisées. C'est la technique de segmentation comportementale désormais adoptée, notamment en matière de marketing et de publicité, qui est une « *technique couramment utilisée visant à l'élaboration de profils de clientèle, sur la base desquels chaque client est associé à un profil spécifique. À chaque profil correspond une stratégie commerciale visant à permettre au commerçant de maximiser le bénéfice de la relation commerciale [...]*

[550] OECD, "Exploring the Economics of Personal Data", *Id.,* p. 12.

[551] Datafication : néologisme qui désigne la mise en données du monde et/ou la mise en corrélations des comportements en ligne, employé de manière récurrente ; pour ne citer que quelques exemples : CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.*; V. MAYER-SCHÖNBERGER & K. CUKIER, *Big Data, op. cit.*; Séminaire de l'ISCC, « Datafication, privacy and (dis)empowerment », du 2 mai 2016 (Intervenant : Jo Pierson, discutant : Mélanie Dulong de Rosnay), Paris ; E. SADIN, *La Vie algorithmique - Critique de la raison numérique,* Paris, L'Échappée, coll. Pour en finir avec, 2015.

[552] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, op. cit.,* p. 49.

»[553]. Une entreprise peut, dès lors, choisir quelle catégorie ou quel segment de client à viser, en fonction des profils établis, pour faire la promotion d'un produit en ciblant adéquatement les publicités tout en améliorant le rapport produit-consommateur. La technique de segmentation comportementale « *permet ainsi de réduire les coûts d'une campagne de publicité ainsi que d'élaborer des produits à destination exclusive de tel ou tel segment de clientèle* »[554].

Plus spécifiquement, les divers outils analytiques développés permettent d'anticiper, avec un certain degré d'exactitude, des besoins ou des comportements. C'est, par exemple, la technologie dite « *Dynamic Retargeting* » proposée par la société Criteo qui vend des services de publicités ciblées sous forme de bannières s'affichant sur les sites consultés. Cette technique de re-ciblage dynamique génère, selon l'entreprise, plus de vente de manière rentable en livrant la meilleure publicité au moment le plus adéquat dans le parcours du consommateur, grâce à un « *custom piece of code placed on your site* [that] *enables the Criteo Engine to see shoppers' engagement and power product recommendations in your ads* »[555]. Elle permet aussi la collaboration et la coopération entre les consommateurs et les éditeurs premiums, de hautes gammes, en accordant l'accès aux meilleurs inventaires publicitaires[556] disponibles, procurant ainsi un placement publicitaire optimal d'annonces à travers les sites de références incontournables et dominants. Enfin, cette technique de re-ciblage ferait en sorte de ramener les consommateurs pour effectuer un achat ultérieur. En effet, l'entreprise promet de stimuler davantage les ventes provenant des internautes visitant le site web mais n'effectuant aucun achat, étant donné que « *personalised offers, delivered at just the right time and in the right format, can bring this pool of shoppers back* »[557]. C'est bel et bien de la segmentation comportementale minutieuse où l'analyse d'une large masse d'informations sur les habitudes et les comportements des consommateurs établit des corrélations, et prédit *in fine* leurs achats et leurs situations financières.

En ce sens, l'entreprise américaine Target[558] est, depuis longtemps, parvenue à identifier les femmes enceintes simplement en analysant leurs habitudes d'achat. En examinant l'historique d'achats des femmes ayant souscrit à leur liste de cadeaux pour nourrissons, les analystes ont

---

[553] G. DESGENS-PASANAU, *La protection des données personnelles*, Paris, LexisNexis, 2ème Ed., 2016, p. 133-134.
[554] G. DESGENS-PASANAU, *La protection des données personnelles*, *Id.,* p. 134.
[555] Criteo, "How Criteo Dynamic Retargeting Works for You", https://www.criteo.com/for-marketers/products/criteo-dynamic-retargeting/
[556] Selon l'Autorité de la concurrence, l'inventaire publicitaire mis à la disposition des annonceurs désigne la place que le média décide d'allouer à la publicité : Autorité de la concurrence, Avis n° 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne, p. 7, point 25.
[557] Criteo, "How Criteo Dynamic Retargeting Works for You", *Id.,* et: https://www.criteo.com/insights/category/retargeting/
[558] https://www.target.com

observé que ces femmes commençaient à acheter des crèmes sans parfum aux alentours du troisième mois de grossesse et que, quelques semaines plus tard, elles avaient tendance à se procurer des suppléments alimentaires. L'équipe a, en fin de compte, détecté à peu près une vingtaine de produits qui, utilisés comme des « proxys », des variables intermédiaires, permettaient à l'entreprise de calculer une cote de « prédiction de grossesse prévisible » pour chaque client ayant payé avec une carte de crédit ou ayant utilisé une carte de fidélité ou un coupon (un coupon-rabais)[559]. De plus, ces corrélations « *let the retailer estimate the due date within a narrow range, so it can send relevant coupons for each stage of the pregnancy. "Target", indeed* »[560].

La plupart des entreprises tirent, à notre époque, leur source de croissance de leur capacité à mettre ces masses de données au service de la publicité et du marketing et donc, à leur profit. Le web, par la souplesse et l'efficacité de ses plateformes et technologies, sert à proposer des offres variées, notamment en termes de ciblage publicitaire, de format et de processus de tarification. En outre, les offres de publicités numériques sont généralement réparties par segments dont les plus importants, selon l'Autorité de la concurrence, sont « *les moteurs de recherche (« search »), l'affichage (« display ») et les annuaires* »[561].

La publicité en ligne a, tout d'abord, la possibilité de recourir aux techniques classiques de ciblage, similaires à celles des médias hors ligne, fondées notamment sur des critères d'audience et d'affinité avec l'audience ciblée. Ces critères sont principalement sociodémographiques (âge, sexe, catégorie socio-professionnelle, etc.) mais, « *à la différence des autres médias, Internet permet aussi de prendre en compte la tranche horaire et la localisation* »[562]. Une autre technique, dite contextuelle, cible de manière plus fine, en se basant sur le contenu de la page web visitée, pour proposer une publicité qui répond le plus aux centres d'intérêts révélés par la lecture du contenu du site. Cela peut être un raffinement de chaînes thématiques particulières, de type relation, rencontre, immobilier, mode, sport et ainsi de suite, mais peut aussi résulter d'une lecture automatique opérée par un algorithme analysant l'occurrence des mots pour dégager des thématiques notables et révélatrices. Cette catégorie de publicité contextuelle est plus aisément proposée par les moteurs de recherche ayant les ressources et les capacités nécessaires pour trouver et insérer, de manière pertinente, les

[559] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data, op. cit.,* p. 57-58.
[560] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data, Id.,* p. 58.
[561] Autorité de la concurrence, Avis n° 10-A-29 sur le fonctionnement concurrentiel de la publicité en ligne, *Id.,* p. 12-14, points 53-71.
[562] Autorité de la concurrence, Avis n° 10-A-29 sur le fonctionnement concurrentiel de la publicité en ligne, *Ibid.,* p. 10, point 42.

annonces dans les pages web dont les contenus ont été analysés. Une dernière technique de publicité, dite comportementale, est de plus en plus adoptée en matière de publicités sur internet. Celle-ci constitue une forme de publicité dans laquelle les annonces sont sélectionnées en fonction du comportement navigationnel de l'internaute qui, analysé, révèle un intérêt sur un sujet particulier. Elle propose ainsi des annonces en adéquation avec les attentes supposées de l'individu, telles qu'elles ressortent de sa navigation sur le web. Comme le constate D. Cardon, « *alors que le système d'achat d'espace pour les publicitaires propose d'ajuster les bannières commerciales au contenu éditorial du site, en supposant que celui-ci s'adresse à des catégories sociodémographiques spécifiques, le ciblage comportemental piste l'individu et lui seul* »[563]. En effet, celui-ci va jusqu'à supposer une intention d'achat grâce aux techniques de traçage permettant de proposer des annonces et des nouveaux produits pour ramener les acheteurs à la suite de leur navigation sur le site commercial sans achat ; et le ciblage comportemental facilite, également, les techniques de « *retargeting* » qui visent à proposer le même produit à un même internaute alors qu'il navigue sur d'autres pages – techniques proposées et employées par Criteo tel que vu précédemment[564]. En France, et dans le monde d'ailleurs, la publicité en ligne représente une source de revenu principale, la valeur de ce marché étant estimée, en 2017, à plus de 4 milliards d'euros[565].

Internet représente désormais le premier média publicitaire dans le monde, mais aussi l'outil permettant le développement de nouveaux modèles économiques. Il tend à surpasser les autres techniques économiques et publicitaires avec « *une croissance soutenue, portée par la généralisation des technologies programmatiques, le développement de la publicité vidéo, et le fort taux d'utilisation des réseaux sociaux, des moteurs de recherche et des plateformes de partage de vidéos* »[566]. Ce marché de l'e-pub connaît une croissance rapide, qui ne fait que s'accélérer avec, en France, un taux de croissance de 12% en 2017. Ce nouveau secteur de l'économie foisonne ces derniers temps de nouveaux acteurs, multiples et variés, dont les services sont principalement fondés, à différents degrés, sur l'exploitation massive des traces et gisements d'informations circulant sur les personnes grâce aux nouvelles pratiques et capacités informatiques. En effet, l'efficacité du ciblage promise par les nouvelles techniques de publicité en ligne a bouleversé le secteur économique, permettant un rendement supérieur à

[563] D. CARDON, *A quoi rêvent les algorithmes, op. cit.*, p. 35.
[564] *Cf.* p. 145, 380 et s., 430 et s.
[565] Sources : http://www.irep.asso.fr/marche-publicitaire-chiffres-annuels.php & https://fr.statista.com/statistiques/489558/revenus-publicite-digitale-france/
[566] Autorité de la concurrence, Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, p. 4.

celles d'autres techniques en termes de retour sur investissement. En ce sens, la forte croissance du *display* et la bonne dynamique de la technique du *search* contribuent à la croissance du marché. Ainsi, la technique du *display*, qui inclut tous les formats, tous les appareils et tous les modes de commercialisation, a permis une croissance de 20% du marché en France pour l'année 2017, estimé à 1 450 millions d'euros[567]. Plusieurs acteurs sont, dorénavant, touchés par ce nouveau secteur et les nouvelles pratiques technologiques innovantes. Chaque entreprise peut alors adopter les méthodes lui permettant d'optimiser son capital en développant son propre modèle économique personnalisé. L'entreprise Criteo a bien fondé sa croissance sur le développement de techniques informatiques permettant de cibler un individu et lui adresser des publicités spécifiquement liées à ses données navigationnelles et à ses intentions d'achat.

En outre, le développement des publicités comportementales ciblées a été facilité par la technique des *cookies tiers* : comme leur nom l'indique, ce sont des *cookies* venant de tierces parties, placés par les serveurs de domaines autres que celui du site visité par l'internaute. Ils servent généralement à suivre les activités de l'utilisateur à des fins analytiques ou de ciblage comportemental pour des stratégies de marketing[568]. À la différence des *first party cookies*, souligne Cardon, « *ils n'appartiennent pas à un éditeur unique qui les dépose dans le navigateur de l'internaute pour le reconnaître lorsqu'il arrive sur son site, mais ils sont la propriété d'une régie publicitaire en ligne, un ad-network comme Weborama, Double-Click, Critéo ou Right Media* »[569]. L'entreprise Weborama, qui propose d'optimiser les stratégies marketing des entreprises à l'aide d'actifs technologiques, de data et d'expertises en data science[570], a fait évoluer son modèle économique en se fondant sur les nouvelles technologies, et exploite des plateformes de gestion de données, dont une établie en France, fournissant de l'aide et des solutions à sa clientèle pour concevoir de nouvelles offres ou pour identifier de nouveaux marchés. Toutes ces entreprises, y compris les start-ups, ont été développées et ont fondé leur modèle économique autour de métiers, de stratégies et de technologies propres à la publicité en ligne et, surtout, en programmatique.

Dans ce contexte, il est important de relever que le nouveau RGPD précise que toute information adressée à un utilisateur doit être concise, aisément accessible et facile à

[567] 19ème édition de l'Observatoire de l'e-pub du SRI, réalisé par PwC, en partenariat avec l'UDECAM, Bilan 2017 - janvier 2018, p. 7 ; disponible en ligne : http://www.sri-france.org/etudes-et-chiffre-cles/observatoire-de-le-pub-sri/19eme-observatoire-de-pub-sri/

[568] Sources : https://academy.visiplus.com/definitions/cookie-tiers.php ; http://www.digitude.fr/definition-web/cookie-tiers/

[569] D. CARDON, *A quoi rêvent les algorithmes*, *Id.*, p. 35.

[570] https://weborama.com/fr/

comprendre, tel qu'exigé par le principe de transparence. Le Règlement souligne en outre la nécessité, dans certains cas, d'illustrer à l'aide d'éléments visuels afin de faciliter la compréhension de l'information tout en insistant que « *ceci vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne* »[571].

§2. L'économie des données : une source à diverses tendances

L'économie des données constitue, également, une source à diverses tendances dont une tendance d'étude analytique et statistique (à moindre coût) (A) ainsi qu'une tendance de recherche et de développement innovants ayant de nombreuses finalités et vocations (B).

A. Une tendance d'étude analytique et statistique (à moindre coût)

L'accroissement progressif de la quantité de données, notamment ces dernières années, a contraint les entreprises à développer, de manière continue, des outils et technologies informatiques leur permettant de stocker et de traiter en temps réel la masse d'informations, provenant de nombreuses sources, se trouvant à leur disponibilité. L'enjeu primordial est alors celui de croiser ces données, « *de les enrichir très rapidement avec un seul but : mieux connaître et comprendre la réalité et anticiper les besoins futurs* »[572].

L'émergence du Big data et l'évolution du web, y compris son extension caractérisée par le web sémantique, tendent, comme il a été vu, à faire parler les masses de données en attribuant aux informations un sens bien défini permettant une meilleure coopération entre les machines et les hommes. La tendance est, de ce fait, celle de l'analyse, toujours plus pointue et déterminante, et celle des statistiques pour pouvoir accomplir l'objectif avidement poursuivi en matière d'économie des données : « *on parle désormais de modèles prédictifs, dans lesquels des variables connues, dites explicatives, vont être utilisées pour déterminer des variables inconnues, dites à expliquer* »[573].

Un renversement des tendances anciennes qui, jusqu'à récemment, guidaient nos actions s'observe alors : là où un modèle était adopté mais des données étaient nécessaires pour le vérifier, la tendance actuelle est celle d'avoir une masse de données disponible mais des doutes

[571] RGPD, Cons. 58.
[572] C. BRASSEUR, *Enjeux et usages du Big Data*, *op. cit.,* p. 49.
[573] C. BRASSEUR, *Enjeux et usages du Big Data*, *Id.,* p. 49.

quant au modèle qui peut en découler. À travers le développement des nouvelles technologies, parallèlement à l'évolution de la culture entourant les données, la société est progressivement passée du simple dénombrement des ressources à la statistique et aux algorithmes d'intelligence artificielle.

En elles-mêmes, les données ne constituent pas une invention nouvelle ; les data existent et circulent depuis des dizaines de milliers d'années. Par le passé, tout ce qui pouvait être dénombré faisait l'objet de calcul par les hommes. D'ailleurs, les chiffres ont précédé les lettres et, avant même l'invention de l'écriture par les sumériens, des entailles, ciselures et marques servaient au comptage des animaux et des objets en terre cuite pour calculer lors des échanges commerciaux[574]. Avec l'avènement des États, le domaine des calculs et du dénombrable s'est largement démultiplié en vue de compter les forces vives existantes dans chaque État. Que ce soit dans un but de recensement des forces militaires ou de répartition des impôts, les gouvernements ont commencé à entreprendre de larges opérations de dénombrement de la société. Au XVIII^{e} Siècle et grâce aux nouveaux modes d'organisation de la collecte, ces pratiques de dénombrement et de recensement se sont généralisées, devenant de plus en plus fiables. Ainsi, en Suède, le rapprochement entre les administrations étatique et religieuse a permis un recensement plus fiable de la société, notamment à l'aide des registres d'enterrement dont disposaient les curés dans leurs paroisses et qui comportaient des données relatives à l'âge, au sexe et à l'état matrimonial des personnes[575]. L'augmentation de la fréquence du recours à ces pratiques a permis d'observer l'évolution des mesures et de la société dans le temps. Le comptage, le dénombrement, s'élaborait selon une statistique qui permettait de fournir des assurances, ou encore de rendre compte des risques pris par les navires ou les militaires : « *la statistique se conçoit alors comme un instrument de mesure objectif, permettant de connaître une réalité sociale auparavant inaccessible et complexe* »[576]. Il semble évident que les données existent et circulent depuis que les hommes existent et circulent, mais ce n'est qu'avec la statistique que leur valeur et l'utilité de leur collecte et analyse se sont réellement manifestées. Étymologiquement, la statistique désigne l'étude méthodique des faits sociaux avec l'idée d'établir un état des lieux. En latin médiéval, *status* signifie « l'inventaire » et concerne donc les affaires de l'État[577]. En latin moderne, *statisticus* désigne tout ce qui est relatif à l'État, et

[574] Voir : J. Chadwick, B.F. Cook, L. Bonfante, J.F. Healey, J.T. Hooker, W.V. Davies (Collectif), *La Naissance des écritures. Du cunéiforme à l'alphabet*, Ed. du Seuil, 1997, et, M. Bouzeghoub et R. Mosseri (dir.), *Les Big Data à découvert*, Ed. CNRS, 2017.
[575] O. REY, *Quand le monde se fait nombre*, Ed. Stock, Coll. Les essais, 2016, p. 56.
[576] A. BASDEVANT, J.-P. MIGNARD, *L'empire des données – Essai sur la société, les algorithmes et la loi*, Ed. Don Quichotte, 2018, p. 29.
[577] O. REY, *Quand le monde se fait nombre*, *Id.,* p. 31.

son dérivé *statista* se réfère à l'homme d'État[578]. C'est un instrument qui a pour objectif de mesurer l'étendue, la population ainsi que les ressources d'un État. Un mot a alors été créé « *pour désigner la science de cette partie de l'économie politique* [les dénombrements], *et l'appellent statistique* »[579].

La statistique, en allemand *Staatistik*, dérivée de « *Staatswissenschaft* » qui désigne la science de l'État, correspond plus à « l'arithmétique politique » utilisée en Angleterre telle qu'élaborée par W. Petty et J. Graunt en 1662 et fondée sur des recensements chiffrés[580]. Le terme a donc un lien étymologique et historique avec l'État, mais il n'empêche que sa pratique était initialement employée dans les sphères marchandes et pour les besoins de gouvernement des entreprises. Comme le souligne A. Supiot, « *les livres de compte sont sans doute la première expression moderne de l'établissement d'un lien entre le nombre et le droit, la quantification et l'obligation juridique* »[581].

L'origine de l'opération de rendre des comptes provient donc des usages privés des commerçants du Moyen-âge pour les besoins de comptabilité. La responsabilité commerciale découle ainsi de cette obligation de reddition de comptes et de la tenue conforme de la comptabilité. Cette responsabilité, plus large que celle civile, s'exerce vis-à-vis des contractants mais aussi vis-à-vis de l'État et du public en général[582]. Le concept de cette responsabilité financière évoque parfaitement le concept anglais d'*accountability* qui implique la mise en œuvre de trois acteurs : celui qui a des comptes à rendre (*accountor*), celui auprès duquel ces comptes doivent être rendu (*accountee*) et celui qui établit lesdits comptes, à savoir le comptable (*accountant*). À l'époque médiévale, lieu de naissance de la comptabilité moderne, l'obligation de tenir des livres de compte découlait de la *lex mercatoria*, les règlements des

---

[578] CNRTL, « Statistique » : http://www.cnrtl.fr/etymologie/statistique

[579] L.P. BACHAUMONT, *Mémoires secrets pour servir à l'histoire de la République des Lettres en France*, depuis MDCCLXII jusqu'à nos jours, ou J. 1534, Journal d'un observateur, t. 29, Londres – Chez John Adamson, 1785, p. 102.

[580] Sir W. PETTY, "Natural and Political Observations upon the Bills of Mortality" *in The Economic Writings of Sir William Petty, together with The Observations upon Bills of Mortality, more probably by Captain John Graunt*, ed. Charles Henry Hull, Cambridge University Press, 1899, 2 vols & *Political Arithmetick Or a Discourse Concerning, The Extent and Value of Lands, People, Buildings: Husbandry, Manufacture, Commerce, Fishery, Artizans, Seamen, Soldiers; Publick Revenues, Interest, Taxes, Superlucration, Registries, Banks, Valuation of Men, Increasing of Seamen, of Militia's, Harbours, Situation, Shipping, Power at Sea, etc. as the same relates to every country in general, but more particularly to the territories of His Majesty of Great Britain, and his neighbors of Holland, Zealand, and France*, Printed for Robert Clavel at the Peacock, and Hen. Mortlock at the Phoenix in St. Paul's Church-yard (1690), McMaster University-Archive for the History of Economic Thought, 1998, C. Shelburne (éd.), Londres, Robert Clavel et Hen. Mortlock, p. 261-348.

[581] A. SUPIOT, *La gouvernance par les nombres*, Cours au Collège de France (2012-2014), Institut d'études avancées de Nantes/Fayard, Coll. Poids et mesures du monde, 2015, p. 120.

[582] Pour une nomenclature des droits et obligations des commerçants : I. Grossi, L. Merland, J. Mestre, M.-È. Pancrazi, N. Tagliarino-Vignal, *Droit commercial*, Paris, Ed. Lextenso, LGDJ 2012 (29ème édition), N° 249, p. 235 et *sq.*

corporations de marchands[583]. Avec les cités-États italiennes, cette obligation fut peu à peu imposée et généralisée à tous les commerçants en vue d'instaurer un mode de preuve et de prévenir contre les faillites. Puis, la mondialisation et l'émergence des nouvelles économies du marché ont requis la quantification de nouveaux phénomènes de masse, stimulant à son tour la volonté des États de recourir à ces outils et techniques pour organiser leur société. Ce lien entre le nombre et le droit, ainsi que « *le rapprochement de ces différents usages privés et publics de la quantification, permet de mettre en lumière les quatre fonctions normatives qui lui ont été progressivement conférées : rendre compte, administrer, juger et légiférer* »[584].

Ces concepts et fonctions se retrouvent, aujourd'hui, raffinés et exploités à l'ère du Big data : ainsi la responsabilité commerciale, au sens de l'*accountability*, est un concept clé du nouveau Règlement sur les données personnelles qui impose aux responsables du traitement de données de rendre des comptes en tenant un registre des activités, mais surtout, de prendre toutes les « *mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer* »[585] le respect de leurs obligations[586]. La méthodologie statistique est apparue dans un contexte où il était de plus en plus nécessaire d'appréhender les nouvelles sociétés en formation, initiées par les poussées préindustrielles et l'émergence du capitalisme. De manière plus concrète, la statistique, telle qu'employée aujourd'hui, avant de devenir une discipline autonome, provenait, comme il a été indiqué, de deux sources distinctes : d'une part, la statistique descriptive allemande et, d'autre part, l'arithmétique politique anglaise.
Utilisé pour la première fois au XVIII[e] Siècle par l'économiste allemand Gottfried Achenwall, le terme statistique désignait une activité purement descriptive et qualitative présentant les caractéristiques d'un État, son territoire et sa population, principalement à l'aide de tableaux croisés. Cette méthode, fondée sur la *Topographia Politica*, la description de l'état actuel du pays, telle qu'introduite par Leibniz[587], permettait de comparer et de classer, de manière

[583] B. GOLDMAN, « Frontières du droit et *lex mercatoria* », *In Archives de philosophie du droit*, t. IX - Le droit subjectif en question, 1964, p. 177-192.
[584] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 120.
[585] RGPD, Art. 24 « Responsabilité du responsable du traitement ».
[586] *Cf.* p. 232 et s.
[587] Dans une note de 1678, Leibniz, alors conseiller du duc Jean-Frédéric de Hanovre, indiqua les informations qui méritaient d'être recueillies : « *Topographia Politica ou description de l'état actuel du pays. Comprenant le nombre et la condition de tous les biens immobiliers et des constructions, de tous les habitants et de leur propriété. Tous les produits ou matières brutes, qui se trouvent dans le sol, leur emplacement, quantité et qualité ; toutes les manufactures ou les objets qui sont fabriqués à travers les pays ; ce qu'on consomme approximativement en chaque lieu dans le pays, quelles marchandises sont importées, lesquelles sont exportées ; le prix des marchandises avec lesquelles chacun se nourrit, combien gagne chacun par son travail et combien il travaille. Liste de ceux qui dépassent les autres par leur zèle et leur invention et qu'on peut utiliser pour des*

pertinente, une variété de savoirs hétérogènes en opérant des distinctions entre les richesses naturelles et matérielles ou les types de régimes et les administrations. En ce sens, « *il s'agissait d'une nomenclature à intention holistique, visant à faciliter la mémorisation des faits et l'enseignement, pour le bon usage des hommes de gouvernement* »[588]. Au XIX[e] siècle, dans une Allemagne que la guerre de Trente Ans a émiettée et divisée en trois cents micro-États, se manifeste la volonté de mettre en place un cadre général, dans le but d'appréhender, classer, cataloguer, archiver, les informations en vue d'organiser la mémoire collective puis, sur ce fondement, la justice, le commerce et la politique publique à suivre. L'avènement des statistiques s'avérait, dans ce contexte, être le corollaire de la création de l'État moderne qualifié par Hobbes d' « homme artificiel »[589].

Parallèlement, l'arithmétique politique de Petty, autre méthode de statistique descriptive, se fondait entièrement sur les recensements chiffrés : des opérations et des dépouillements qui ont pour but « *des recherches utiles à l'art de gouverner les peuples* »[590], tels que le recensement de la population d'un pays, la quantité de nourriture à prévoir, la construction de tables de mortalité, le calcul des espérances de vie, ou encore la classification des sols et la fertilité des terres. Petty, pionnier de ces méthodes et techniques, décrit l'arithmétique politique comme étant l'art de raisonner par les chiffres sur tout ce qui touche aux questions relatives au gouvernement. Il précise que « *the Method I take is not yet very usual; for instead of using only comparative and superlative Words, and intellectual Arguments, I have taken the course (as a Specimen of the Political Arithmetic I have longed aimed at) to express myself in terms of Number, Weight, or Measure; to use only Arguments of Sense, and to consider only such*

---

tâches particulières. », *Sämtliche Schriften und Briefe*, I. Reihe, 2, n° 70, p. 74-75, Cité et traduit par O. REY, *Quand le monde se fait nombre*, *Id.,* p. 17.

588 A. BASDEVANT, J.-P. MIGNARD, *L'empire des données, Id.,* p. 31.

589 T. HOBBES, *Léviathan ou Matière, forme et puissance de l'État chrétien et civil,* (1651), éd. et trad. de l'anglais par Gérard Mairet, Coll. Folio essais (n° 375), Ed. Gallimard, 2000, p. 63-64 : « *La nature, qui est l'art pratiqué par Dieu pour fabriquer le monde et le gouverner, est imitée par l'art de l'homme, qui peut, ici comme en beaucoup d'autres domaines, fabriquer un animal artificiel. Puisqu'en effet la vie n'est qu'un mouvement des membres, dont l'origine est dans quelque partie interne, pourquoi ne pourrait-on dire que tous les automates (ces machines mues par des ressorts et des roues comme dans une montre) ont une vie artificielle ? Car, qu'est-ce que le cœur, sinon un ressort, les nerfs, sinon autant de courroies et les articulations autant de roues, toutes choses qui, selon l'intention de l'artisan, impriment le mouvement à tout le corps ? Mais l'art va plus loin en imitant l'œuvre raisonnable et la plus excellente de la nature : l'homme. C'est l'art, en effet, qui crée ce grand LEVIATHAN, appelé RÉPUBLIQUE ou ÉTAT (CIVITAS en latin) qui n'est autre chose qu'un* ***homme artificiel****, quoique de stature et de force plus grandes que celles de l'homme naturel, pour la défense et la protection duquel il a été conçu.* »

590 D. DIDEROT, « Arithmétique Politique », article de *l'Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers, par une société de gens de lettres*, t. I, mis en ordre & publié par M. DIDEROT, de l'Académie Royale des Sciences & des Belles Lettres de Pruffe ; quant à la Partie Mathématique, par M. D'ALEMBERT, de l'Académie Royale des Sciences de Paris, de celle de Pruffe, et de la Société Royale de Londres, à Paris Chez Briasson, David l'aîné, Le Breton, Durand, 1751 (p. 678-680), scanné par l'Université de Chicago sur Gallica, p. 678 : https://gallica.bnf.fr/ark:/12148/bpt6k50533b.r=Encyclopédie.langFR

Causes, as have visible Foundations in Nature; leaving those that depend upon the mutable Minds, Opinions, Appetites, and Passions of particular Men, to the Consideration of others [...] »[591].

C'est donc une pratique permettant d'aider les gouvernants dans l'administration de leurs pays, en s'appuyant sur des bases précises et des données rigoureusement constatées. C'est une forme d'économie politique qui a émergé *via* l'application de théories scientifiques aux problèmes politiques et économiques, aussi bien coloniaux que modernes. Elle s'assimile, en ce sens, à une philosophie naturelle appliquée, une science naturelle, non seulement une méthode de savoir permettant surtout d'exploiter, de manipuler, la nature, y compris celle de la nature humaine, dans l'intérêt de l'État. Le développement des techniques de quantification, par le biais d'outils mathématiques et informatiques, est destiné à appréhender une masse diverse supposée non maîtrisable.

Il s'avère ainsi que la principale différence entre le modèle anglais et le modèle allemand réside dans le fait que la statistique descriptive allemande aspirait à rendre une image globale de l'État, de manière descriptive et sans faire appel à la quantification, là où l'arithmétique politique anglaise, qui se rapproche beaucoup plus de la statistique telle qu'elle est employée aujourd'hui, était principalement basée sur des principes de comptabilité et des inventaires chiffrés. Et, indique A. Supiot, *« le mot « comptable » est trompeur : la comptabilité ne compte pas (au sens de dénombrer des choses de même nature), elle évalue ; et elle n'évalue pas seulement ce qui est, mais ce qui peut advenir en utilisant la monnaie comme un moyen de domestiquer l'avenir* »[592]. Ces deux méthodes ont fini par converger, créant la statistique moderne fréquemment utilisée par les États, les entreprises, les associations, et ainsi de suite. Centrée sur les mathématiques, elle inspire l'objectivité et, par là même, une légitimité d'administration des êtres et des choses. Les premiers bureaux de statistiques officielles, ancêtre des instituts nationaux officiels de statistiques tels que l'INSEE[593], ont dès lors été créés par les États. Toutefois, que ce soit les instituts nationaux de statistiques ou les instituts privés de sondage et d'étude, ils se retrouvent tous fortement secoués par l'émergence du Big data et des algorithmes de prédiction, largement facilités par le développement des outils informatiques permettant de grandes capacités de stockage ainsi que des analyses instantanées et fiables.

---

[591] Sir W. PETTY, "The political anatomy or Ireland [1672], London 1691" *In The Economic Writings of Sir William Petty, together with The Observations upon Bills of Mortality, more probably by Captain John Graunt*, *op. cit.*, Vol. I, p. 201.

[592] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 125.

[593] Institut national de la statistique et des études économiques : « *collecte, produit, analyse et diffuse des informations sur l'économie et la société françaises* », https://www.insee.fr/fr/accueil

En effet, alors que les développements des technologies sont les principaux moteurs de la production et de la circulation des data, l'utilisation de ces données a été considérablement facilitée par le déclin des frais de stockage, de traitement et d'analyse. Par le passé, les frais de stockage de données décourageaient la sauvegarde de toute donnée qui n'était plus, ou qui ne serait probablement plus, nécessaire ou utile. Désormais, « *storage costs have decreased to the point at which data can generally be kept for long periods of time if not indefinitely* »[594].

Dans ce contexte, la loi de Moore, qui stipule que la puissance de traitement double environ tous les 18 mois, par rapport au coût ou à la taille, a été largement étayée. Ceci est particulièrement notable dans les outils de traitement de données développés : outils qui sont devenus de plus en plus puissants, sophistiqués, omniprésents et peu coûteux, rendant les données facilement consultables, corrélables et traçables, non seulement par les gouvernements et les grandes entreprises, mais aussi par de nombreuses autres personnes et entités. Autrement dit, « *Moore's law, which predicts the industry can double the computing power of a microchip every 18 months, affects surveillance computing just as it does everything else: the next generation will be smaller, faster, a lot cheaper and more easily available. As soon as the recognition technologies isolate the people, the computers will be able to do the searching* »[595]. Or, il semble bien que la loi de Moore soit déjà dépassée avec les dernières avancées en matière technologique ; en réalité, « *Moore's Law is no longer valid. It has been rendered obsolete by new developments, such as "flash" technology that permits more than one digit to be stored on a single transistor; or "megaships" that operates at three times the speed of today's most powerful chips; or quantum transistors that could be not only much faster than today's transistors but use much less power; or research on even more microscopic transistor substitutes based on molecules or, the latest and most remarkable of all, carbon "nanotubes" only a few atoms in diameter that could apparently be made to act as semiconductors* »[596].

---

[594] OECD, "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data", *OECD Digital Economy Papers*, No. 222, OECD Publishing, Paris, 2013, p. 9: http://dx.doi.org/10.1787/5k47zw3fcp43-en

[595] B. SCHNEIER, *Secrets & Lies: Digital Security in a Networked World – With new information about post 9/11 security*, Wiley Publishing Inc., Paperback Edition, 2004, p. 31.

[596] R. WHITAKER, *The end of privacy: how total surveillance is becoming a reality*, The New Press, New York, 1999, p. 53; et l'auteur indique en outre que "*early in 1998, it was reported that "Israeli scientists have become the first to coax individual biological molecules into forming an electric circuit. This marriage of biotechnology and electronics will eventually make possible the production of a transistor sized 1/100,000th of the width of human hair, 100th or less of the space required today". Protein-based semiconductors may eventually replace silicon altogether with biomolecular computers. There appears to be no end in sight for the upward trajectory of the miniaturization of computing power. If anything, the technology may already have surpassed the practical capacity to make short-term use of its full potential*." (p. 53-54)

Cette diminution des coûts des nouvelles technologies et outils informatiques génère ainsi une grande facilité et une panoplie de moyens permettant d'opérer des séries de statistiques, des corrélations statistiques et de nombreuses études analytiques et prédictives. Il est vrai que cela relève « *d'une révolution technologique dont la portée et la puissance sont fonctions du nouvel entrant économique que représente la multitude,* [… or] *une donnée n'est pas quelque chose de naturel, mais de construit. Les données sont construites, produites et le processus de fabrication est aussi important que la donnée en elle-même* »[597].

B. Une tendance de recherche et de développement innovants à nombreuses finalités

Que ce soit pour le secteur public ou privé, les nouvelles pratiques et méthodes développées grâce aux opportunités offertes par le Big data, permettent d'appréhender les données dans plusieurs nouvelles perspectives aussi diverses que variées. Corrélativement, le développement de la statistique moderne et des nouveaux outils de statistique et d'analyse répondent successivement à diverses préoccupations médiévales ou modernes. Dans la tradition médiévale, la statistique, dans un premier temps à vocation pédagogique, servait principalement à instruire le pouvoir royal et lui refléter sa grandeur à travers la description des provinces, du royaume, du territoire et du montant des impôts à collecter. La statistique se concentra, par la suite, sur l'état de la société civile et de ses habitants, tels que le recensement de la population ou l'inventaire des produits agricoles et industriels disponibles, répondant, dans ce cadre, à une vocation pratique. Les situations sociales vécues subséquemment, comme la famine, les épidémies ou les guerres, ont mené la statistique vers des études de plus en plus régulières et spécialisées[598]. Depuis, les opportunités et les préoccupations se sont démultipliées, entraînant l'émergence d'une tendance régulière et innovante ayant plusieurs vocations et de nombreuses finalités.

Il faut admettre que, d'une certaine façon, le Big data s'avère être un grand révélateur objectif du réel et du quotidien. Alors que l'action, publique ou privée, reposait sur l'expérience d'agents, leurs intuitions et leurs croyances, elle se fonde désormais sur des séries et des faits statistiques. Aujourd'hui, que ce soit à vocation pédagogique, pratique, administrative, commerciale, de recherche, d'information ou de renseignement, la masse de données disponible, combinée aux outils et technologies constamment développés, représente une source d'une grande valeur et porteuse de nombreuses vocations et tendances. La quantité de

[597] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 17.
[598] A. DESROSIÈRES, *La politique des grands nombres – Histoire de la raison statistique*, Paris, Ed. La Découverte & Syros, 1993, p. 39-40.

données, l'étendue de leurs traitements, utilisations et réutilisations ne font que s'élargir entraînant, par conséquent, l'élargissement des domaines pouvant y recourir : que ce soit dans le domaine de la santé, de l'énergie, de l'environnement, de la sécurité, ou, simplement, pour renseigner tout un chacun sur différents sujets allant de la qualité de l'air aux points d'accès wifi du quartier, au budget voté par les représentants locaux ou aux bureaux de tabacs disponibles aux alentours.

Ainsi, à partir des données publiques de santé, de nombreuses perspectives et opportunités de réutilisations et d'analyses innovantes de ces données se manifestent. Plusieurs bénéfices peuvent être tirés de ces statistiques et analyses, tels que le passage d'une logique curative à une logique préventive facilitée par une meilleure prise en charge des patients médicaux, ou encore l'ouverture de nouveaux terrains d'analyses et d'expérimentations aux chercheurs scientifiques comme les maladies chroniques, l'épidémiologie ou la pharmacovigilance. Par ailleurs, grâce au Big data et à l'Open data, de nouvelles méthodes de recherches scientifiques ont émergé : au lieu d'être fondées sur la méthode déductive à partir d'hypothèses préalables, elles se basent désormais sur une méthode inductive à partir de l'observation de corrélations statistiques. Dans cette perspective, à partir d'analyses aléatoires d'une masse de données, de nombreux facteurs et éléments environnementaux, alimentaires, pharmacologiques ou génétiques des maladies pourraient être identifiés.

Profitant des progrès de la science et du numérique, la médecine s'oriente progressivement vers la prévention, la prédiction, la participation, mais aussi la personnalisation des soins en améliorant l'accompagnement des patients et en instaurant un terrain de partage entre les médecins et les patients. Grâce à l'imagerie médicale et aux avancées technologiques, de nouvelles pratiques sont apparues permettant d'analyser encore plus de cas, d'opérer encore plus de prédictions ou d'interventions. Précisément, il est aujourd'hui possible de *« modéliser des organes sur ordinateur, étudier des systèmes biologiques complexes, détecter des maladies et même optimiser des gestes chirurgicaux avec la réalité augmentée et des robots spécialisés »*[599]. Une étude[600] conduite par la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS)[601], devenue le 1er janvier 2018 la Caisse nationale de

[599] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.,* p. 20.

[600] CNAMTS 2, « Benfluorex, valvulopathies cardiaques et décès », complète et précise la précédente note intitulée « Benfluorex, valvulopathies cardiaques et décès » demandée par l'Afssaps le 25/8/2010 et transmise à cette dernière le 28/9/2010 ; disponible en ligne : https://www.ameli.fr/fileadmin/user_upload/documents/Note_complementaire_Cnamts_novembre_2010_-_Benfluorex.pdf

[601] http://www.securite-sociale.fr/-CNAMTS-

l'assurance maladie (CNAM)[602], a ainsi pu détecter, mais surtout confirmer, les troubles cardio-vasculaires et neurotoxiques résultant de la consommation du médicament Mediator[603] à partir des données du Système National d'Information Inter-régimes de l'Assurance Maladie (SNIIRAM)[604] qui compte un peu plus de 18 tétraoctets de données individualisées, rassemblant l'intégralité des remboursements d'assurance maladie et des séjours hospitaliers de 63 millions de français[605].

De plus, les grandes capacités de stockage et de calcul ont permis le développement de techniques, d'outils et de logiciels analysant le génome complet d'un être humain de manière plus facile et plus rapide, et ce, à un coût dérisoire. Ainsi, l'entreprise Illumina vise à libérer la puissance et les vertus du génome et propose des « *sequencing and array-based solutions for analysis of genetic variation and function, in fields ranging from cancer research to agriculture* »[606]. Elle met au point et fournit des systèmes de plateforme de séquencage pour une analyse génétique et génomique fonctionnelle comme le « Genome Analyzer*IIx* System » qui, selon l'entreprise, « *gives you the power to go from DNA or RNA to data in under a week with less than four hours of hands-on time, with superior raw-read accuracy and the industry's simplest automated workflow* »[607]. Une large quantité de données génétiques et de données sensibles peuvent ainsi être gérées et traitées dans différents niveaux des bases de données disponibles et pour diverses finalités[608]. Le temps d'analyse a chuté à moins d'une semaine au lieu d'une

[602] https://lannuaire.service-public.fr/gouvernement/etablissement-public_168383 & https://travail-emploi.gouv.fr/emploi/emploi-et-handicap/prevention-et-maintien-dans-l-emploi/cnamts

[603] Rapport d'information n° 675 fait au nom de la Mission commune d'information sur : « Mediator : évaluation et contrôle des médicaments » (2010-2011), de Mme M.-T. HERMANGE, déposé au Sénat le 28 juin 2011, p. 43-52 ; disponible en ligne : http://www.senat.fr/rap/r10-675-1/r10-675-1.html

[604] Créé en 1999 par la loi de financement de la Sécurité sociale, le SNIIRAM est une base de données nationale dont les objectifs sont de contribuer à une meilleure gestion de l'Assurance Maladie et des politiques de santé, d'améliorer la qualité des soins et de transmettre aux professionnels de santé les informations pertinentes sur leur activité : https://www.ameli.fr/l-assurance-maladie/statistiques-et-publications/sniiram/finalites-du-sniiram.php

[605] SAS Communiqué, « Assurance maladie : la biostatistique au cœur du pilotage du système de santé » : https://www.sas.com/fr_ma/customers/temoignages-clients/cnamts-pilotage-du-systeme-de-sante.html

[606] Source : https://www.illumina.com

[607] Specification Sheet: Illumina® Sequencing, « Genome Analyzer$_{IIx}$ System - The most proven, widely adopted next-generation sequencing platform», Pub. No. 770-2009-017 Current as of 27 April 2011: https://www.illumina.com/content/dam/illumina-marketing/documents/products/datasheets/datasheet_genome_analyzeriix.pdf

[608] *Cf.* p. 618.

dizaine d'années, tel que ce fut le cas pour le « *Human Genome Project* »[609], et il est désormais possible d'effectuer, pour moins de mille euros, un séquençage de génome humain[610].

En outre, l'apport du numérique est stratégique, visant à améliorer l'accès à des soins toujours plus personnalisés à travers le développement de la santé à domicile ou celui du « *quantified self* »[611]. Mouvement apparu en 2007-2008, le *quantified self*, la connaissance de soi numérique, par une quantification, la mesure de soi, désigne de nouveaux moyens, principes et outils permettant de suivre, de traiter et d'analyser les données du quotidien d'une personne. Il vise au « mieux-être » par l'analyse des diverses activités liées au mode de vie et au quotidien d'un individu, afin de mieux gérer son bien-être, sa santé et sa productivité de manière simple, efficace et durable[612]. Ces outils peuvent être des objets connectés, des applications mobiles ou encore des applications web. Un capteur synchronisé avec une application mobile, par exemple, saisissant de nombreux évènements qui y sont déclarés, mesure les constantes physiques, dont les valeurs numériques fixées, impliquant une grandeur physiquement mesurable, observées lors de ceux-ci. C'est donc la quantification d'une activité ou d'un facteur physique avec des applications mobiles ou web, telles que Runkeeper[613] ou Nike+ Run Club[614]. C'est aussi surveiller la nutrition par une estimation des calories avec des applications telles que MyFitnessPal[615], ou surveiller le poids à l'aide de balances connectées comme celles proposées par Withings[616], ou encore mesurer la qualité de sommeil avec des applications comme

[609] The Human Genome Project (HGP) was the international, collaborative research program whose goal was the complete mapping and understanding of all the genes of human beings. All our genes together are known as our "genome.". it started in 1990 and was completed in April 2003: National Human Genome Research Institute, "An Overview of the Human Genome Project" : https://www.genome.gov/12011238/an-overview-of-the-human-genome-project/

[610] C. DELUZARCHE, « La chute vertigineuse du coût du séquençage ADN », JDN, du 04/06/2014 : https://www.journaldunet.com/economie/sante/1139340-le-sequencage-adn-a-bas-cout-une-revolution-fabuleuse-et-dangereuse/1139341-chute-des-couts & G. ROZIÈRES, « Pour 999 dollars, le séquençage de votre génome disponible sur une app », Le HuffPost, du 10/03/2016 : https://www.huffingtonpost.fr/2016/03/08/sequencage-genome-999-dollars-veritas-genetics-application_n_9408484.html

[611] Quantified Self – Self-knowledge through numbers: http://quantifiedself.com

[612] Pour plus d'informations : E. GADENNE, *Le guide pratique du Quantified Self. Mieux gérer sa vie, sa santé, sa productivité*, France, Fyp éditions, 2012.

[613] https://runkeeper.com

[614] Suivez chaque run, bénéficiez d'un coaching adapté à vos besoins et invitez vos amis à vous rejoindre. Tout est possible avec l'application Nike+ Run Club : https://www.nike.com/fr/fr_fr/c/running/nike-run-club

[615] Fitness starts with what you eat. Take control of your goals. Track calories, breakdown ingredients, and log activities with MyFitnessPal: https://www.myfitnesspal.com

[616] Body, Weight & BMI Wi-Fi Scale. Smart scale. Smarter you: https://www.withings.com/be/en/body

iSommeil[617], par exemple. En 2018, un peu plus de 325 000 applications de santé mobiles pour iOS et Android ont été recensées[618].

Dans le domaine médical, l'observation des corrélations statistiques entre des paramètres ne présentant aucun lien, en apparence, permet de réaliser une meilleure détection de pathologies, et une prévention plus réussie que l'action concertée des médecins. L'analyse de la masse de données collectées ouvre, dans ce contexte, la voie à l'automatisation d'une partie du secteur médical, à l'image de l'automatisation du secteur de marketing en matière de recommandations[619]. Ainsi, l'entreprise Apple a, depuis 2014, lancé sa base de données médicale centralisée, Healthkit[620], au sein de laquelle les utilisateurs peuvent retrouver toutes leurs données de santé collectées par le biais de leur iPhone ou des objets connectés[621]. Nombreux établissements hospitaliers et instituts médicaux sont en partenariat avec l'entreprise afin d'accéder aux données des patients. À cet égard, Apple propose et suggère aux développeurs d'applications et d'objets connectés à vocation médicale, « *de stocker toutes les données issues des capteurs de santé dans Healthkit, pour que l'utilisateur puisse toutes les consulter ensemble* »[622] dans l'application « Santé » qu'il a développé en marge. De plus, cette technologie sert de base, de feuille de route, d'API[623], pour créer de nouvelles applications en matière de santé personnalisées. L'entreprise propose ainsi d'utiliser ses ressources pour se renseigner sur la conception et la construction d'applications de santé et de bien-être en recourant au HealthKit, en promettant que ces applications peuvent fonctionner avec les données de santé et les données d'activités des utilisateurs pour fournir des expériences plus

[617] iSommeil : mon mobile veille sur mon sommeil : http://zz.isommeil.net

[618] mHealth App Economics 2017 – Current Status and Future Trends in Mobile Health, Health Apps Market Update – Research2Guidance: http://www.myhealthappsblog.com/mhealth/research2guidance-market-update/

[619] *Cf.* p. 128 et s., p. 430 et s.

[620] "*HealthKit provides a central repository for health and fitness data on iPhone and Apple Watch. With the user's permission, apps communicate with the HealthKit store to access and share this data.*": https://developer.apple.com/documentation/healthkit#topics

[621] "*Integrate HealthKit into your health and fitness apps for iOS and watchOS to create a more seamless user experience. When a customer provides permission for your app to read and write health and activity data to their Health app, your app becomes a valuable data source and can deliver deeply informed health and fitness solutions*.": https://developer.apple.com/healthkit/

[622] G. CHAMPEAU, « HealthKit, l'inquiétante base de données médicales d'Apple », Numerama – Sciences, du 02 juin 2014 : https://www.numerama.com/magazine/29561-healthkit-sante-apple-donnees-medecine-hopitaux-big-data.html

[623] Abbreviation for 'application programming interface': "*a set of programming tools that enables a program to communicate with another program or an operating system, and that helps software developers create their own applications (= pieces of software)*": https://www.oxfordlearnersdictionaries.com/definition/english/api & "*A set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service*": https://www.lexico.com/definition/api

riches[624]. L'App Santé promet, par ailleurs, à ses utilisateurs un savoir plus complet, centralisé et simple sur leurs états de santé, mais vise aussi à améliorer leurs santés en rassemblant *« les données de santé de votre iPhone, de votre Apple Watch et des apps tierces que vous utilisez déjà* »[625]. Ceci permet de consulter la totalité de ces informations sur l'application qui, en outre, établit des catégories en premier plan, à savoir « Activité, Sommeil, Pleine conscience et Nutrition », et fournit des recommandations concernant d'autres applications utiles pour compléter les données collectées. De plus, l'App Santé « *permet d'effectuer un suivi précis d'un grand nombre de données importantes pour vous : votre tension, votre glycémie, votre poids ou encore votre santé reproductive* »[626].

De surcroît, les acteurs du marché tels qu'Apple proposent des cadres Open source, « *open source frameworks* », facilitant la mise en place d'applications puissantes en matière de recherche médicale et de soins. À cet égard, Apple suggère ResearchKit, « *véritable canevas logiciel open source destiné à la création d'apps, il facilite le recrutement de participants aux études et la réalisation de ces études. Depuis son lancement, la quantité de données recueillies, et par conséquent l'ampleur des connaissances acquises, battent tous les records* »[627]. L'entreprise a également lancé CareKit, un logiciel Open source qui permet de créer des applications visant une meilleure compréhension et une meilleure gestion de la santé de l'utilisateur au jour le jour[628]. Quant à l'entreprise IBM, en partenariat avec l'entreprise CGI[629], elle a créé en 2012 un logiciel de médecine prédictive le « *Patient Care and Insights* »[630], une solution d'analyse et de gestion de soins distinguée qui se donne pour vocation : permettre aux médecins et aux prestataires de soins de santé d'anticiper et de déterminer les possibilités d'intervention et de traitement, en transformant ces connaissances et observations en actions concrètes grâce à une gestion des soins coordonnée, automatisée, responsable et centrée sur le

---

[624] "*Health and Fitness Apps: Use these resources to learn about designing and building health and fitness apps that use HealthKit. Your apps can work with users' health and activity data to provide richer experiences.*": https://developer.apple.com/healthkit/

[625] Apple, « Une toute nouvelle façon de voir votre santé » : https://www.apple.com/fr/ios/health/

[626] Apple, « Une toute nouvelle façon de voir votre santé » : *Id.*

[627] Apple, « ResearchKit – Faciliter la recherche médicale et mieux comprendre la maladie » : https://www.apple.com/fr/researchkit/

[628] Apple, « CareKit – Plus vous en savez sur votre santé, mieux vous vous portez : *[…] Au lieu de compter uniquement sur vos consultations médicales, vous pourrez désormais assurer le suivi de vos symptômes et de vos traitements, mais aussi transmettre toutes les informations vous concernant à vos médecins afin qu'ils aient une meilleure vue d'ensemble de votre santé* » : https://www.apple.com/fr/researchkit/

[629] CGI, qui signifiait « Conseillers en gestion et informatique » : « *Nous coconstruisons en toute agilité des projets porteurs de retour sur investissement rapide en nous appuyant sur un écosystème dynamique valorisant l'intelligence collective* » : https://www.cgi.fr/fr-fr

[630] IBM Software Solution Brief, "IBM Patient Care and Insights - Identify new intervention and treatment opportunities and deliver coordinated, personalized care to help improve patient outcomes and lower costs", IBM Corporation October 2012: https://dsimg.ubm-us.net/envelope/119833/305432/1361139266_IBM_Patient_Care_and_Insights.pdf

patient[631]. Composé de deux solutions étroitement intégrées, l'une visant l'agrégation, l'analyse et la visualisation des données, et l'autre aspirant à délivrer activement des interventions et des soins personnalisés et coordonnés, ce logiciel puise dans les différentes bases de données regroupant les données de santé afin d'assurer, à terme, une meilleure prise en charge préventive, améliorer les soins délivrés aux patients et exploiter efficacement les informations recensées : « *Among the many benefits it offers is the potential to improve patient care by helping to effectively harness information for the benefit of patients – in other words by turning data into patient value* »[632].

Par ailleurs, l'analyse du Big data peut fournir des indicateurs avancés et fiables pour de nombreuses tendances et vocations différentes. Dans le secteur sportif, des capteurs biométriques d'analyse et de nouveaux outils informatiques ont été progressivement mis en place afin d'évaluer la performance des joueurs et d'assurer un meilleur suivi, en quantifiant toutes les données captées liées à la puissance, l'endurance, la localisation, l'efficacité, la distance parcourue ou le rythme cardiaque. Ainsi, le *miCoach Speed_Cell* développé par Adidas est un capteur qui peut être fixé sur les chaussures, traçant et enregistrant les données de performance relatives à la vitesse et à la distance parcourue, et ce pour une somme moindre ne dépassant pas les 100 euros[633]. De même, l'analyse de l'activité et des requêtes des internautes sur les moteurs de recherche, tel que Google, fournit des indicateurs permettant de détecter les épidémies de grippe. À cet égard, en se basant sur les requêtes formulées, Google a créé une méthode analysant une large quantité de requêtes de recherches Google pour traquer et mesurer les syndromes grippaux d'une population donnée, avec des résultats assez probants[634].

---

[631] CGI, « Patient Care & Insights to support patient-centered care »: "*Patient Care and Insights is composed of two tightly-integrated solutions: IBM Advanced Care Insights extrapolates insights from patient information aggregated from multiple provider settings and across populations to identify high-risk patients and opportunities for intervention that can reduce costs and improve care quality. IBM Care Manager enables providers, clinicians and care managers to create coordinated treatment plans that provide seamless care transitions spanning primary care physicians, specialist, hospitals, clinics, and home-care settings.*", CGI Group Inc. 2013: https://www.cgi.com/sites/default/files/brochures/cgi-ibm-patient-care-and-insights.pdf

[632] KPMG, « Healthcare Insights - Turning data into patient value», KPMG's Creative Services, December 2015, Foreword by S. Murphy, p. 1: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/01/healthcare-insights-dec-2015-2.pdf

[633] https://news.adidas.com/GLOBAL/Products/micoach-speed_cell/s/b4bf3f5e-02b0-4427-86b6-8f00d21ea8ac

[634] J. Ginsberg et *al*., « Detecting influenza epidemics using search engine query data », *in* Nature Vol. 457, 19 February 2009: "*One way to improve early detection is to monitor health-seeking behavior in the form of online web search queries, which are submitted by millions of users around the world each day. Here we present a method of analyzing large numbers of Google search queries to track influenza-like illness in a population. Because the relative frequency of certain queries is highly correlated with the percentage of physician visits in which a patient presents with influenza-like symptoms, we can accurately estimate the current level of weekly influenza activity in each region of the United States, with a reporting lag of about one day*." http://dx.doi.org/10.1038/nature07634

Le Big data offre ainsi une multitude d'opportunités et de capacités de suivi et d'amélioration de performance, de meilleure prise en charge, de meilleure gestion, d'aide à la décision, d'indication et localisation, de nouvelles méthodes et outils de recherche, et ainsi de suite. Rares sont les domaines qui échappent, aujourd'hui, à ces capacités et opportunités désormais disponibles : le secteur militaire y recourt, par exemple, pour fonder ses stratégies et ses décisions ; le domaine de l'agriculture se trouve, pour sa part, métamorphosé à l'aide de la collecte et du traitement des données des capteurs, pulvérisateurs automatiques, drones et satellites ; dans le secteur de l'énergie, le développement des « *smart grids* », les réseaux intelligents, captant et traitant les données collectées par les compteurs communiquants, tels que les compteurs Linky, ou les objets connectés, permet d'effectuer des économies d'énergies significatives, une meilleure gestion de l'énergie, ou encore une réduction des émissions de gaz (à effet de serre). Dans ce contexte, il s'avère que, comme l'ont souligné les anciens députés, « *le progrès technique est si rapide en la matière qu'il importe de laisser aux mécanismes protecteurs des libertés une suffisante souplesse de jeu et des possibilités d'adaptation constante* »[635].

[635] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *op. cit.,* p. 5783.

TITRE II – UNE RÉALITÉ LÉGALE

« *La question* [de la vérité] *s'est transformée. Non plus quel est le chemin le plus sûr de la Vérité ? mais quel a été le chemin hasardeux de la vérité ?* »[636]

L'identité numérique a bel et bien une existence sociale, caractérisant la réalité sociale complexe et dynamique qui l'environne ainsi au XXI[e] Siècle, impliquant nécessairement une interrogation quant à l'existence, complémentaire, d'une réalité légale qui consacre cette notion puisque, tout compte fait, « *la saisie croissante du numérique par le droit est à la fois une réalité et une nécessité* »[637].

Le droit représente, dans un sens objectif, l'ensemble des règles régissant les rapports entre les hommes[638], véhiculant également les valeurs de la société[639] ; il est question, dans ce contexte, de l'étendue de la réalité légale consacrant le concept d'identité numérique et celui de données à caractère personnel. En effet, le traitement des données personnelles devrait être conçu « *pour servir l'humanité* » : « *le droit à la protection des données à caractère personnel […] doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux* »[640]. Ce qui caractérise, à ce titre, « *l'environnement* [légal] *concret et matériel de l'homme* »[641] relatif aux données personnelles, en ce sens que le droit assurant la protection des personnes et de leurs données n'est pas substantiellement figé, mais doit plutôt être nécessairement lu et interprété en fonction de la société, du « monde des hommes »[642]. Cette approche aspire ainsi à suivre celle adoptée par le Professeur Carbonnier en ce qui concerne le droit, et qui se fonde « sur l'identification du « phénomène juridique » au sein des phénomènes sociaux »[643].

Il est vrai que l'essor croissant et rapide du numérique, ces dernières années en particulier, a entraîné la mise en œuvre de nombreuses réponses juridiques s'avérant essentielles et

---

[636] J. REVEL, *Le vocabulaire de Foucault*, *op. cit.*, p. 64.
[637] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *op. cit.,* p. 6.
[638] S. GUINCHARD et T. DEBARD (dir.), *Lexique des termes juridiques*, Dalloz, 19[ème] Ed., 2012, p. 327 : « *Droit : Droit objectif : ensemble des règles visant à organiser la vie en société et sanctionnées par la puissance publique. Droit subjectif : prérogative attribuée dans son intérêt à un individu par le système juridique, lui permettant de jouir d'une chose, d'une valeur ou d'exiger d'autrui une prestation. […]* »
[639] En France, par exemple, les valeurs de la République sont « Liberté, Égalité, Fraternité », tel qu'énoncé à l'Art. 2 de la Constitution : « *[…]. La devise de la République est "Liberté, Égalité, Fraternité". Son principe est : gouvernement du peuple, par le peuple et pour le peuple.* » ; Disponible en ligne : https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006527453/
[640] RGPD, Cons. 4.
[641] CNRTL, « Réalité » : *op. cit*.
[642] CNRTL, « Réalité » : *Id*.
[643] J. CARBONNIER, *Sociologie juridique*, PUF, Coll. « Quadrige », 2[ème] Ed., Paris, 2004, p. 13.

fondamentales pour la protection des données à caractère personnel, et celle des individus et de leurs droits et libertés. L'usage toujours plus récurrent et continu des outils et technologies numériques, parallèlement à l'émergence et à l'utilisation du Big data, engendrent souvent une multitude de conséquences pouvant, éventuellement, introduire des difficultés concrètes et porter atteinte aux droits des personnes : *« By their very nature, many of the […] technologies deployed on our phones and in our homes, offices, and on lampposts and rooftops across our cities are collecting more and more information. Continuing advances in analytics provide incentives to collect as much data as possible not only for today's uses but also for potential later uses. Technologically speaking, this is driving data collection to become functionally ubiquitous and permanent, allowing the digital traces we leave behind to be collected, analyzed, and assembled to reveal a surprising number of things about ourselves and our lives. These developments challenge longstanding notions of privacy and raise questions about the "notice and consent" framework, by which a user gives initial permission for their data to be collected* »[644].

Dès lors, il a fallu mettre en place un régime de protection, des données et des droits des individus, réel et effectif, conformément à la vision du droit romano-germanique et, en particulier, à celle du droit français, en ce sens que « *le pouvoir de l'informatique est contrebalancé, grâce aux dispositions de la loi, par un pouvoir du citoyen selon la règle posée par Montesquieu, et qui a une valeur permanente : "Pour qu'on ne puisse abuser du pouvoir, il faut que le pouvoir arrête le pouvoir."* »[645]. Ainsi, le régime de protection des données actuellement mis en œuvre dans l'Union vise à inclure dans son corpus, *in concreto*, toutes les dimensions et les caractéristiques légales entourant la notion d'identité numérique, en déclarant respecter tous les droits fondamentaux ainsi que tout autre principe ou liberté consacré par la Charte des droits fondamentaux et les traités internationaux, notamment le respect de la vie privée et de la dignité, la protection des données à caractère personnel, la liberté de pensée, ou encore la liberté d'expression et d'information[646].

Quelle est, par conséquent, l'étendue de l'existence légale du concept d'identité numérique ? Comment ce concept et ses implications est-il, à l'époque de la révolution numérique,

---

[644] Executive Office of the President, "Big data: Seizing opportunities, preserving values", The White House, Washington, May 2014, p. 58; disponible en ligne: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[645] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*., p. 5789.

[646] RGPD, Cons. 4, *Id*. « *[…]. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique.* »

juridiquement appréhendé et construit, notamment avec la mise en œuvre du RGPD et de la loi Informatique et libertés renouvelée ?

L'objectif de cette partie est donc d'étudier le régime de protection des données en vigueur, afin d'observer s'il apporte des réponses juridiques suffisantes en la matière : un régime qui se révèle être, dans un premier temps, harmonisé ayant une influence cadre en la matière (Chap. I), et, dans un second temps, transfrontalier à vocation internationale, porteur d'une influence souveraine (Chap. II) ; ces deux perspectives consacrant, *in fine*, la réalité légale de l'identité numérique au XXI^{e} Siècle.

Chapitre I. Un régime de protection harmonisé : Une influence cadre

> « *Le plus fort n'est jamais assez fort pour être toujours le maître, s'il ne transforme sa force en droit, et l'obéissance en devoir. De là le droit du plus fort ; droit pris ironiquement en apparence, et réellement établi en principe.* »[647]

L'influence opérée et induite par le développement des nouvelles technologies de l'information et de la communication réclame la mise en place d'un régime de protection des données des personnes qui soit harmonisé, « rendu harmonieux ». C'est donc un régime de protection qui souhaite « […], établir un ordre, un équilibre », qui prévoit de mettre « en accord »[648] les différentes dispositions relatives à la protection des individus dans leurs quotidiens informatiques et numérisés. Précisément, « *vis-à-vis de la presse la première défense du citoyen est le droit de réponse. Vis-à-vis de l'informatique, ce sera un droit de regard. Il s'agit toujours, face à de nouvelles puissances, d'aménager un nouvel équilibre* »[649].

Cette mise en harmonie s'entend alors, dans ce contexte, comme la « *concordance des parties d'un ensemble qui concourent à une même fin* », le « *rapport d'adéquation, de convenance, entre des êtres ou des choses* »[650] soulignant le rapport de symétrie et de conformité conçu entre, notamment, deux droits initialement distincts, mais affectant de manière égale les individus ; les nouvelles technologies numériques et le développement de la société de l'information suscitant ce besoin de concordance, de symétrie, d'harmonisation. Dès lors, cela a entraîné la création d'un régime cadre, au sens d'une loi-cadre, une « *loi définissant les grandes lignes d'une disposition votée par la législature de manière à permettre au pouvoir exécutif une application souple tout en la maintenant dans les limites définies* »[651] ; plus spécialement, c'est une « *loi comportant, sur un sujet déterminé, des définitions de principe et des règles générales à partir desquelles d'autres textes législatifs ou règlementaires définiront des mesures d'application* »[652]. L'influence est ici circulaire, rotative, formant un cycle, étant donné que l'impact de la révolution numérique a provoqué la mise en œuvre d'un corpus juridique uniforme, symétrique, composé lui-même de manière adaptée et équilibrée des

---

[647] J.-J. ROUSSEAU, *Du Contrat Social ou Principes du Droit Politique*, Ed. Marc Michel Rey, Amsterdam, (1762), 1896, Ed. Hachette Livre Bnf du 1er juin 2012, Livre I, Chap. III – Du droit du plus fort, p. 16.
[648] CNRTL, « Harmoniser » : https://www.cnrtl.fr/definition/harmoniser
[649] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*., p. 5789.
[650] Dictionnaire de l'Académie Française, 9ème Ed., « Harmonie II. » : https://www.dictionnaire-academie.fr/article/A9H0201
[651] CNRTL, « Cadre » : https://www.cnrtl.fr/definition/cadre
[652] Dictionnaire de l'Académie Française, 9ème Ed., « Cadre » : https://www.dictionnaire-academie.fr/article/A9C0133

principes et règles générales en la matière, engendrant conséquemment l'influence légale cadre désormais ressentie dans le domaine de protection des données et des personnes. Une nouvelle feuille de route et de nouvelles lignes directrices, à l'échelle européenne, semblent ainsi avoir vu le jour.

Dès lors, il est utile de s'interroger sur la manière dont s'est constitué ce régime de protection : comment se dessine-t-il ? Quels sont les droits, les libertés et les garanties prévus ?

Il semble que l'harmonisation de ce régime découle, principalement, de la mise en place du droit à la vie privée (dans sa dimension) numérique (Section I) ainsi que de la mise en œuvre de droits relatifs à la personne concernée, dans une dimension numérique (Section II) ; traduisant l'influence cadre désormais portée par le droit à la protection des données et des personnes européen et français.

Section 1 – Le droit à la vie privée numérique

Le droit à la vie privée constitue, à l'heure de la révolution numérique, un droit large et étayé nécessitant, *de lege lata*, une analyse des implications du droit au respect de la vie privée dans son essence (§1), ainsi qu'une étude des implications de ce droit à la vie privée dans sa dimension numérique, en ligne (§2).

§1. Les implications du droit au respect de la vie privée

Le droit au respect de la vie privée implique et dénote, d'une part, un droit au respect de la vie privée dynamiquement large et étendu (A) et, d'autre part, un contrôle des atteintes au respect de la vie privée également vaste et assez pointu (B).

A. L'étendue du droit au respect de la vie privée

À l'occasion d'une question prioritaire de constitutionnalité, le Conseil Constitutionnel, qui a, lentement mais progressivement, reconnu la valeur constitutionnelle du droit au respect de la vie privée, a rappelé les fondements et l'importance de ce droit[653]. Aux termes de cette décision, le droit au respect de la vie privée, liberté fondamentale désormais constitutionnalisée[654], s'étend à plusieurs branches et découle de différents fondements. Ce droit est certes absent des termes de la Constitution de 1958 ou du préambule de la Constitution de 1946, mais en 1999,

[653] Conseil Constitutionnel, Décision n° 2010-25 QPC du 16 septembre 2010.

[654] La constitutionnalisation du droit signifie « *une irrigation de l'ordre juridique par la Constitution* » : F. MÉLIN-SOUCRAMANIEN, *Texte intégral de la Constitution française*, Ed. Dalloz, 2009, p. XV.

le Conseil annonce[655] que la liberté proclamée par l'article 2 de la Déclaration de 1789[656] implique le respect de la vie privée. De même, le préambule de la Constitution de 1946, en proclamant que tout être humain sans distinction « *possède des droits inaliénables et sacrés* »[657], réaffirme, selon le Conseil, les droits et libertés consacrés par la Déclaration de 1789, qu'il en découle que *« la sauvegarde de la dignité de la personne contre toute forme d'asservissement et de dégradation est au nombre de ces droits et constitue un principe à valeur constitutionnelle* »[658]. Le Conseil Constitutionnel souligne, par ailleurs, que le droit au respect de la vie privée implique également le respect de la présomption d'innocence, le principe de dignité de la personne humaine ainsi que la liberté individuelle. Les considérations du Conseil évoquent et s'assemblent ainsi avec l'abondance des consécrations de ce droit dans les lois et jurisprudences internes, comme dans celles européennes et internationales[659].

Ce droit au respect de la vie privée figure à l'article 9 du Code civil français introduit par la loi du 17 juillet 1970[660], et est prévu par l'article 12 de la Déclaration universelle des droits de l'homme des Nations Unies[661], l'article 8 de la Convention européenne des droits de l'homme, l'article 7 de la Charte des droits fondamentaux de l'Union, l'article 11 de la Convention américaine sur le respect des droits de l'homme[662], l'article 16 de la Convention internationale des droits de l'enfant[663] ou encore l'article 1 de la Convention 108[664], pour n'en citer que

---

[655] Premièrement, dans sa décision n° 99-416 DC du 23 juillet 1999, Loi portant création d'une couverture maladie universelle, Cons. 45.

[656] Art. 2 précité « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression.* »

[657] Préambule de la Constitution du 27 octobre 1946 : « *1. Au lendemain de la victoire remportée par les peuples libres sur les régimes qui ont tenté d'asservir et de dégrader la personne humaine, le peuple français proclame à nouveau que tout être humain, sans distinction de race, de religion ni de croyance, possède des droits inaliénables et sacrés. Il réaffirme solennellement les droits et libertés de l'homme et du citoyen consacrés par la Déclaration des droits de 1789 et les principes fondamentaux reconnus par les lois de la République* ».

[658] Conseil Constitutionnel, Décision n° 2010-25 QPC du 16 septembre 2010, *Id.,* Cons. 7, p. 6.

[659] *Cf.* p. 65.

[660] Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

[661] Déclaration universelle des droits de l'homme du 10 décembre 1948, Art. 12 : « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ».

[662] American Convention on Human Rights, november 21, 1969, Art. 11. "*Right to Privacy*
1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks."

[663] Convention internationale des droits de l'enfant - Convention des Nations-Unies du 20 novembre 1989, Art. 16 « *1. Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.*
2. L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

[664] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (Convention 108), Conseil de l'Europe, Série des traités européens - n° 108, Strasbourg, 28 janvier 1981, Art. 1 : « *Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses*

quelques exemples.

Dans un sens premier, explicite, ce droit offre une protection contre toute intrusion ou ingérence dans l'intimité de la personne, qu'elle soit opérée par un État ou des personnes privées. Dans ce contexte, et de manière intuitive, la notion de vie privée semble expressément liée au domicile, à la correspondance et aux relations intimes, pour lesquels le secret et l'intimité doivent être préservés. Vu sous cet angle, la constitutionnalisation du droit au respect de la vie privée était inévitable : « *elle seule permettait d'assurer en pleine lumière l'épanouissement de l'individu dans la sphère intime, à l'abri du regard de l'État et de la société, que le développement des techniques, de la science, de l'informatique, de la presse, de l'Internet, et des moyens de communication menace chaque jour davantage* »[665]. La jurisprudence considérablement volumineuse en matière de respect de la vie privée, qu'elle soit celle du Conseil Constitutionnel, de la Cour de Cassation, de la Cour européenne des droits de l'homme ou de la Cour de justice de l'Union (anciennement la Cour de justice des communautés européennes), confirme et réaffirme ce constat et la valeur fondamentale du droit au respect de la vie privée, y compris son pouvoir créateur.

En droit français, jusqu'à présent, la notion de vie privée s'est trouvée en quelque sorte bousculée et secouée par des dispositions légales autorisant la vidéosurveillance, les procédés de fouille, les intrusions dans le domicile, la géolocalisation, les interceptions téléphoniques et électroniques, la publication ou la communication d'information exposant la vie privée, le manque de transparence des procédures d'enquêtes et ainsi de suite. Parallèlement, c'est ce qui a, toutefois, permis de mettre en exergue l'aspect fondamental et dynamique de cette notion, essentielle au droit et à la société. Dès lors, il s'avère impossible de dresser une cartographie exhaustive des composantes de la vie privée, en raison même de son caractère évolutif et extensible. La jurisprudence, avec la consécration des techniques et des applications numériques touchant de plus en plus de domaines, pourrait élargir le champ d'application et les frontières de cette notion ou autonomiser d'autres composantes du droit au respect de la vie privée, tel que ce fut le cas pour les données personnelles, la liberté de s'autodéterminer, de se découvrir et de se développer personnellement, ou encore d'établir et d'entretenir des rapports avec d'autres personnes, par exemple.

---

droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données»). »

[665] V. MAZEAUD, « La constitutionnalisation du droit au respect de la vie privée », Nouveaux cahiers du Conseil Constitutionnel n° 48 (2015/3) – Dossier : Vie Privée, Ed. Lextenso, Juin 2015, (p. 7 à 20), p. 8. Et l'auteur rajoute en note : « *Menaces dont, non sans paradoxe, les titulaires du droit au respect de la vie privée sont souvent l'origine, de sorte qu'il faudra un jour les protéger contre eux-mêmes* ».

Il apparaît *de facto* quasi-impossible de circonscrire les périmètres de cette notion induisant la liberté, privée ou publique, mais aussi la défense de la vie privée, la préservation de la sécurité, du secret et de l'intimité, la prévention contre toute atteinte ou ingérence.
D'un premier abord, identifier les bénéficiaires de ce droit apporte une meilleure compréhension quant à sa conception et à son contenu. Au sein de la jurisprudence remarquable et substantielle en la matière, les titulaires du droit à la vie privée sont largement déterminés, impliquant, *in fine,* la vie humaine : des nationaux et des étrangers, des personnes publiques et médiatiques (tel qu'un candidat à l'élection présidentielle[666]) et celles qui ne le sont pas (par exemple, l'image d'une personne non publique ou non célèbre captée par un système de vidéosurveillance), des personnes physiques et morales. Cette obligation de respecter la vie humaine, imposée par ce droit et ses fondements variés, bénéficie, comme son nom l'indique, à tout être humain. Au-delà de cette certitude, il est délicat de déterminer ce que recouvre concrètement et explicitement ce droit au respect de la vie privée.

Souvent invoqué devant les instances nationales et européennes, c'est la Cour européenne des droits de l'homme qui a, principalement, donné à ce droit, à compter des années 1990, une interprétation extensive[667]. Ainsi, ce droit paraît se décomposer en deux secteurs initiaux : la protection du « secret de la vie privée », conçue comme une protection contre la révélation de tout élément de la vie intime, un droit au secret, ainsi que la « liberté de la vie privée » perçue comme la liberté de faire des choix existentiels dans les domaines relevant de la sphère privée[668]. La protection de la vie privée comprend donc deux notions principales : le secret et la liberté. Même ainsi délimitée, le caractère mouvant et extensible de la notion de vie privée a été souligné à plusieurs reprises[669] : la Cour européenne a estimé, dès 1992, qu'il serait trop restrictif de la limiter à un « *cercle intime* », et que le respect de la vie privée doit aussi englober « *le droit pour l'individu de nouer et développer des relations avec ses semblables* »[670].
La jurisprudence constitutionnelle est celle qui retient une conception des plus classique et assez restrictive de cette notion : mis à part la question des données personnelles, « reflet moderne de

[666] Voir par ex., Conseil Constitutionnel Décision n° 2013-675 DC du 9 octobre 2013 - Loi organique relative à la transparence de la vie publique.
[667] Il est utile de rappeler que la Cour de cassation, dans un attendu de principe, a affirmé que les États adhérents à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales « *sont tenus de respecter les décisions de la Cour européenne des droits de l'homme, sans attendre d'être attaqués devant elle ni d'avoir modifié leur législation* », Assemblée plénière, Arrêt n° 589 du 15 avril 2011, pourvoi n° 10-17.049, Bulletin civil I, n° 1.
[668] F. RIGAUX, « La liberté de la vie privée », *In* Revue internationale de droit comparé, Vol. 43 N°3, Juillet-septembre 1991 (p. 539-563), p. 547-548.
[669] *Cf.* p. 65 et 72.
[670] CEDH, Affaire Niemietz c. Allemagne du 16 décembre 1992, *loc. cit.,* §29.

la personnalité », le Conseil consacre les composantes traditionnelles de ce droit en garantissant « *la liberté d'aller et venir, l'inviolabilité du domicile, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789* »[671]. En ce sens, la vie privée recouvre le domicile, perçu de manière large incluant les automobiles ou les navires, la liberté de choisir son domicile même en cas de changement fréquent de domicile, le secret des correspondances et par prolongation, les correspondances électroniques, ainsi que le secret et l'intimité de la vie privée. Néanmoins, de manière apophatique, le Conseil refuse d'étendre le champ du droit à la vie privée et se borne à le protéger contre les atteintes dont il peut faire l'objet. Il a ainsi considéré que la nationalité ne relevait pas de l'intimité et qu'une contestation ou une déchéance de nationalité ne mettait pas en cause le droit au respect de la vie privée. D'une manière analogue, en se prononçant sur la loi interdisant la dissimulation du visage dans l'espace public[672], le Conseil Constitutionnel a refusé d'examiner la question sous l'angle du droit au respect de la vie privée alors que les juges de Strasbourg ont estimé « *que les choix faits quant à l'apparence que l'on souhaite avoir, dans l'espace public comme en privé, relèvent de l'expression de la personnalité de chacun et donc de la vie privée* »[673].

Il est vrai que la jurisprudence du Conseil se démarque des jurisprudences judicaires ou européennes, et dénote une volonté de circonscrire le champ de la notion de vie privée. Toutefois, cette conception classique demeure assez particulière dans la mesure où le Conseil a pu invoquer cette notion afin de contrôler l'installation de la vidéosurveillance dans les lieux publics[674]. De même, il a eu l'occasion d'affirmer que les dispositions concernant les déclarations patrimoniales des candidats aux élections présidentielles et parlementaires relevaient du droit au respect de la vie privée[675]. Il semble bien que chacune de ces institutions cultive une vision particulière de la notion de vie privée, certaines se limitant à sa défense, d'autres l'érigeant en source de nouveaux droits, mais le constat frappant, quoique rassurant, est que l'ensemble de ces juridictions la conçoivent de manière assez étendue, et veillent continuellement à sa protection.

---

[671] Par ex. : Décision n° 2004-492 DC du 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité, Cons. 4 & Décision n° 2014-420/421 QPC du 9 octobre 2014, M. Maurice L. et autre [Prolongation exceptionnelle de la garde à vue pour des faits d'escroquerie en bande organisée], Cons. 9.

[672] Conseil Constitutionnel, Décision n° 2010-613 DC du 7 octobre 2010 - Loi interdisant la dissimulation du visage dans l'espace public.

[673] CEDH, Grande Chambre, Affaire S.A.S. c. France du 1er juillet 2014, Requête n° 43835/11, §107.

[674] Conseil Constitutionnel, Décision n° 94-352 DC du 18 janvier 1995 - Loi d'orientation et de programmation relative à la sécurité, Cons. 3, 4 et 15.

[675] Conseil Constitutionnel Décision n° 2013-675 DC du 9 octobre 2013 - Loi organique relative à la transparence de la vie publique, Cons. 6, 7 et 29.

Dans ce contexte, c'est le droit au respect de la vie privée qui garantit l'encadrement de la publicité de la situation d'un couple en s'abstenant de révéler leur préférence sexuelle[676]. C'est toujours ce droit qui justifie l'anonymat d'une mère ayant accouché sous X, ou qui réclame la possibilité d'avoir certains contacts avec la collectivité pénitentiaire[677]. C'est encore ce droit qui atteste que « *le principe de l'indisponibilité de l'état des personnes ne signifie pas que cet état soit intangible* »[678], ou qui induit que le « *droit à l'identité, dont relève le droit de connaître son ascendance, fait partie intégrante de la notion de vie privée* »[679]. C'est aussi ce droit qui sert de fondement à la « notion d'autonomie personnelle », et qui protège la sphère personnelle de chaque individu, « *la faculté pour chacun de mener sa vie comme il l'entend* »[680]. C'est toujours le respect de la vie privée qui exige que « *chacun puisse établir les détails de son identité d'être humain et que le droit d'un individu à de telles informations est essentiel du fait de leurs incidences sur la formation de la personnalité* »[681].

La notion de vie privée semble alors constituer une notion souche, ayant la capacité de s'adapter et de s'étendre à plusieurs branches : elle recouvre les activités sexuelles, les relations de couple ou de filiations, les activités sociales, les relations professionnelles, l'intégrité physique et morale, des aspects de l'identité physique, la construction et le développement de soi, l'autonomie personnelle, les correspondances, l'interception des communications, ou encore l'immixtion dans la sphère intime d'une personne. Dans cette perspective, le droit au respect de la vie privée « *fait presque figure d'attrape-tout et son potentiel d'extension est si important que, pour les plus optimistes, il rendrait toute tentative de définition « quasi-impossib(le) », à moins qu'elle ne soit vouée à l'échec* »[682].

---

[676] Conseil Constitutionnel, Décision n° 99-419 DC du 9 novembre 1999 - Loi relative au pacte civil de solidarité, Cons. 74.

[677] CEDH, Affaire McFeeley et al. C. Royaume-Uni, Requête n° 8317/78 du 15 mai 1989, §82 : « *la Commission fait observer qu'elle a précédemment déclaré dans l'affaire X. c/ Islande, (décision du 18 mai 1976, Décisions et Rapports 5 p. 86) que le concept de vie privée tel que le vise la Convention comprend « dans une certaine mesure le droit d'établir et d'entretenir des relations avec d'autres êtres humains, notamment dans le domaine affectif, pour le développement et l'accomplissement de sa propre personnalité ». La Commission estime que cet élément du concept de vie privée s'étend au domaine de la détention et que l'interdiction faite aux requérants d'entretenir des contacts avec d'autres constitue donc, à cet égard, une ingérence dans l'exercice de leur droit à la vie privée* ».

[678] Cour de Cassation (Ass. plén.), arrêt du 11 décembre 1992, Pourvoi n° 91-12.373, Arrêt N°2 – Moyen Annexé produit par la SCP Masse-Dessen, Georges et Thouvenin, avocats aux Conseils, Bulletin A.P. 1992 N° 13, p. 27.

[679] CEDH, Cour (3ème section), Affaire Jäggi c. Suisse du 13 juillet 2006, Requête N° 58757/00, §37.

[680] CEDH, Affaire Pretty c. Royaume-Uni du 29 avril 2002, *loc. cit.*, § 62.

[681] CEDH, Affaire Mikulić c. Croatie du 7 février 2002, *loc. cit.*, § 54. Voir aussi : CEDH, Cour (Plénière), Affaire Gaskin c. Royaume-Uni du 7 juillet 1989, Requête N° 10454/83, §39 et CEDH, Affaire Christine Goodwin c. Royaume-Uni du 11 juillet 2002, *loc. cit.*, § 90.

[682] V. MAZEAUD, « La constitutionnalisation du droit au respect de la vie privée », *Id.*, p. 11.

In fine, il semble ainsi que les caractères constitutionnaliste et fondamentaliste de ce droit au respect de la vie privée, également consacré de manière abondante et variée en liberté fondamentale, démarquent et concrétisent l'importance de la vie privée et de sa protection, essentielle à tout être humain.

B. L'étendue du contrôle des atteintes au respect de la vie privée

Le droit au respect de la vie privée, constitutionnellement et conventionnellement garanti, peut facilement entrer en conflit avec d'autres droits ou libertés fondamentales. C'est ce qui a pu être observé à travers de nombreux cas où une atteinte à la vie privée est alléguée face à un autre droit également protégé, menant les juges vers une appréciation de cette allégation en considération des autres intérêts en question à travers une mise en balance desdits droits.
Le contrôle mis en œuvre en matière d'atteinte à la vie privée semble être pointu quoique souple, sous-tendant la portée étendue du droit au respect de la vie privée. Selon une formule bien célèbre du Conseil Constitutionnel, il appartient au législateur « d'assurer la conciliation » entre, d'une part, « *la protection des droits et libertés constitutionnellement garantis, au nombre desquels figurent le respect de la vie privée* »[683], et, d'autre part, la sauvegarde des droits et principes à valeur constitutionnelle aussi nombreux que variés, tels que la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions[684], la sauvegarde de l'ordre public[685], la lutte contre la fraude fiscale[686], la protection du droit de propriété[687], la lutte contre la fraude[688] ou encore la prévention et la lutte contre les conflits d'intérêts[689]. De même, du côté de la jurisprudence judiciaire ou européenne, ce droit est fréquemment en conflit avec plusieurs autres, comme il a déjà été observé, tels que la liberté d'expression, la liberté d'information ou le droit à la preuve, pour ne citer que quelques exemples.

[683] Par ex. : Décision n° 2004-492 DC du 2 mars 2004, *loc. cit.*, Cons. 4
[684] Par ex. : Conseil Constitutionnel, Décision n° 2010-25 QPC du 16 septembre 2010, *loc. cit.,* Cons. 11 et Décision n° 2013-357 QPC du 29 novembre 2013 - Société Wesgate Charters Ltd [Visite des navires par les agents des douanes], Cons. 6.
[685] Par ex. : Conseil Constitutionnel, Décision n° 2008-562 DC du 21 février 2008 - Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, Cons. 30.
[686] Par ex. : Conseil Constitutionnel, Décision n° 2013-685 DC du 29 décembre 2013 - Loi de finances pour 2014, Cons. 106, et Décision n° 2013-684 DC du 29 décembre 2013 - Loi de finances rectificative pour 2013, Cons. 10.
[687] Par ex. : Conseil Constitutionnel, Décision n° 2009-580 DC du 10 juin 2009 - Loi favorisant la diffusion et la protection de la création sur internet, Cons. 23.
[688] Par ex. : Conseil Constitutionnel, Décision n° 2007-557 DC du 15 novembre 2007 - Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile, Cons. 11.
[689] Par ex. : Décision n° 2013-675 DC du 9 octobre 2013, *loc. cit.,* Cons. 28.

La mise en œuvre de la balance entre ces divers intérêts est souvent complexe, subtile, et suppose de trouver un juste équilibre entre des droits et libertés qui s'opposent. Cette responsabilité de mise en balance et de contrôle pèse aussi bien sur les législateurs que les juges. Comme l'a si bien affirmé le Conseil Constitutionnel, « *les atteintes portées à cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi* »[690] n'introduisant pas de discriminations injustifiées ; formulation souvent reprise par les juges judicaires et européens. Le respect de la vie privée est bien une liberté qui, s'analysant comme « *un droit public subjectif*, [est] *une norme juridique d'effet direct opposable à la puissance publique* »[691]. En ce sens, l'administration est débitrice du droit ou de la liberté concernée et, simultanément, les justiciables peuvent s'en prévaloir devant les juges en cas d'atteinte. De plus, en tant que principe constitutionnel, le respect de la vie privée est doté d'un effet direct. Le principal objectif d'une liberté fondamentale est d'assurer la protection d'un intérêt individuel déterminé, visant la libre construction et le libre développement de l'individu, en imposant à l'État une action d'un contenu défini et précis. Dans le cas de la vie privée, le terme « respect » cible l'action, l'obligation qui peut être aussi bien passive/négative, telle que l'absence d'immixtion, qu'active/positive, perçue comme une obligation de garantie et de protection.

L'article 8 de la Convention européenne cite, en plus du droit à la protection de la vie privée, les cas précis où une ingérence dans ce droit, de la part des puissances publiques, peut être justifiée : « *il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* »[692]. Ces différentes dispositions constituent, généralement, la base légale des procès se déroulant devant les hautes juridictions en ce qui concerne les diverses atteintes et/ou restrictions portées à la vie privée, et servent concurremment la défense des États. Ainsi, toutes les affaires présentées devant ces institutions soulevaient la question de l'équilibre entre, d'une part, l'intérêt public, comme la prévention des activités criminelles[693] ou le maintien de la stabilité

[690] Par ex. : Décision n° 2008-562 DC du 21 février 2008, *loc. cit.,* Cons. 13.
[691] O. LE BOT, « Le respect de la vie privée comme liberté fondamentale », Note sous CE, ord., 25 oct. 2007, Mme Y, n° 310125, mentionnée aux tables du recueil, RFDA N° 3 - 2008, p. 328.
[692] Art. 8, al. 2, Droit au respect de la vie privée et familiale, ConventionEDH.
[693] À titre d'exemple, dans l'affaire Uzun c. Allemagne, requête n° 35623/95 du 02 septembre 2010, le requérant était soupçonné d'implication dans des activités criminelles d'un groupe terroriste, et a été d'un trait, condamné pour multiples chef d'accusation : tentative d'homicide par le biais d'explosifs. Et dans l'affaire Bykov c. Russie, requête n° 4378/02, du 10 mars 2009, le requérant était soupçonné d'être l'instigateur, le provocateur à l'infraction d'homicide de son ancien associé.

gouvernementale[694], et, d'autre part, le droit de tout individu au respect de sa vie privée. Lors de chaque requête, les autorités publiques prétendaient que la protection de l'intérêt public prévalait et sur-pesait l'atteinte portée au droit susvisé. Il est important de souligner que les prolégomènes de ces conflits d'intérêts se sont manifestés avec l'essor des mesures de surveillance étatique et le besoin de sécurité et de défense, avant même que l'émergence des mesures et techniques de renseignements du secteur privé ne les concurrencent pour des finalités économiques.

À la suite d'une étude d'initiative associative, des principes internationaux concernant l'application des droits de l'homme à la surveillance des communications[695] ont été dégagés, proclamant que toute restriction au respect de la vie privée doit être prévue par la loi, nécessaire à l'accomplissement d'un but légitime au sein d'une société démocratique et proportionnée à l'objectif poursuivi. En ce sens, l'article 29 de la Déclaration universelle des droits de l'homme de 1948 précise que « *dans l'exercice de ses droits et dans la jouissance de ses libertés, chacun n'est soumis qu'aux limitations établies par la loi exclusivement en vue d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux justes exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique* »[696]. De même, le Comité des droits de l'homme des Nations Unies a eu l'occasion de souligner en 1999 que, « *to be permissible, restrictions must be provided by law, must be necessary in a democratic society for the protection of these purposes and must be consistent with all other rights recognized in the Covenant* »[697].

C'est aussi la position de la jurisprudence européenne qui opère constamment un contrôle des atteintes et des restrictions apportées au droit en question, tout en visant à maintenir une balance entre les différents intérêts en jeu, y compris la marge d'appréciation laissées aux États leur

---

[694] Par ex., dans l'affaire Escher c. Brésil de la Cour Interaméricaine des Droits de l'Homme, du 6 juillet 2009, Série C n° 200, les interceptions téléphoniques des membres de deux organisations suspectées d'être connecté au Mouvement « Landless », mouvement rebelle au Brésil. Ou encore, dans l'affaire Amman c. Suisse précitée, une information judiciaire confidentielle a été ouverte contre un vendeur de produits cosmétiques suite à la réception de renseignements de la part du consulat russe, ce qui a entrainé des soupçons quant à son association au mouvement communiste.

[695] Necessary and Proportionate Coalition, *Necessary & Proportionate - International principles on the application of Human Rights to Communications Surveillance*, Final version May 2014: "*Privacy International, in conjunction with the Electronic Frontier Foundation, Access and a range of civil society organisations and academic experts, launched the International Principles on the Application of Human Rights to Communications Surveillanc*e": http://necessaryandproportionate.org/principles

[696] Déclaration universelle des droits de l'homme de 1948, Art. 29 – Devoirs et limitations, al. 2 ; et l'alinéa 1 de cet article dispose que « *L'individu a des devoirs envers la communauté dans laquelle seul le libre et plein développement de sa personnalité est possible.* »

[697] UN Human Rights Committee (HCR), CCPR General Comment N° 27: Art. 12 *(Freedom of Movement*), Adopted at the Sixty-seventh session of the Human Rights Committee, on 2 November 1999, CCPR/C/21/Rev.1/Add.9, General Comment N° 27. (General Comments), §11 ; Disponible en ligne : https://www.refworld.org/docid/45139c394.html

incombant, au titre de l'article 8, dans la mise en œuvre de ce droit et où tout va dépendre de l'intérêt en jeu pour déterminer l'ampleur de cette marge qui, selon l'aspect en cause, va être restreinte ou relativement large. La Cour de Strasbourg est même allée jusqu'à préciser quelles obligations procédurales sont particulièrement adéquates pour déterminer la marge d'appréciation accordée, et procède à un examen des garanties procédurales mises à disposition des individus afin d'évaluer si l'autorité publique n'a pas fixé le cadre réglementaire en outrepassant les limites de son pouvoir discrétionnaire. De plus, les juges affirment que, « *selon la jurisprudence constante de la Cour, même si l'article 8 ne renferme aucune condition explicite de procédure, il faut que le processus décisionnel débouchant sur des mesures d'ingérence soit équitable et respecte comme il se doit les intérêts de l'individu protégés par l'article 8* »[698].

Le principe de légalité invoque que toute limitation au droit au respect de la vie privée doit être prévue expressément par une loi. De telles législations doivent être à la disposition du public, suffisamment accessibles, tout en présentant certaines caractéristiques que sont la clarté, la précision et la prévisibilité afin d'en permettre une meilleure compréhension de la part des individus. La qualité de la loi doit donc être compatible avec la prééminence du droit[699]. Et la Cour européenne des droits de l'homme n'hésite pas à le rappeler : « *les mots «prévu par la loi» impliquent des conditions qui vont au-delà de l'existence d'une base légale en droit interne et exigent que celle-ci soit «accessible» et «prévisible»* »[700].

La loi doit être, en particulier, suffisamment prévisible pour deux raisons d'importance égale : d'une part, permettre aux individus d'agir conformément à la loi, et, d'autre part, définir clairement et nettement l'étendue du pouvoir d'appréciation des États. Dans une affaire relative à des mesures de surveillance secrète, la Cour a ainsi avancé que « *[…] especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated. The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort*

[698] Par ex. : CEDH, Cour (Chambre), Affaire Buckley c. Royaume-Uni du 25 septembre 1996, Requête n° 20348/92, §76, CEDH, Cour (3ème section), Affaire Tanda-Muzinga c. France du 10 juillet 2014, Requête n° 2260/10, §68, et, CEDH, Cour (4ème section), Affaire M. S. c. Ukraine du 11 juillet 2017, Requête n° 2091/13, §70.
[699] CEDH, Cour (Chambre), Affaire Halford c. Royaume-Uni du 25 juin 1997, Requête n° 20605/92, §49.
[700] CEDH, Affaire Amann c. Suisse, requête n° 27798/95, du 16 février 2000, §55.

to any measures of secret surveillance and collection of data »[701]. Et, dans une autre affaire, elle a jugé qu'il y a eu violation de l'article 8 puisque les dispositions du droit suisse sur lesquelles étaient fondées les mesures de surveillance secrètes litigieuses, soumises par la compagnie d'assurance de la requérante, manquaient de clartés et de précisions[702].

Une ligne de conduite est tenue par les juges lors du traitement de ces affaires : celle de savoir si les actions ou les mesures prises par les puissances publiques, réputées comme portant atteinte au droit au respect de la vie privée, ont été entreprises dans le respect de la loi. Dans la plupart des cas, la première position de défense des États est de prétendre que leur législation nationale autorisait les actions contestées et que celles-ci étaient donc prévues par la loi. Dans l'affaire Uzun précitée, par exemple, le gouvernement prétendait que la surveillance du requérant par GPS trouvait une base légale au sein du Code pénal allemand.

Quand bien même la Cour européenne reconnaît l'importance du principe de légalité en matière de violation du droit au respect de la vie privée, elle est peu disposée à admettre des réclamations formelles, dénuées de fonds, stipulant que la législation nationale, à elle toute seule, justifie la violation alléguée. En effet, la Cour a souligné à plusieurs reprises la nécessité de vérifier la conformité de la législation en cause à un critère supplémentaire : la qualité de la loi qui doit être notamment claire et prévisible pour les différents intérêts en cause. Tel que précisé par la Cour, l'expression "prévue par la loi" non seulement exige et impose le respect du droit interne mais porte aussi sur la qualité de cette loi, celle-ci devant être compatible avec l'État de droit et la prééminence du droit[703]. Et elle a noté à maintes reprises que « *consequently, domestic law must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities so as to ensure to individuals the minimum degree of protection to which they are entitled under the rule of law in a democratic society* »[704].

Par ailleurs, le principe de légalité exige l'existence de garanties effectives et appropriées permettant d'assurer le respect des droits des personnes découlant de l'article 8. La responsabilité des autorités publiques relative à la protection de la vie privée implique fréquemment des obligations positives, actives, qui visent à assurer une protection, effective et appropriée, des droits garantis au niveau national. Les juges strasbourgeois ont ainsi estimé que,

[701] CEDH, Cour (1ère section), Affaire Shimovolos c. Russie du 21 juin 2011, Requête n° 30194/09, §68.
[702] CEDH, Cour (3ème section), Affaire Vukota-Bojić c. Suisse du 18 octobre 2016, requête n° 61838/10, §67-68.
[703] CEDH, Cour (Grande ch.), Affaire Bykov c. Russie du 10 mars 2009, Requête n° 4378/02, §76.
[704] CEDH, Cour (4ème section), Affaire Piechowicz c. Pologne du 17 avril 2012, Requête n° 20071/07, §212 ; Voir aussi : CEDH, (4ème section), Affaire Nurzyński c. Pologne du 21 décembre 2010, requête n° 46859/06, §36.

nonobstant la marge d'appréciation de l'État, le droit suédois pertinent, lors de la production de l'acte particulier de filmer en secret une enfant nue (par son beau-père en l'espèce), « *n'assurait pas à l'intéressée une protection de son droit au respect de sa vie privée propre à faire conclure que les obligations positives découlant pour l'État défendeur de l'article 8 de la Convention se trouvaient satisfaites* »[705]. De plus, en matière de surveillance secrète, ils ont souligné que « *in addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law* »[706].

Il est utile de relever qu'il suffit à la Cour européenne de constater que la disposition incriminée n'était pas « prévue par la loi », au sens qu'elle accorde à cette expression, pour conclure à une violation de la vie privée. Par conséquent, elle ne s'attarde plus sur l'examen du « but légitime » poursuivi par la mesure, ou si celle-ci était « nécessaire dans une société démocratique »[707].

L'article 8 indique les cas précis où le but légitime est susceptible de justifier une ingérence dans l'exercice des droits qu'il protège. En observant les pratiques suivies par la Cour, celles-ci s'avèrent être assez succinctes et profondes[708] : bien qu'elle admette que la violation du respect de la vie privée par l'État puisse servir un « but légitime » correspondant à un intérêt public fondamental, cela n'était pas suffisant. C'est une condition qui doit être dûment remplie et respectée afin de pouvoir légitimement justifier l'atteinte portée à ce droit.

Ainsi, elle a affirmé que la prise en compte des intérêts économiques du pays et la protection des droits et libertés d'autrui justifiaient, légitimement, les restrictions apportées lors de l'élaboration de la mesure[709]. En se prononçant sur la loi interdisant la dissimulation du visage dans l'espace public, elle a pris en compte le fait que l'État considère que le visage joue un rôle important dans l'interaction sociale, elle explique qu'elle peut comprendre les cultures et pratiques sociales au sein de la société considérée, qu'elle peut admettre que le port du voile intégral soit perçu par le gouvernement comme portant atteinte au droit d'autrui d'évoluer dans

---

[705] CEDH, Cour (Grande ch.), Affaire Söderman c. Suède du 12 novembre 2013, Requête n° 5786/08, §117.
[706] CEDH, Affaire Shimovolos c. Russie du 21 juin 2011, *Id.*, §68.
[707] CEDH, Cour (2ème section), Affaire M.M. c. Pays bas du 8 avril 2003, Requête n° 39339/98, §46 "*That is enough for the Court to find that there has been a violation of Article 8. It is not necessary to go into whether the interference in question pursued a "legitimate aim" or was "necessary in a democratic society" in pursuit thereof*".
[708] CEDH, Cour (Grande ch.), Affaire S.A.S. c. France du 1er juillet 2014, Requête n° 43835/11, §114 « *La pratique de la Cour est d'être plutôt succincte lorsqu'elle vérifie l'existence d'un but légitime, au sens des seconds paragraphes des articles 8 à 11 de la Convention* ».
[709] CEDH, Cour (Grande ch.), Affaire Hatton et autres c. Royaume-Uni du 8 juillet 2003, Requête n° 36022/97, §121.

un espace de sociabilité facilitant la vie ensemble, mais elle précise que « *cela étant, la flexibilité de la notion de « vivre ensemble » et le risque d'excès qui en découle commandent que la Cour procède à un examen attentif de la nécessité de la restriction contestée* »[710]. Dans une autre affaire, elle a conclu à une violation du respect de la vie privée de la part de l'État défendeur, qui n'a fourni aucune information pour justifier l'ingérence opérée. Elle avance, à cet égard, que même à supposer que certaines dispositions mentionnées par le gouvernement « *puissent passer pour avoir fourni une base légale à l'ingérence en cause, la Cour ne discerne pas quel « but légitime », tel que requis par l'article 8§2, était visé par cette dernière* »[711].

Enfin, la Cour précise que l'immixtion dans la vie privée par un État, qui poursuit un but légitime mais qui n'apparaît pas, toutefois, « nécessaire » pour aboutir à celui-ci, « *méconnaît* » l'article 8 et les droits qu'il protège, sauf si, prévue par la loi, l'atteinte poursuit un des buts légitimes et, « de surcroît, est nécessaire dans une société démocratique » pour les atteindre[712]. À ce titre, pour déterminer si une atteinte particulière est nécessaire dans une société démocratique, elle doit mettre en balance les intérêts étatiques et les intérêts individuels en cause.

Selon une jurisprudence constante de la Cour, il n'est clairement pas suffisant que l'État ait eu une raison légitime de prendre les dispositions constitutives de l'atteinte, de la restriction ou de la sanction. Dès 1976, dans un arrêt de principe, la haute juridiction a précisé que si l'adjectif « nécessaire » n'est pas synonyme « d'indispensable », « *[...] il n'a pas non plus la souplesse de termes tels qu' « admissible », « normal », « utile », « raisonnable » ou « opportun »* »[713]. Ainsi, même en annonçant que les autorités publiques sont les mieux placées pour se prononcer sur la nécessité de l'atteinte portée, leurs accordant en ce sens une marge d'appréciation, elle affirme cependant qu'il n'en appartient pas moins à ces autorités « *de juger, au premier chef, de la réalité du besoin social impérieux qu'implique en l'occurrence le concept de « nécessité »* »[714]. C'est bien une obligation à la charge des États de se prononcer en premier lieu, dans chaque cas et pour chaque mesure, de la réalité et de la nécessité de pareil besoin, préservant de ce fait leur marge d'appréciation. Leurs décisions et dispositions prises restent, toutefois, soumises au contrôle de la Cour. Et celle-ci affirme que, pour se révéler nécessaire dans une société démocratique, « *dont tolérance et esprit d'ouverture constituent deux des*

[710] CEDH, Affaire S.A.S. c. France du 1er juillet 2014, *Id.*, §122.
[711] CEDH, Cour (3ème section), Affaire Toma c. Roumanie du 24 février 2009, Requête n° 42716/02, §92.
[712] CEDH, Cour (Grande Ch.), Affaire Amann c. Suisse du 16 février 2000, Requête n° 27798/95, §71.
[713] CEDH, Cour (Plénière), Affaire Handyside c. Royaume-Uni du 7 décembre 1976, Requête n° 5493/72, §48
[714] CEDH, Affaire Handyside c. Royaume-Uni, *Id.,* §48.

caractéristiques », une atteinte doit, notamment, être proportionnée au but légitime poursuivi[715].

La Cour européenne rejette donc toute interprétation démesurément étroite ou large de la notion de « nécessité », et semble lui appliquer un contrôle de proportionnalité. Quant aux caractéristiques d'une société démocratique, elle ne s'est jamais prononcée sur leurs détails, évoquant uniquement « la tolérance et l'esprit d'ouverture ». Ceci dit, les juges ont souligné, dans le contexte général de l'article 8, l'importance et la prééminence du droit dans une société démocratique, ainsi que le besoin d'empêcher et de restreindre toute intrusion arbitraire dans les droits et libertés reconnus et protégés par la Convention. Cette dernière doit, en outre, être perçue comme un traité de « garantie collective » des droits de l'homme et des libertés fondamentales[716] dont l'esprit général est destiné à sauvegarder et à promouvoir les « idéaux et les valeurs d'une société démocratique »[717]. Globalement, en ce qui concerne le contexte du respect de la vie privée, l'action nécessaire dans une société démocratique se détermine en trouvant un juste équilibre entre les droits de l'individu et l'intérêt de l'État, à travers l'application du principe de proportionnalité. Celui-ci implique que l'exercice des droits d'un individu doit toujours s'apprécier à la lumière de l'intérêt public, général. C'est un des principaux moyens pour parvenir à un juste équilibre, et est fréquemment employé par les juges, aussi bien européens que nationaux, qui rappellent que « [...] *le souci d'assurer un juste équilibre entre les exigences de l'intérêt général de la communauté et les impératifs de la sauvegarde des droits fondamentaux de l'individu est inhérent à l'ensemble de la Convention* »[718].

La Cour strasbourgeoise souligne, *in fine*, que pour déterminer si les mesures incriminées étaient nécessaires dans une société démocratique, il faut considérer l'affaire dans son ensemble afin d'examiner si les motifs invoqués pour les justifier sont « pertinents et suffisants », et si ces mesures sont « proportionnées » aux buts légitimes poursuivis[719]. De plus, la Cour tient compte de la marge d'appréciation laissée aux autorités étatiques[720], mais ces dernières restent tenues de démontrer l'existence d'un besoin social impérieux sous-jacent à l'atteinte[721]. La même attitude est, de manière générale et équivalente, suivie par les jurisprudences judicaires

[715] CEDH, Cour (Plénière), Affaire Dudgeon c. Royaume-Uni du 22 octobre 1981, Requête n° 7525/76, §53.
[716] CEDH, Cour (Plénière), Affaire Irlande c. Royaume-Uni du 18 janvier 1978, Requête n° 5310/71, §239.
[717] CEDH, Cour (Plénière), Affaire Soering c. Royaume-Uni du 7 juillet 1989, Requête n° 14038/88, §87.
[718] CEDH, Affaire Soering c. Royaume-Uni, *Id.*, §89.
[719] CEDH, Cour (Chambre), Affaire Z. c. Finlande du 25 février 1997, Requête n° 22009/93, §94.
[720] La CEDH rappelle dans son affaire Paradiso et Campanelli du 24 janvier 2017, Requête n° 25358/12, §§179-184, les principes directeurs concernant la marge d'appréciation laissée aux États.
[721] CEDH, Affaire Piechowicz c. Pologne du 17 avril 2012, *Id.,* §212.

et constitutionnelles. Et le Conseil constitutionnel a fréquemment relevé que les restrictions apportées par les mesures aux droits et libertés constitutionnellement garantis doivent être « nécessaires », « proportionnées » et ne doivent pas introduire de « discriminations injustifiées »[722].

§2. Les implications du droit au respect de la vie privée en ligne

En ce qui concerne les implications du droit au respect de la vie privée en ligne, elles se traduisent, principalement, par un droit à la protection des données personnelles étendu et autonome (A), ainsi que par un droit à la protection contre les ingérences et les immixtions numériques également vaste et élargi (B).

A. L'étendue du droit à la protection des données personnelles

À travers sa courte histoire, le droit à la protection des données personnelles a connu un bouleversement profond des enjeux qui y sont liés, enjeux qui sont, en réalité, plus large que ceux afférents au respect de la vie privée hors ligne, tels que connus par les générations précédentes. Le souci d'assurer une protection réelle et effective des données personnelles s'est manifesté dès la fin des années 60, et ne cesse de se renouveler depuis. Un cadre stable et assez rigoureux a été ainsi instauré, visant à assurer le même niveau de protection et de garanti que celui du respect de la vie privée dont découle, en particulier, le régime de protection des données personnelles.

En ce sens, l'Assemblée générale des Nations Unies a clairement affirmé que « *les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne, y compris le droit à la vie privée* »[723]. L'Assemblée a, par ailleurs, au lieu de simplement les y inviter, demandé aux États, de respecter et de protéger le droit à la vie privée, y compris dans le contexte de la communication numérique, mais aussi, de revoir leurs procédures, pratiques et législations relatives à la surveillance et à l'interception des communications et à la collecte de données personnelles, « *notamment à grande échelle* », dans le souci de défendre le droit à la vie privée, en insistant sur la nécessité pour les États de veiller à respecter pleinement et effectivement toutes leurs obligations au regard du droit international des droits de l'homme[724]. De plus, tout

[722] Décision n° 2010-25 QPC du 16 septembre 2010, *op. cit.,* Cons. 11, p. 7.
[723] Résolution 68/167, *Le droit à la vie privée à l'ère du numérique*, adoptée par l'Assemblée générale le 18 décembre 2013, Soixante-huitième session, A/RES/68/167, p. 2.
[724] Résolution 69/166, *Le droit à la vie privée à l'ère du numérique*, adoptée par l'Assemblée générale le 18 décembre 2014, 73e séance plénière (A/RES/69/166), point 4, p. 4.

en constatant que les métadonnées ont la capacité d'offrir des avantages, l'Assemblée relève cependant que « *certains types de métadonnées peuvent aussi, par agrégation, révéler des informations personnelles et donner une idée du comportement, des relations sociales, des préférences personnelles et de l'identité de particuliers* »[725], et doivent donc faire l'objet de protection au même titre que la protection des données.

Texte fondateur, la loi Informatique et libertés de 1978, rédigée sur la base des recommandations du Rapport Tricot remis le 27 juin 1975, a été la première à reconnaître le droit à la protection des données personnelles sans nécessairement les nommer. À l'époque de sa rédaction, elle ne pouvait envisager le développement et la croissance d'internet, ni celle de la puissance de calcul ou de la valeur économique acquise par les données et leurs traitements. Et pourtant, le cadre légal issu de cette loi pour la protection des données s'est avéré être d'une grande stabilité et n'a subi que quelques réformes notables, pour transposer la directive européenne de 1995 par exemple, et, à partir de 2016, par les lois et ordonnances visant à consolider le texte de la loi en question pour l'harmoniser et le rapprocher du RGPD, désormais entré en application depuis le 25 mai 2018. À l'heure actuelle, pour avoir une meilleure conception et compréhension de ce cadre juridique relatif à la protection des données personnelles, il faut nécessairement entreprendre, comme l'a observé la CNIL, une lecture combinée du Règlement européen sur la protection des données et certaines dispositions nationales, prises au titre des marges de manœuvre laissées aux États par ledit Règlement, produisant par conséquent le nouveau texte de la loi du 6 janvier 1978 ainsi consolidée. Dans son avis sur le projet de loi relatif à la protection des données personnelles, la CNIL annonce ainsi que « *cette combinaison d'un Règlement et de textes nationaux remplacera le corpus unique que constitue aujourd'hui la loi de 1978* »[726].

Comme il a été précédemment vu, cette loi reste quelque part associée dans la mémoire collective à l'émotion provoquée suite au projet SAFARI[727] révélé dans un article intitulé « Safari ou la chasse aux Français »[728]. Ce projet aspirait à rassembler les différentes fiches dispersées dans différents services de police, et manifestait une volonté de les interconnecter avec d'autres fichiers de différents services (cadastre, impôt, etc.) ; et le numéro INSEE attribué

[725] Résolution 69/166, *Le droit à la vie privée à l'ère du numérique*, *Id.*, p. 2.
[726] Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978 (demande d'avis n°17023753), Commission nationale de l'informatique et des libertés, p. 4 ; disponible en ligne : https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf
[727] *Cf.* p. 72 et s.
[728] Article de Philippe Boucher, Le Monde, 21 mars 1974, p. 9 ; disponible en ligne : http://bugbrother.blog.lemonde.fr/files/2010/12/le_monde_-_21_03_1974_009_800_px.1292949083.jpg

à tout individu aurait servi d'identifiant unique permettant cette interconnexion. Ayant suscitée beaucoup de ripostes, cette affaire a entraîné de nombreuses réactions publiques dont une circulaire de 1974 du Premier ministre interdisant toute nouvelle interconnexion entre les systèmes informatiques des ministères[729], ainsi que la constitution d'une Commission informatique et libertés chargée de la rédaction d'un rapport, qui fut nommé rapport Tricot[730]. Ceci a débouché à l'élaboration et à l'adoption de la loi Informatique et libertés afin de protéger les citoyens du fichage administratif et policier. En effet, l'interconnexion, mis à part son aspect purement technique qui sert à relier deux machines, organes périphériques informatiques, présente une autre aspiration, « *celle de rapprocher différents systèmes de traitement afin de permettre des interrogations, des réponses, des échanges qui enrichiront chaque système grâce aux apports des autres* »[731]. Elle se caractérise alors par une double prétention, facilement observée à l'heure actuelle, une interconnexion technique entre les équipements informatiques ainsi qu'une communication fonctionnelle entre les systèmes.

Ceci dit, il est important de relever que d'autres travaux avaient précédé ceux mentionnés : le Conseil d'État français, à l'occasion d'une réflexion conduite en 1969[732], avait annoncé que « *les Français vont donc vivre dans une civilisation de l'information* [où] *la recherche de l'information devient une activité rentable, sa détention une source de puissance* » et avait déjà en quelque sorte identifié le risque d'établissement de « banques de données » dans lesquelles seraient regroupées et interconnectées toute sorte d'informations concernant une personne. De même, la Suède avait adopté en 1973 une loi sur la protection des données[733], l'Allemagne en 1977 une loi fédérale portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement de données[734], ainsi que d'autres législations dans les Länder (notamment de Hesse et de Bavière), le Danemark en 1978 avait adopté une loi sur les registres privés et une autre sur les registres des pouvoirs publics[735], la Finlande en 1987 sur les

[729] Circulaire du Premier ministre du 29 mars 1974 : voir, par exemple, Rapport Tricot de la Commission informatique et libertés remis le 27 juin 1975 (décret n° 74.938 du 8 novembre 1974), La Documentation française (410), p. 55 et Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *op. cit.,* p. 70.
[730] Rapport Tricot de la Commission informatique et libertés remis le 27 juin 1975, *Id.*
[731] Rapport Tricot de la Commission informatique et libertés remis le 27 juin 1975, *Ibid.*, p. 56.
[732] Conseil d'État, *Les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives,* Rapport annuel de 1969-1970, La Documentation française.
[733] Loi du 11 mai 1973 sur la protection des données, Suède.
[734] Loi fédérale du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement de données, modifiée par la loi fédérale de protection des données du 20 décembre 1990 et amendée par la loi du 14 septembre 1994, République fédérale d'Allemagne.
[735] Loi n° 293 du 8 juin 1978 sur les registres privés et loi n° 294 du 8 juin 1978 sur les registres des pouvoirs publics, amendées en 1988 et en 1991, Danemark.

fichiers de données à caractère personnel[736]. Et du côté du Continent américain, le cadre légal sur la protection des données personnelles résulte d'une combinaison de lois sectorielles particulières : dans le secteur public, le *Privacy Act* de 1974[737] établit un *Code of fair information practices*[738] (Code des pratiques d'information « justes ») qui gouverne la collecte, la conservation, l'utilisation et la dissémination d'information concernant des particuliers. Six pratiques générales peuvent être dégagées de ce code de pratiques : limitation des conditions de divulgation d'information (et pouvoir en rendre compte)[739], possibilité d'accès aux informations[740], limitation de la finalité (sauf accord ou consentement préalable)[741], possibilité de modifier des informations[742], interdiction de systèmes d'enregistrement secret des données[743] et la sécurité des informations[744] ; pratiques désormais prévues par le RGPD[745]. Par ailleurs, le *Privacy Act* distingue une catégorie particulière de données « sensibles », à savoir « *record describing how any individual exercises rights guaranteed by the First Amendment*[746] », dont la conservation est, en principe, interdite sauf autorisation exprès ou si elle se trouve être légalement pertinente[747].

Du côté des acteurs privés, seules certaines catégories de données font l'objet d'une protection législative : les données de communications électroniques[748], les données de santé[749], les

[736] Loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant la police, Finlande.
[737] The Privacy Act of 1974, 5 U.S.C. § 552a (2012), U.S. Department of Justice, Office of Privacy and Civil Liberties; Disponible en ligne: https://www.justice.gov/opcl/file/844481/download
[738] Department of Justice's Office of Privacy and Civil Liberties (OPCL), "Overview of the Privacy Act of 1974", 2015 Edition, The United States Department of Justice: https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition
[739] The Privacy Act of 1974, *Id.*, Sections (b) Conditions of disclosure & (c) Accounting of certain disclosures.
[740] The Privacy Act of 1974, *Id.*, Section (d) Access to records.
[741] The Privacy Act of 1974, *Ibid.*, Section (e) Agency requirements.
[742] The Privacy Act of 1974, *Ibid.*, Section (f) Agency rules, Subsection (4).
[743] The Privacy Act of 1974, *Ibidem*, Section (e) Agency requirements, Subsections (2 & 3).
[744] The Privacy Act of 1974, *Ibidem*, Section (e) Agency requirements, Subsection (10).
[745] *Cf.* p. 198 et s., 232 et s., 271 et s.
[746] First Amendment - Religion and Expression "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances*", U.S. Constitution, Passed by Congress September 25, 1789 (Ratified December 15, 1791) The first 10 amendments form the Bill of Rights.
[747] The Privacy Act of 1974, *Id.*, Section (e) Agency requirements, Subsection (7) "*maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity*;"
[748] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510: https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap119-sec2510.pdf
[749] The Health Insurance Portability and Accountability Act of 1996 (HIPAA): https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

données de mineurs[750] ainsi que les données financières[751]. Il est vrai que le quatrième amendement de la Constitution américaine assure une protection générale de la vie privée des individus, mais sa portée a cependant été limitée, dès 1967, par la Cour Suprême ayant adoptée une conception restrictive du droit à la vie privée[752]. De plus, en ce qui concerne les acteurs du secteur privé non visés par des lois spécifiques, un code de bonne conduite a été mis en place par la Federal Trade Commission (FTC) mais qui n'est, toutefois, que facultatif, fournissant de simples recommandations et pratiques à suivre[753]. Dès le début des années 70, il a donc semblé évident aux divers gouvernements que le droit au respect de la vie privée ne permettait pas, à lui seul, d'englober les différents enjeux qui peuvent désormais atteindre les données personnelles, malgré le fait que ce droit établit le socle et le niveau de protection nécessaire. Certes, les notions de « vie privée » et de « données personnelles » sont étroitement liées, mais cette dernière semble dépasser le cadre de la première de sorte qu'un droit fondamental autonome, méritant un cadre de protection bien particulier, émerge.

La loi Informatique et libertés a fait des choix fondamentaux qui se justifient jusqu'à aujourd'hui : comme il a été précédemment indiqué[754], elle a adopté une approche transversale qui couvre l'ensemble des données personnelles, désignées à l'époque « informations nominatives », ainsi qu'une approche généraliste visant les traitements des secteurs public et privé ; elle a reconnu des droits aux individus sur leurs informations et a instauré la CNIL, autorité administrative indépendante chargée de veiller au respect de cette loi et des droits qu'elle protège. Ce cadre structurel est jusqu'à présent celui adopté par les instruments juridiques nationaux, internationaux et européens pour la protection des données personnelles. Il a subi quelques modifications pour s'adapter à l'essor et à la croissance du numérique, mais constitue, néanmoins, le socle de référence en matière de protection des données personnelles.

---

[750] Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. 6501–6505, FTC: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule & http://www.coppa.org

[751] The Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. 1681 et *sq*. : https://www.govinfo.gov/content/pkg/CFR-2011-title16-vol1/pdf/CFR-2011-title16-vol1-chapI-subchapF.pdf

[752] U.S. Supreme Court, Katz v. United States, 389 U.S. 347 (1967): https://supreme.justia.com/cases/federal/us/389/347/

[753] Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress, FTC, May 2000: https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission, Start with Security: A Guide for Business, FTC, June 2015: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business, Protecting Personal Information: A Guide for Business, FTC, October 2016: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business & The FTC's Endorsement Guides: What People Are Asking, FTC, September 2017: https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking

[754] *Cf.* p. 74-75.

Le régime mis en place dans le contexte de cette loi dénotait une grande méfiance vis-à-vis de l'informatique publique : l'encadrement des traitements était différent selon qu'il fût mis en œuvre pour le compte de personnes publiques ou privées. Par conséquent, les traitements d'informations nominatives opérés pour le compte de personnes publiques ou de personnes privées chargées d'une mission de service public sont soumis à un régime d'autorisation (acte réglementaire pris après avis de la CNIL), et ceux, quasi-inexistants à l'époque, mis en œuvre par des personnes privées à une obligation de déclaration[755]. Une autre méfiance manifestée était le risque potentiel engendré par l'interconnexion ou encore le recours à identifiant unique : comme ont pu le souligner les parlementaires en 1977, « *est également très important le problème de l'interconnexion des fichiers, de l'existence d'un identifiant unique, comme le numéro de sécurité sociale ou le numéro national d'identité. C'est moins un problème technique que politique car on peut rapprocher aisément des fichiers même sans identifiant unique. L'interdiction pure et simple paraît inopérante* »[756]. Intervient en 2004 la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[757], pour transposer la directive européenne de 1995 relative à la protection des données à caractère personnel[758] et modifier la loi de 1978. Même à l'époque de son adoption, elle est directement apparue datée mais a, cependant, permis d'éliminer la distinction entre acteurs publics et privés soumis à des régimes distincts, désormais unanimement soumis à une obligation de déclaration. À partir de 2016, les réformes se sont toutefois multipliées en comparaison aux années précédentes, tout en conservant la base du régime de protection initialement mis en place : entrent alors en scène, le RGPD le 27 avril 2016, la loi pour une République numérique le 7 octobre 2016 et, dernièrement, la loi sur la protection des données personnelles le 20 juin 2018[759] et l'ordonnance prise en application de cette dernière le 12 décembre 2018[760].

---

[755] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit.*, p. 5783: « *C'est pourquoi le projet prévoit que les dispositions légales s'appliqueront seulement aux traitements automatisés d'informations nominatives, les seules qui soient vraiment dangereuses pour la vie privée et pour les droits individuels des citoyens, et distingue selon que le traitement sera mis en œuvre par une personne morale de droit public ou une personne morale gérant un service public — cela vise les organismes de sécurité sociale — d'une part, ou par une personne physique ou morale privée, d'autre part*. »

[756] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *Id.,* p. 5786.

[757] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[758] Directive 95/46 du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée, Date de fin de validité : 24/05/2018.

[759] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[760] Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6

Au-delà de ce cadre législatif, ce droit fondamental que représente la protection des données personnelles fait également l'objet d'une protection et d'une extension par les instruments juridiques internationaux et européens, le droit souple ainsi que la jurisprudence qui ont, simultanément, joué un rôle dans l'interprétation et dans la contribution au respect des dispositions relatives à la protection des données, les adaptant au fur et à mesure, et, en fonction des besoins, aux évolutions des technologies et des usages numériques. Ayant collectivement adopté une approche similaire, ces divers instruments et institutions juridiques consacrent le droit à la protection des données personnelles, permettant ainsi de l'inscrire à un « *niveau supérieur à celui de la loi dans la hiérarchie des normes* »[761]. Pour illustration, la Convention 108 qui présente un champ d'application général impliquant tous les traitements publics et privés, une approche transversale englobant toutes sortes d'informations, une reconnaissance des droits et garanties des personnes, des prohibitions concernant la collecte et/ou la conservation ainsi que certaines autres dispositions générales encadrant les traitements de données personnelles, à l'image même du cadre adopté par le texte de la loi informatique et libertés. Elle a, de plus, introduit la notion de « qualité des données » imposant 5 principes : collecte et traitement loyal et licite, enregistrement pour des finalités « déterminées et légitimes », proportionnalité des données collectées par rapport à ces dernières, exactitude et mise à jour des données et, enfin, proportionnalité de la durée de conservation des données par rapport aux finalités[762]. L'influence des lignes directrices de l'OCDE, adoptées en 1980, régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel[763] fournit également une autre illustration de ce corpus juridique, de plus en plus large, relatif à la protection des données personnelles et, *in fine*, à la protection de la vie privée numérique.

---

janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

[761] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, op. cit*., p. 76.

[762] Convention n° 108, Art. 5 – Qualité des données : « *Les données à caractère personnel faisant l'objet d'un traitement automatisé sont :*

a. *Obtenues et traitées loyalement et licitement ;*
b. *Enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ;*
c. *Adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ;*
d. *Exactes et si nécessaire mises à jour ;*
e. *Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées* ».

[763] Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel du 23 septembre 1980, Organisation de Coopération et de Développement Économiques (OCDE) ; disponible en ligne : http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm

En outre, la Charte des droits fondamentaux protège, tout en les distinguant, les données personnelles et le respect de la vie privée soulignant, de ce fait, l'importance de protéger ces deux libertés, de manière égale mais interconnectée[764]. Ce choix de les distinguer s'explique, selon les commentaires de G. Braibant vice-président de la « convention » chargée de l'élaboration de la Charte, par l'importance des enjeux de protection des données personnelles : « *avec la bioéthique, l'informatique est l'un des domaines importants des évolutions scientifiques et techniques du XX^e Siècle qui affectent la liste des droits fondamentaux* »[765].

Du côté de la justice, la Cour européenne des droits de l'homme a construit une jurisprudence en la matière en dépit de l'absence de cette distinction dans le texte de la Convention, et juge que « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention* »[766].

Et en 2012, le Conseil Constitutionnel français a précisé les implications du droit à la vie privée en ce qui concerne la protection des données personnelles, en affirmant que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* »[767].

Cela dit, le Haut-Commissaire des Nations-Unies aux droits de l'homme a néanmoins pu souligner, dans son rapport de 2014, que « *l'accent mis sur le contrôle de la collecte et de la conservation des données, bien qu'important, pourrait ne plus suffire à protéger la vie privée du fait en partie que les données massives autorisent de nouveaux modes d'utilisation des données, inventifs et d'une puissance étonnante* »[768].

---

[764] Charte des droits fondamentaux de l'Union Européenne de 2000 :
Art. 7 – Respect de la vie privée et familiale : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.* »
Art. 8 – Protection des données à caractère personnel :
« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

[765] G. BRAIBANT, *La Charte des droits fondamentaux de l'Union Européenne : témoignages et commentaires,* Paris, Ed. Seuil, 2001, p. 112.

[766] CEDH, Affaire S. et Marper, *loc. cit.,* §103.

[767] Conseil Constitutionnel, Décision du 22 mars 2012, Loi relative à la protection de l'identité, *loc. cit.,* Cons. 8.

[768] Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, Le droit à la vie privée à l'ère du numérique, 30 juin 2014, Vingt-septième session, A/HRC/27/37, §18, p. 7.

B. L'étendue du droit à la protection contre les ingérences et immixtions numériques

Dans sa résolution sur le droit au respect de la vie privée à l'ère numérique, l'Assemblée générale des Nations-Unies a réaffirmé que le droit international des droits de l'homme constitue le cadre universel au regard duquel tout atteinte à la vie privée doit être mesurée. Elle précise ainsi, conformément à l'article 12 de la Déclaration universelle des droits de l'homme[769] et à l'article 17 du Pacte international relatif aux droits civils et politiques[770], l'importance et l'étendue du droit à la vie privée notamment face au rythme soutenu du développement des nouvelles technologies de l'information et de la communication. Et l'Assemblée réaffirme « *le droit à la vie privée selon lequel nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance et le droit de toute personne à la protection de la loi contre de telles immixtions [...]* »[771]. Comme il a été préalablement vu, plusieurs dispositions analogues peuvent être retrouvées dans divers instruments internationaux relatifs aux droits de l'homme, ainsi que dans différentes législations nationales ou européennes reconnaissant, *inter alia*, le droit de chacun au respect de sa vie privée et familiale, de son domicile et de sa correspondance, le droit à la reconnaissance et au respect de sa dignité, de son intégrité ou de sa réputation. Que ce soit dans la législation ou dans la pratique, l'importance primordiale et la valeur fondamentale et constante du droit à la vie privée ainsi que la nécessité d'en assurer une protection réelle sont universellement reconnues. En outre, l'exercice du droit à la vie privée « *est important pour la réalisation de la liberté d'expression, du droit de ne pas être inquiété pour ses opinions et du droit de réunion pacifique et de libre association* »[772], et constitue, *ipso facto*, « *l'un des fondements d'une société démocratique* »[773].

Il est important de noter que le droit à la vie privée a la capacité d'être lié à plusieurs autres droits ou libertés, et que le libre exercice de ce droit est fondamental pour réaliser ces divers droits et libertés mentionnés : libertés d'opinion et d'expression, droit à la liberté d'association et de réunion pacifique, droit de rechercher, recevoir et transmettre des informations, droit à la

[769] Déclaration universelle des droits de l'homme, 10 décembre 1948, Art. 12 : « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* »

[770] Pacte international relatif aux droits civils et politiques du 16 décembre 1966, Art. 17 : « *1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.*
2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

[771] Résolution 68/167 « Le droit à la vie privée à l'ère du numérique » adoptée par l'Assemblée générale le 18 décembre 2013 au cours de sa Soixante-huitième session, Assemblée générale des Nations-Unies, A/RES/68/167, p. 1.

[772] Résolution 69/166. Le droit à la vie privée à l'ère du numérique, *loc. cit*., p. 2, et Résolution 68/167, *Id.,* p. 1.

[773] Résolution 69/166, *Id.*, p. 2, et Résolution 68/167, *Ibid.,* p. 1.

santé, ou droit à l'anonymat ou au secret. Le droit au secret est, par exemple, établi comme étant un des droits essentiels de « *notre société libre* », et représente « *la condition d'existence d'une liberté individuelle* »[774]. Toutefois, il apparaît actuellement impossible d'avancer que l'homme moderne, envahi et dépendant des technologies de l'information et de la communication, dispose d'un droit au secret effectif face aux manifestations continues de surveillances de masse, d'interceptions de communications numériques ou encore de collectes de données et de métadonnées. Comme ont pu le constater les parlementaires français en 1977, « *si la vie privée de chacun n'est pas protégée, eh bien ! la liberté n'est plus qu'une liberté surveillée. Chacun a droit à un domaine réservé que recouvrent le silence et, un jour, l'oubli* »[775].

Pour des préoccupations relatives à l'ordre public et à la sécurité publique, des dispositions prévoyant la surveillance et l'interception des données des communications électroniques peuvent représenter des mesures nécessaires et efficaces, poursuivant des objectifs légitimes au sens des conventions et des législations en la matière. Cela dit, les révélations faites concernant les surveillances numériques de masse, dorénavant plus facilement entreprises, mènent à des interrogations quant à la conformité de ces pratiques aux normes et garanties juridiques nationales et internationales. Si la prévention et la répression du terrorisme sont des activités d'intérêt public revêtant une grande importance, il n'empêche que les États doivent veiller à ce que toute mesure prise soit conforme aux obligations faites par les dispositions nationales et internationales. Autrement dit, la mesure ne doit pas se traduire par une immixtion arbitraire ou illégale dans la vie privée, la famille, le domicile ou la correspondance d'une personne, et l'État est tenu de prendre des dispositions spécifiques assurant la protection des personnes contre de telles immixtions. En effet, la surveillance illicite ou arbitraire ou l'interception des communications, ainsi que la collecte illicite ou arbitraire de données personnelles constituent « *des agissements des plus intrusifs* »[776] et sont « *des actes extrêmement envahissants* »[777].

En ce sens, la mesure prévoyant l'ingérence, telle que la surveillance des communications numériques, doit être conforme aux obligations nationales et internationales, qu'elles soient actives ou passives, reposer sur un cadre juridique suffisamment accessible à tous, clair, précis, complet et non discriminatoire, et aucune limitation du droit à la vie privée prévue *« ne doit être arbitraire ou illicite, ni déraisonnable au regard des objectifs légitimes poursuivis* »[778].

---

[774] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *op. cit.*, p. 5787.
[775] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *Id.*, p. 5787.
[776] Résolution 69/166, *Id.*, p. 3.
[777] Résolution 68/167, *Id.,* p. 2.
[778] Résolution 69/166, *Id.*, p. 3.

Les nombreuses dispositions sur le droit à la vie privée prévoient la protection contre les ingérences ou les immixtions arbitraires ou illégales dans la vie privée des personnes, mais aussi contre toute atteinte illégale à leur honneur, dignité ou réputation. Dans son Observation générale n° 16, le Comité des droits de l'homme précise que le droit protégé par ces dispositions « *doit être garanti contre toutes ces immixtions et atteintes, qu'elles émanent des pouvoirs publics ou de personnes physiques ou morales* »[779].

Au regard de tout ce qui a été analysé, plusieurs législations, textes, conventions, organes, comités ou institutions juridiques ont fourni des orientations et des précisions quant au contenu et au champ du droit à la vie privée, ainsi qu'au sens à donner à une ingérence ou une immixtion dans la vie privée d'un individu. Ainsi, le respect de ces dispositions exige que l'intégrité et le caractère confidentiel de la correspondance soient garantis en fait et en droit, en ce sens que « *la correspondance doit être remise au destinataire, sans interception, sans être ouverte, et sans qu'il en soit pris autrement connaissance* »[780]. Certains suggèrent que la communication et l'échange numériques de données personnelles supposent un compromis selon lequel les personnes livrent volontairement, en toute connaissance de cause, les informations qui les concernent ainsi que les relations qu'ils entretiennent en échange de l'accès numérique, la plupart du temps promu comme gratuit, à des biens, des services et des données. Il paraît toutefois raisonnable de s'interroger sur la mesure à laquelle les internautes sont réellement conscients de ce qu'ils partagent, avec qui, de quelle manière ou encore de l'usage potentiel qu'il en sera fait. L'Assemblée générale des Nations Unis s'est ainsi dite, à plusieurs reprises, « *profondément préoccupée par l'incidence néfaste que la surveillance ou l'interception des communications, y compris en dehors du territoire national, ainsi que la collecte de données personnelles, en particulier lorsqu'elle est effectuée à grande échelle, peuvent avoir sur l'exercice des droits de l'homme* »[781].

Par ailleurs, d'autres soulèvent que l'interception ou la collecte de données sur une communication, et non sur le contenu de celle-ci, ne constitue pas à elle seule une ingérence dans la vie privée. Or, au regard de l'étude extensive du droit à la vie privée, cette distinction n'est pas convaincante[782]. Les métadonnées permettent, à l'heure actuelle, de fournir des indications sur la conduite d'un individu, sa localisation, ses relations, ses préférences ou son

[779] Comité des Droits de l'Homme, Observation générale n° 16 : Art. 17 (Droit au respect de la vie privée), Trente-deuxième session (28 septembre 1988), Documents officiels de l'Assemblée générale, quarante-troisième session, Supplément n° 40 (A/43/40), annexe VI, § 1.
[780] Comité des Droits de l'Homme, Observation générale n° 16, (A/43/40) annexe VI, *Id.,* §8.
[781] Résolution 68/167, *Id.,* p. 2, et, Résolution 69/166, *Id*., p. 3.
[782] *Cf.* p. 182.

identité, allant parfois bien au-delà de ce qui peut être obtenu par l'accès ou la collecte du contenu d'une communication. Comme l'a observé la Cour de justice de l'Union, « *ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* », alors même que les contenus des communications n'étaient pas conservées[783]. Par conséquent, toute collecte de données sur les communications peut potentiellement constituer une ingérence dans la vie privée, sans oublier que la collecte et la conservation de ces données constituent également une immixtion, que les données soient ou non consultées ou utilisées par la suite.

Ainsi, la CEDH a déclaré, à de nombreuses reprises, que toute mémorisation de données relatives à la vie privée constitue une ingérence en soulignant que « *l'utilisation ultérieure des informations mémorisées importe peu* »[784]. La simple existence d'une possibilité d'intercepter une information relative à des communications, créant une « menace de surveillance », établie à elle seule une ingérence dans la vie privée[785], et peut également être attentatoire à d'autres droits, sans avoir besoin de « *spéculer sur le caractère sensible ou non des éléments recueillis ni sur les éventuels inconvénients subis* »[786]. Dans ce contexte, la simple existence d'un programme de surveillance, de masse ou secret, constitue une ingérence dans la vie privée et, selon le Comité des droits de l'homme, « *la surveillance, par des moyens électroniques ou autres, l'interception des communications téléphoniques, télégraphiques ou autres, l'écoute et l'enregistrement des conversations devraient être interdits* »[787]. Il reviendra donc à l'État de démontrer que l'immixtion ou l'ingérence caractérisant l'atteinte au droit à la vie privée n'est ni arbitraire ni illégale.

Il s'ensuit un contrôle assez analogue à celui entrepris en cas d'atteinte portée au droit au respect de la vie privée. Dans son Observation générale n° 16, le Comité souligne que l'adjectif « illégal » signifie qu'aucune immixtion ne peut avoir lieu « *sauf dans les cas envisagés par la*

[783] CJUE, arrêt de la Cour (Grande ch.), Digital Rights Ireland et autres du 8 avril 2014, Affaires jointes C-293/12 et C-594/12, §§ 26, 27, 28 et 37.
[784] Par ex. : CEDH, Cour (Chambre), Leander c. Suède du 26 mars 1987, requête n° 9248/81, §48 ; CEDH, Affaire Amann c. Suisse, *loc. cit.*, §69 ; CEDH, Affaire S. et Marper c. Royaume-Uni, *loc. cit.,* §67.
[785] Par ex. : CEDH, Cour (3ème Section), Affaire Weber et Saravia c. Allemagne du 29 juin 2006, requête n° 54934/00, §78, et CEDH, Cour (Plénière), Affaire Malone c. Royaume-Uni du 2 août 1984, requête n° 8691/79, §64.
[786] CEDH, Affaire Amann c. Suisse, *Id.*, §70.
[787] Comité des Droits de l'Homme, Observation générale n° 16, (A/43/40) annexe VI, *Id.,* §8.

loi »[788]. Une ingérence n'est autorisée que si elle est prévue par une loi qui doit elle-même être conforme à des dispositions, et poursuivre des buts et des objectifs légitimes. Autrement dit, une ingérence peut être prévue par une loi qui peut, néanmoins, être illégale si elle n'est pas conforme à la Déclaration universelle des droits de l'homme, ou au Pacte international relatif aux droits civils et politiques ou à la Convention de sauvegarde des droits de l'homme. En ce sens, la Cour de Strasbourg a déclaré, dès 1978, que les États ne disposent pas « *d'une latitude illimitée pour assujettir* », à des mesures de surveillance ou de collecte, les personnes soumises à leur juridiction, et rajoute que, « *consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre […]* », les États ne sauraient prendre, au nom de la lutte contre le terrorisme ou la préservation de l'ordre public ou autre, « *[…] n'importe quelle mesure jugée par eux appropriée* »[789].

Quant au terme « arbitraire », même lorsqu'il n'a pas été expressément nommé, il vise les immixtions arbitraires y compris celles prévues par une loi. Toute ingérence dans la vie privée prévue par la loi doit être conforme aux dispositions légales en la matière et aux finalités légitimes qui, dans certains cas, sont limitativement énumérés, comme dans la Convention de sauvegarde par exemple. Le Comité a, à ce titre, expliqué que cette notion d'arbitraire a été principalement introduite pour garantir la conformité de toute immixtion envisagée afin qu'elle soit, dans tous les cas, « raisonnable eu égard aux circonstances particulières »[790]. Lors de l'affaire *Toonen* porté devant lui, le Comité des droits de l'homme a eu l'occasion de préciser l'interprétation de l'adjectif « raisonnable », cité dans son Observation, qui implique que, pour être raisonnable, toute ingérence dans la vie privée doit être proportionnée au but recherché et doit être nécessaire dans les circonstances propres à chaque cas[791].

Des indications sur le sens des termes « arbitraire et illégal » peuvent être tirées des nombreuses sources nationales et internationales : des principes de Syracuse concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations et comprennent, notamment, des principes généraux d'interprétation applicables en

[788] Comité des Droits de l'Homme, Observation générale n° 16, (A/43/40) annexe VI, *Ibid.,* §3.
[789] CEDH, Cour (Plénière), Affaire Klass et autres c. Allemagne du 6 septembre 1978, Requête n° 5029/71, série A n° 28, §49.
[790] Comité des Droits de l'Homme, Observation générale n° 16, (A/43/40) annexe VI, *Id.,* §4.
[791] Comité des Droits de l'Homme, Communication N° 488/1992, Toonen c. Australie, 31 mars 1994, U.N. Doc CCPR/C/50/D/488/1992 (1994), §8.3 : « *As to whether it may be deemed arbitrary, the Committee recalls that pursuant to its General Comment 16[32] on article 17, the "introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by the law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the circumstances".(4) The Committee interprets the requirement of reasonableness to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.*».

matière de justification des restrictions[792] ; des observations générales du Comité des droits de l'homme, en particulier des Observations générales n[os] 16[793], 27[794], 29[795], 31[796] et 34[797], ou des constatations émises lors des communications ou requêtes individuelles[798] ; des jurisprudences nationales, régionales et internationales[799] ; d'avis d'experts indépendants[800]. La multiplicité de ces sources étend l'interprétation des termes en question sans pour autant affecter sa base, mais plutôt en la concrétisant : collectivement, elles mettent en évidence l'importance des grands principes de légalité, de nécessité et de proportionnalité. Par conséquent, toute restriction, atteinte ou ingérence au droit à la vie privée doit être prévue par la loi, celle-ci devant être accessible, claire et précise permettant de vérifier qui est autorisé et dans quelles circonstances, nécessaire pour atteindre un but légitime, mais aussi proportionnée à ce but, constituant *ipso facto* l'option la moins intrusive possible. Pour reprendre les propos du Conseil d'État, « *l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, […], d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectuées de manière adéquate et proportionnée au regard de ces finalités* »[801].

---

[792] Commission des droits de l'hommes, État des Pactes internationaux relatifs aux droits de l'homme, 28 septembre 1984, Quarante et unième session, Conseil économique et social des Nations Unis, E/CN.4/1985/4, Annexe « Principes de Syracuse concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations », p. 4.
[793] Comité des Droits de l'Homme, Observation générale n° 16, (A/43/40) annexe VI, *Id.*
[794] Comité des Droits de l'Homme, Observation générale n° 27 : Liberté de circulation (art.12), U.N. Doc. CCPR/C/21/Rev.1/Add.9 (1 novembre 1999).
[795] Comité des Droits de l'Homme, Observation générale n° 29 : États d'urgence (art. 4), CCPR/C/21/Rev.1/Add.11 (adoptée le 24 juillet 2001 à sa 1950e session).
[796] Comité des Droits de l'Homme, Observation générale n° 31 : La nature de l'obligation juridique générale imposée aux États parties au Pacte (Quatre-vingtième session), U.N. Doc. CCPR/C/21/Rev.1/Add.13 (26 mai 2004).
[797] Comité des Droits de l'Homme, Observation générale n° 34 : Liberté d'opinion et liberté d'expression (art. 19), CCPR/C/GC/34 (12 septembre 2011).
[798] Par ex. : Comité des Droits de l'Homme, Communication N° 488/1992, Toonen c. Australie, *Id.,* et, Communication N° 903/1999, Antonius Cornelis Van Hulst c. Pays-Bas, 5 novembre 2004, U.N. Doc. CCPR/C/82/D/903/1999 (2004).
[799] Par ex. : CEDH, affaire Uzun c. Allemagne, du 02 septembre 2010, *loc. cit.,* et, Affaire Weber et Saravia c. Allemagne du 29 juin 2006, *loc. cit.* ; et Cour Interaméricaine des Droits de l'Homme, Escher et autres c. Brésil, interprétation, 20 novembre 2009, série C, n° 208.
[800] Par ex. : Rapports du Haut-Commissariat des Nations Unis sur la promotion et la protection du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles (A/HRC/28/39), Rapport sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (A/HRC/28/38), Rapport sur le rôle de la prévention dans la promotion et la protection des droits de l'homme (A/HRC/28/30), et les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications, *op. cit.,* disponible à l'adresse: https://fr.necessaryandproportionate.org/text.
[801] Conseil d'État, Assemblée, Décision Association pour la promotion de l'image du 26 octobre 2011, requête n° 317827, Recueil Lebon, p. 505.

De plus, les États doivent démontrer que l'immixtion permettra de réaliser l'objectif énoncé tout en étant compatible avec d'autres droits de l'homme, et sans vider le droit de son sens. Si l'ingérence prévue ne répond pas à ces critères, elle sera déclarée illégale et/ou l'atteinte portée au droit sera arbitraire. De nos jours, la plupart des atteintes ou des ingérences représentent des programmes ou des mesures de surveillance, secrets ou de masse, employés particulièrement par les États invoquant, souvent, des raisons de sécurité nationale ou de lutte contre le terrorisme[802]. La surveillance pour des raisons de sécurité, de défense ou de maintien de l'ordre public peut répondre à un objectif légitime, mais le degré d'ingérence doit être évalué afin de déterminer si la mesure est nécessaire ou non à la réalisation de cet objectif et si elle présente un intérêt réel à cette fin. Autrement dit, « *il ne suffit pas que les mesures soient ciblées pour trouver certaines aiguilles dans une botte de foin ; ce qu'il convient d'examiner, c'est leur impact sur la botte de foin, au regard du risque de préjudice, c'est-à-dire déterminer si la mesure est nécessaire et proportionnée* »[803].

À ce titre, lorsqu'ils mettent en place des ingérences ou des restrictions, les États devraient toujours être guidés par « *le principe selon lequel les restrictions ne doivent pas porter atteinte à l'essence même du droit […] ; le rapport entre le droit et la restriction, entre la règle et l'exception, ne doit pas être inversé* »[804]. Par conséquent, les lois autorisant les atteintes doivent être formulées selon des critères précis, avec « une netteté suffisante », et sans conférer des pouvoirs illimités aux personnes chargées de leur application et/ou de leur contrôle, afin de fournir à l'individu une « protection adéquate contre l'arbitraire » ; c'est bien dans le contexte des surveillances à grande échelle ou secrètes que le danger d'arbitraire réside « avec une netteté singulière »[805]. En ce sens, les juges strasbourgeois ont souligné que « *puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la « loi » irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites* »[806]. S'interroger sur le fait de savoir si l'accès et l'utilisation des données correspondent à des buts légitimes mènent à s'interroger sur les pratiques des institutions publiques actuelles qui consistent à s'en remettre, de plus en plus, aux acteurs privés pour conserver les données, afin de pouvoir y accéder ultérieurement. C'est précisément ce qu'a entrepris la Cour de justice de l'Union à l'occasion

[802] *Cf.* p. 168 et s., 363 et s., 480 et s., 498 et s.
[803] Rapport du Haut-Commissariat des Nations Unies, Le droit à la vie privée à l'ère du numérique, 30 juin 2014, A/HRC/27/37, *op. cit.,* §25, p.9.
[804] Comité des Droits de l'Homme, Observation générale n° 27, *loc. cit.*, §13, p.4.
[805] CEDH, Affaire Malone c. Royaume-Uni du 2 août 1984, *loc. cit.*, §§67-68, et Affaire Amann c. Suisse du 16 février 2000, *loc. cit.,* §56.
[806] CEDH, Affaire Malone c. Royaume-Uni, *Id.*, §§67-68, et Affaire Amann c. Suisse, *Ibid.,* §56.

de plusieurs questions préjudicielles remettant en cause des dispositions de la Directive européenne de 2006 sur la conservation de données[807], à travers lesquelles elle a affirmé que force est de constater que l'ingérence que comporte cette directive dans les différents droits fondamentaux consacrés par la Charte s'avère « *[…] d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave* »[808]. Et la Cour souligne que *« la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, […], le sentiment que leur vie privée fait l'objet d'une surveillance constante* »[809].

Il est, par ailleurs, utile de s'interroger sur l'usage qui est fait des données et le type d'intervenant autorisé à y accéder et s'il existe des limites à leur utilisation. Multiples législations ne posent pas de limites particulières à l'utilisation des données, autorisant ainsi la collecte des données pour un objectif légitime donné, puis l'utilisation ultérieure de celles-ci à d'autres fins. Et cette absence de limites s'est accentuée depuis les évènements du 11 septembre 2001, « *la frontière entre la justice pénale et la protection de la sécurité nationale s'étant considérablement brouillée* »[810]. Il en résulte un partage de données entre divers services et organes publics et/ou privés qui risque d'enfreindre au droit étudié, puisque certaines mesures de surveillance nécessaires et proportionnées, poursuivant un objectif légitime, peuvent très bien ne pas l'être pour une autre fin.

Une étude comportant des informations sur les lois et les pratiques de neuf États en matière « d'accès gouvernemental/public systématique »[811] aux données du secteur privé a permis de dégager plusieurs grands thèmes généraux communs, retrouvés dans ces lois et pratiques nationales[812] : dans la mesure où les différents services publics bénéficient d'une grande facilité d'accès aux données du secteur privé, la liberté de plus en plus croissante qu'ont ces organismes

[807] Directive européenne 2006/24 du Parlement européen et du Conseil en date du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (Data Retention Directive), Plus en vigueur (Date de fin de validité : 08/04/2014).
[808] CJUE, Digital Rights Ireland et autres du 8 avril 2014, *loc. cit.*, §37.
[809] CJUE, Digital Rights Ireland, *Id.*, §37.
[810] Rapport du Haut-Commissariat des Nations Unies, Le droit à la vie privée à l'ère du numérique, 30 juin 2014, A/HRC/27/37, *Id.,* §27, p. 10.
[811] F. CATE, J. DEMPSEY et I. RUBINSTEIN, « Systematic government access to private-sector data », *International Data Privacy Law,* vol. 2, n° 4, novembre 2012, p. 195–199: "*Governments have sought access to personal information held by the private sector not only by asking companies to produce specific records about a single target or a small number of people at a time but increasingly via what we refer to here as 'systematic' government access*".
[812] F. CATE, J. DEMPSEY et I. RUBINSTEIN, «Systematic government access to private-sector data», *Id.*, Study comprises papers on the law and recent controversies concerning systematic access in nine countries: Australia, Canada, China, Germany, India, Israel, Japan, the United Kingdom, and the United States.

de partager ces données et de les utiliser à d'autres fins entraîne systématiquement un affaiblissement des protections accordées jusque-là aux données et, *in fine*, aux personnes. Selon cette étude, il apparaît qu'en analysant les demandes des autorités publiques pour un accès systématique, *« data collection and use for national security and law enforcement are generally beyond the scope of those laws or constitute an express exception to them* »[813]. En outre, les dispositions séparées prévoyant les mesures de surveillance et d'accès gouvernementaux sont souvent ambiguës, permettent une grande latitude dans le domaine de la sécurité nationale et se trouvent, récemment, dépassées par la technologie[814]. Dans plusieurs régions, le régime de partage des données a été abrogé à la suite d'un contrôle juridictionnel pour ces raisons, tel que ce fut le cas pour la directive européenne de 2006 susmentionnée.

Section 2 – Les droits de la personne numériques

Dans le monde numérique, ces droits de la personne, érigés par les nouvelles dispositions légales, se composent principalement des droits d'accès et de regard (§1), mais aussi des droits de rectification et d'opposition (§2), assurant, par conséquent, une protection adéquate de la personne et de ses données personnelles.

§1. Droits d'accès et de regard

Les droits d'accès et de regard assurés par les nouvelles législations, au profit des individus, impliquent, d'une part, un droit d'accès effectif et concret (A) et, d'autre part, un droit à l'information réel (B).

A. Un droit d'accès effectif

En marge du droit à la protection des données de la personne concernée, est apparu le droit d'accès de celle-ci, un droit fondamental comprenant l'accès à internet, l'accès aux données personnelles et publiques ainsi que l'accès à l'information. L'accès à internet a été internationalement reconnu comme étant une condition de la liberté de communication, et entretient l'exercice d'autres droits fondamentaux tels que la liberté d'association ou la liberté d'entreprendre.

[813] F. CATE, J. DEMPSEY et I. RUBINSTEIN, « Systematic government access to private-sector data », *Id.*, p. 197.
[814] F. CATE, J. DEMPSEY et I. RUBINSTEIN, « Systematic government access to private-sector data », *Ibid.,* p. 197.

À l'occasion d'une affaire remettant en question des dispositions du *Communications Decency Act* de 1996[815], la Cour Suprême des États-Unis a jugé que les restrictions à la liberté d'expression, qu'elle admettait précédemment en matière de diffusion audiovisuelle, n'étaient pas transposables à internet. Selon la Cour, internet « *is a medium that receives full First Amendment[816] protection* »[817]. Avec l'essor du numérique, internet est bien devenu, de manière unique et innovante, un moyen de communication humaine mondial, et en restreindre ou limiter son accès reviendrait à restreindre des libertés fondamentales telles que la liberté d'expression, la liberté de communication, la liberté de s'autodéterminer, ou la liberté d'entreprendre. Pour reprendre la formule devenue célèbre du juge Dalzell du tribunal de district de Pennsylvanie, dont le jugement était contesté devant la Cour suprême en ce qui concerne le CDA, « *the internet may fairly be regarded as a never-ending worldwide conversation* [… and] *the most participatory form of mass speech yet developped* »[818].

En France, le Conseil Constitutionnel, à l'occasion d'un recours contre la loi favorisant la diffusion et la protection de la création sur internet[819] qui confiait à une Autorité administrative indépendante, la HADOPI[820], des pouvoirs de sanctions, notamment, de suspension de l'accès à internet, a souligné « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions* », le droit de libre communication, et de la liberté de parler, écrire et imprimer, protégé par l'article 11 de la Déclaration des droits de l'homme[821], « *implique la liberté d'accéder à ces services* »[822]. Il a ainsi considéré que les pouvoirs de sanctions institués, consistant à réduire ou à empêcher l'accès à internet des personnes, peuvent « *conduire à*

---

[815] Communications Decency Act of 1996, 47 U.S.C. §230, declared unconstitutional by the US Supreme Court in 1997.

[816] U.S. Constitution, First Amendment – Religion and expression "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*".

[817] United States Supreme Court, Reno, Attorney General of the United States *et al. v.* American Civil Liberties Union *et al.*, No. 96-511, June 26, 1997, 521 U.S. 844 (1997), (b).

[818] US District Court for the Eastern District of Pennsylvania, Reno, Attorney General of the United States *et al. v.* American Civil Liberties Union, et H. Abelson, K. Ledeen, H. R. Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*, Addison-Wesley, 2008, p. 241.

[819] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n° 0135 du 13 juin 2009, p. 9666, texte n° 2.

[820] Haute autorité pour la diffusion des œuvres et la protection des droits sur l'internet (Hadopi), instituée par la loi du 12 juin 2009 et chargée de « veiller à la prévention et à la sanction du piratage des œuvres ».

[821] Déclaration des Droits de l'Homme et du Citoyen de 1789, Art. 11. « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi* ».

[822] Conseil Constitutionnel, Décision du 10 juin 2009, *loc. cit.,* Cons. 12.

restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile »[823], la conduisant dès lors à censurer les dispositions litigieuses en cause.

Du côté européen, la directive de 2009, composante du « troisième paquet télécoms », précise que « *les mesures prises par les États membres concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques respectent les libertés et droits fondamentaux des personnes physiques, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les principes généraux du droit communautaire* »[824]. Modifiant la directive de 2002, dite directive cadre, elle dispose que toute mesure concernant l'accès à internet doit être « appropriée, proportionnée et nécessaire dans le cadre d'une société démocratique » et subordonnée à des garanties procédurales adéquates. De même, elle impose le respect du principe de la présomption d'innocence et du droit au respect de la vie privée ainsi que la mise en place d'une procédure « préalable, équitable et impartiale » avant toute restriction de l'accès, dénotant une volonté de limiter fermement toute restriction au droit d'accès à internet et à l'espace numérique. En effet, la liberté d'accès à internet est la « *voie royale vers d'autres droits* »[825], tels que le droit à l'éducation, le droit de participer à la vie culturelle et à jouir des bienfaits du progrès scientifique et de ses applications, les droits civils et politiques ou le droit à la liberté d'association et de réunion. Et internet, « *en servant de catalyseur grâce auquel les individus exercent leur droit [...], facilite également la réalisation de tout un ensemble d'autres droits de l'homme* »[826]. Il semble bien qu'il existe une obligation négative/passive incombant aux États, celle de ne pas couper ou restreindre, de manière illégale ou disproportionnée, l'accès à internet.

De ce droit découle également tout le débat sur la neutralité du net, qui implique une égalité de traitement et d'acheminement de l'ensemble des flux de données par tous les opérateurs informatiques (FAI, intermédiaires assurant l'interconnexion de réseau etc.), quelque que soit

[823] Conseil Constitutionnel, Décision du 10 juin 2009, *Id.,* Cons. 16.

[824] Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques, Art. premier - Modifications apportées à la directive 2002/21/CE (directive «cadre»).

[825] F. LA RUE, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 16 mai 2011, Conseil des droits de l'homme, Dix-septième session, A/HRC/17/27, §22, p. 7.

[826] F. LA RUE, Rapport sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Id.*, §22, p. 7.

leur contenu ou leur destinataire/émetteur[827]. La neutralité semble correspondre à l'architecture originelle du réseau, invoquant principalement la liberté d'accès à internet, la liberté de communication, la liberté d'expression et d'opinion, les principes de non-discrimination ou de transparence. Que ce soit dans la directive de 1995 ou dans le nouveau RGPD, le principe de neutralité est absent des termes de leurs dispositions. Le Règlement se contente pour sa part d'affirmer simplement qu'afin « *d'éviter de créer un risque de contournement grave […]* », la protection des individus « *[…] devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées* », en précisant que cette protection « *devrait s'appliquer aux traitements de données à caractère personnel à l'aide de procédés automatisés ainsi qu'aux traitements manuels, si les données à caractère personnel sont contenues ou destinées à être contenues dans un fichier* »[828]. Plusieurs opposants et partisans à ce principe peuvent être mondialement recensés, certains allant même jusqu'à dire que la neutralité du net serait « une solution à la recherche d'un problème »[829].

En France, l'ARCEP a fourni en 2010 dix propositions et recommandations relatives à la neutralité d'internet et des réseaux, les plus cruciales étant : la liberté et la qualité dans l'accès à internet, la non-discrimination des flux dans l'accès à l'internet, l'encadrement des mécanismes de gestion de trafic de l'accès à l'internet (à travers le respect notamment des « critères généraux de pertinence, de proportionnalité, d'efficacité, de non-discrimination des acteurs et de transparence »), la transparence accrue vis-à-vis des utilisateurs finaux, ou encore le suivi du marché de l'interconnexion de données[830]. Certaines de ces propositions ont été reprises par le Règlement européen sur l'internet ouvert de 2015, qui déclare, à titre liminaire, que les mesures prévues par ses dispositions respectent « *le principe de la neutralité technologique, c'est-à-dire qu'elles n'imposent ni ne favorisent l'utilisation d'aucun type particulier de technologie* »[831], et ce notamment dans le cadre de ses dispositions visant à

[827] Pour plus d'informations : T. Wu, "Network neutrality, Broadband discrimination", *Journal of Telecommunications and High technology Law*, Vol. 2, 2003, p. 141, et, Les actes de l'ARCEP, *Neutralité de l'internet et des réseaux. Propositions et recommandations*, septembre 2010.

[828] RGPD, Cons. 15.

[829] D. BRENNER, "Net Neutrality: A Solution In Search Of A Problem", 25 septembre 2012, Forbes: https://www.forbes.com/sites/ciocentral/2012/09/25/net-neutrality-a-solution-in-search-of-a-problem/#29659ce93fc5

[830] Les Actes de l'ARCEP, « Neutralité de l'internet et des réseaux : Propositions et recommandations », septembre 2010, Annexe – Rappel des 10 propositions, p. 58 et s. ; disponible en ligne : https://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010.pdf

[831] Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union, Cons. 2.

« garantir l'accès à un internet ouvert »[832]. Alors que du côté américain, la Federal Communications Commission (FCC) a récemment voté pour une abrogation des « *Net Neutrality Rules* »[833].

Les différentes vagues de manifestations, observées ces vingt dernières années dans le monde, ont permis d'illustrer le rôle fondamental que peut jouer internet dans la mobilisation des citoyens pour réclamer justice, égalité, responsabilité ou un respect plus concret des droits de l'homme. Par conséquent, « *faciliter l'accès à l'internet à tous les individus, avec le minimum de restrictions sur les contenus, devrait être la priorité de tous les États* »[834]. Aux termes du RGPD, devenu la loi-cadre en matière de protection des données personnelles, et de la loi de 1978, modifiée dernièrement par la loi du 20 juin 2018[835], toute personne justifiant de son identité a le droit d'interroger le responsable d'un traitement de données personnelles, afin d'obtenir la communication, rapide, lisible et accessible, des données à caractère personnel la concernant, ainsi que toute autre information relative à l'origine, la durée de conservation et/ou les destinataires de celles-ci, aux finalités du traitement, ainsi qu'aux droits et garanties existants[836]. Les individus ont donc un droit d'accès direct aux données les concernant ainsi qu'aux informations sur les données collectées et sur le traitement de celles-ci. Et ces différents accès sous-entendent une liberté d'accès à internet, « l'un des instruments les plus puissants du XXIe Siècle » fondé sur une communication interactive, permettant de renforcer la transparence

---

[832] Règlement (UE) 2015/2120 établissant des mesures relatives à l'accès à un internet ouvert, *Id.,* Art. 3 – garantir l'accès à un internet ouvert « *1. Les utilisateurs finals ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet. […]*
3. Dans le cadre de la fourniture de services d'accès à l'internet, les fournisseurs de services d'accès à l'internet traitent tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés.
Le premier alinéa n'empêche pas les fournisseurs de services d'accès à l'internet de mettre en œuvre des mesures raisonnables de gestion du trafic. Pour être réputées raisonnables, les mesures sont transparentes, non discriminatoires et proportionnées, et elles ne sont pas fondées sur des considérations commerciales, mais sur des différences objectives entre les exigences techniques en matière de qualité de service de certaines catégories spécifiques de trafic. Ces mesures ne concernent pas la surveillance du contenu particulier et ne sont pas maintenues plus longtemps que nécessaire. »

[833] Par ex. : C. KANG, "F.C.C. Repeals Net Neutrality Rules", 14 décembre 2017, The New York Times: https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html ; K. COLLINS, "Why Net Neutrality Was Repealed and How It Affects You", 14 décembre 2017, The New York Times: https://www.nytimes.com/2017/12/14/technology/net-neutrality-rules.html?module=inline

[834] F. LA RUE, Rapport sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Id.*, §2, p. 4.

[835] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[836] RGPD, Art. 15 – Droit d'accès de la personne concernée ; Loi Informatique et libertés, Section 2 - Droits des personnes à l'égard des traitements de données à caractère personnel, Art. 39.

dans la conduite des puissants (publics ou privés) ainsi que l'accès à l'information et au savoir, mais aussi, de faciliter la participation active des citoyens à l'édification de sociétés démocratiques[837]. En effet, plusieurs législations, résolutions, conventions ou jurisprudences soulignent et insistent « *sur l'importance du respect intégral de la liberté de rechercher, de recevoir et de répandre des informations, et notamment sur l'importance capitale de l'accès à l'information et de la participation démocratique* »[838].

Il semble alors que ce droit d'accès, qualifié de droit fondamental, se décline en plusieurs aspects comprenant un droit d'accès à internet, un droit d'accès aux données personnelles, un droit d'accès à l'information subjectif, personnel, visant les informations nominatives les concernant et les traitements dont elles font l'objet, ainsi qu'un droit d'accès à l'information objectif, général, caractérisant l'accès à l'information, au savoir, à la vérité. Ce droit d'accès se trouve, en plus, favoriser et faciliter par le potentiel croissant et les nombreuses capacités offertes par les nouvelles technologies et outils numériques, les deux formant ainsi des libertés qu'il convient de protéger : « *il faut donc garantir la liberté des citoyens et la liberté nouvelle de l'informatique, l'une par l'autre, par un système de réciprocité. La liberté des citoyens est garantie par un pouvoir concret, leur droit à l'information et leur pouvoir d'accès aux données qui les concernent personnellement* »[839].

S'inscrivant dans la même lignée que ces ancêtres, le RGPD consacre le droit de toute personne concernée d'accéder aux données personnelles collectées à son sujet. L'exercice de ce droit par la personne doit pouvoir s'opérer « facilement et à des intervalles raisonnables », lui permettant de prendre connaissance du traitement dont ses données font l'objet et d'en vérifier la licéité[840]. Ceci comprend le droit d'accéder aux données concernant le compte bancaire de la personne concernée, ses impôts ou sa santé, par exemple, en vue d'obtenir les données de leurs dossiers contenant une multitude d'informations, telles que les crédits, dettes, épargnes, niveau d'imposition, diagnostics, résultats d'examens, les avis ou les interventions opérées et ainsi de suite. À ce titre, l'individu concerné doit avoir le droit « de connaître et de se faire communiquer » les finalités du traitement des données, la durée du traitement si possible, les destinataires des données personnelles, la logique sous-jacente guidant leur éventuel traitement

[837] F. LA RUE, Rapport sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Ibid.*, §2, p. 4.
[838] Par ex. : Résolution 68/167, *op. cit.,* p. 2 ; Résolution 69/166, *op. cit*., p. 2, ; et, Résolution 7/36. Mandat du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 28 mars 2008, Conseil des droits de l'homme, Quarante-deuxième séance, p. 2.
[839] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *op. cit*., p. 5789.
[840] RGPD, Cons. 63.

automatisé et les conséquences qu'il pourrait avoir, « au moins en cas de profilage »[841]. En outre, le RGPD impose que, dans la mesure du possible, le responsable du traitement doit pouvoir assurer l'accès à distance à un système sécurisé, qui permet à la personne d'accéder directement aux données personnelles la concernant. Mais cette obligation a été tempérée afin d'éviter qu'elle ne porte atteinte à d'autres droits ou libertés, comme le secret des affaires, le secret professionnel ou encore la propriété intellectuelle protégeant notamment le logiciel employé. Ceci dit, ces considérations, indiquent les législateurs européens, ne peuvent aboutir à refuser toute communication d'informations à la personne ayant formulée une demande ; le responsable du traitement est tenu de faire le nécessaire pour répondre à la demande de la personne concernée, y compris demander à celle-ci plus de précisions quant à sa demande pour pouvoir lui fournir une réponse adéquate et accessible. Néanmoins, précisent-ils, « *un responsable de traitement ne devrait pas conserver des données à caractère personnel à la seule fin d'être en mesure de réagir à d'éventuelles demandes* »[842].

Par ailleurs, ce nouveau dispositif-cadre pour la protection des données personnelles fournit des précisions concernant les restrictions et limitations autorisées. Ainsi, des limitations au droit à l'information, au droit d'accès aux données personnelles, aux droits de rectification et d'effacement, au droit à la portabilité des données, au droit d'opposition, à la communication d'une violation de données personnelles et à certaines obligations connexes des responsables du traitement peuvent être imposées par la loi (au niveau européen, communautaire ou national) « dans la mesure nécessaire et proportionnée dans une société démocratique » en vue de garantir divers objectifs limitativement énumérés[843]. De plus, ces restrictions aux droits et libertés doivent respecter les exigences énoncées par la Charte et la Convention européennes, ainsi que les interprétations et précisions jurisprudentielles apportées en la matière.

En outre, il est utile de noter que le Règlement prend en compte, dans son application, le mouvement de l'Open data. Le principe de l'accès du public aux documents officiels est ainsi

---

[841] RGPD, Cons. 63 et 64, et Art. 13, 14 et 15.

[842] RGPD, Cons. 63 et 64.

[843] RGPD, Cons. 73 : « *[…] pour garantir la sécurité publique, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ou de manquements à la déontologie des professions règlementées, et pour garantir d'autres objectifs d'intérêt public importants de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, la tenue de registres publics conservés pour des motifs d'intérêt public général, le traitement ultérieur de données à caractère personnel archivées pour fournir des informations spécifiques relatives au comportement politique dans le cadre des régimes des anciens États totalitaires ou la protection de la personne concernée ou des droits et libertés d'autrui, y compris la protection sociale, la santé publique et les finalités humanitaires. […]* ».

reconnu et considéré comme étant dans l'intérêt public[844]. En ce sens, les données personnelles, qui figurent dans les documents détenus par une autorité ou une institution publique ou un organisme privé chargé d'une mission publique, doivent pouvoir être rendues publiques dans la mesure où cette communication est prévue par le droit européen ou le droit national dont relève l'autorité ou l'organisme[845]. Ces dispositions servent principalement à concilier, d'une part, le droit d'accès du public aux documents officiels et la réutilisation des informations du secteur public ainsi que, d'autre part, le droit à la protection des données personnelles. Dans ce contexte, la directive européenne de 2003[846] n'affecte en rien le niveau de protection des personnes à l'égard du traitement des données garanti par les dispositions en question, et laisse intact le droit et les obligations prévus par celles-ci. Elle devrait ainsi être écartée si l'accès aux documents est exclu ou limité pour des motifs de protection des données personnelles, ou si la loi prévoyant l'accès est incompatible avec les dispositions prévoyant la protection des personnes à l'égard du traitement de données à caractère personnel[847].

À l'occasion d'une affaire inédite, la Cour de justice de l'Union a jugé que le droit d'accéder aux informations ou d'obtenir la rectification ou la suppression de celles-ci est l'essence du droit à la protection des données personnelles. Selon la Cour, une législation qui ne prévoit aucune possibilité pour un individu d'exercer des voies de droit en vue d'obtenir l'accès aux données personnelles le concernant, ou d'obtenir la rectification ou la suppression de celles-ci, « ne respecte pas le contenu essentiel » du droit fondamental à une protection juridictionnelle effective ni du droit fondamental au respect de la vie privée dans toutes ses composantes[848].

B. Un droit à l'information réel

Des expressions telles que « liberté de l'information », « droit à l'information » et « droit d'accès à l'information » font toutes référence au droit qui découle de la liberté d'expression et de communication, selon lequel toute personne a droit à la liberté de chercher, de recevoir et de répandre des informations et des idées, sans considération de frontières et sans ingérences, par

[844] RGPD, Cons. 154.
[845] RGPD, Art. 86 – Traitement et accès du public aux documents officiels.
[846] Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, JO L 345 du 31.12.2003, p. 90-96.
[847] RGPD, Cons. 154.
[848] CJUE, Cour (Grande Ch.), Maximillian Schrems c. Data Protection Commissioner du 6 octobre 2015, affaire C-362/14, §§ 23, 94 et 95.

n'importe quel moyen d'expression de son choix[849]. De plus en plus, ce droit à l'information joue un rôle d'une importance cruciale « *qui ne se limite pas à garantir la liberté de la presse. Les gouvernements et le secteur privé sont trop enclins au culte du secret* »[850]. Il est, certes, impossible de nier l'importance d'une protection juridique des droits de la défense comme des droits de la propriété intellectuelle, cela étant, « *le déni du droit à l'information ne sert nullement l'intérêt général* »[851]. L'évolution croissante des technologies et la mondialisation ont, conjointement, créé de nouveaux enjeux pour la protection des données personnelles et les droits des personnes[852]. En effet, l'ampleur de la collecte, du traitement et du partage des données ne cesse d'augmenter, les technologies permettant « *tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités* »[853]. Dès lors, le droit d'accès à l'information implique le principe de transparence et les obligations de notification à plusieurs niveaux, que ce soit pour la collecte, l'analyse, le traitement ou encore le transfert des données, formant ainsi une garantie appropriée.

Selon le législateur européen, le principe de transparence exige que toute information ou communication, adressée à la personne concernée ou au public, soit concise, aisément accessible, facile à comprendre, formulée en des termes clairs et simples, et, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels[854]. La notion de transparence est mentionnée dans plusieurs considérants du Règlement, se trouve inscrite en tant que principe à l'article 5, et est détaillée dans le contexte des droits de la personne. Cependant, le législateur n'a pas fourni de définition propre à ce concept, mais en apporte des éclaircissements permettant de dégager un fil conducteur. Il en ressort ainsi que l'objectif principal visé est, notamment, celui de permettre aux personnes de savoir et de comprendre si des données personnelles les concernant font l'objet d'une collecte, par qui et à quelle fin[855] ; et pour atteindre cet objectif, le principe de transparence se trouve être indispensable. En effet, « *les personnes concernées doivent recevoir*

[849] Par ex. : Art. 19 Déclaration universelle des droits de l'homme de 1948 ; Art. 19 du Pacte international relatif aux droits civils et politiques de 1966 ; Art. 10 Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950.
[850] Commission des droits de l'homme, Promotion et protection du droit à la liberté d'opinion et d'expression, Rapport du Rapporteur spécial, M. A. Hussain, établi en application de la résolution 1993/45 de la Commission des droits de l'homme, 17 décembre 1994, Cinquante et unième session, Conseil économique et social, E/CN.4/1995/32, §135, p. 45.
[851] Commission des droits de l'homme, Promotion et protection du droit à la liberté d'opinion et d'expression, E/CN.4/1995/32, *Id.,* §135, p. 45.
[852] *Cf.* p. 480 et s..
[853] RGPD, Cons. 6.
[854] RGPD, Cons. 39 et 58, et Art. 12.
[855] RGPD, Cons. 58.

des informations claires sur les données qui sont traitées, notamment les données observées ou déduites les concernant, être mieux informées sur la manière dont leurs données sont utilisées et sur les finalités pour lesquelles elles sont utilisées, y compris la logique algorithmique qui sert à déterminer les hypothèses et les prévisions à leur sujet »[856]. Ce qui contribue à accorder plus de contrôle et d'autonomie aux personnes afin de mieux déceler les « préjugés injustes et contester les erreurs », et d'empêcher l'utilisation ultérieure des informations pour des finalités non conformes aux attentes légitimes des individus concernés. Ces exigences se justifient tout particulièrement, selon les rédacteurs du Règlement, dans des situations où « *la multiplication des acteurs et la complexité des technologies utilisées* » font en sorte qu'il est difficile et ésotérique pour les individus de savoir et de comprendre si des données personnelles qui les concernent sont collectées, par qui et poursuivant quelle finalité, comme dans le cas de la publicité en ligne[857].

Le droit à l'information implique, en outre, le principe de traitement loyal et transparent dont découle plusieurs exigences à la charge du responsable du traitement. Dans ce contexte, le fait que des données personnelles sont collectées, utilisées, consultées ou traitées d'une autre manière, et la mesure dans laquelle celles-ci sont ou seront traitées doivent être transparents au regard des personnes. En ce sens, le principe de transparence vaut, en particulier, pour toute information transmise aux personnes concernées sur l'identité du responsable du traitement, sur les finalités du traitement ainsi que pour toute autre information visant à assurer un traitement loyal et transparent à leur égard. Cela comprend aussi leurs droits d'obtenir la confirmation et la communication des données qui les concernent, faisant l'objet d'un traitement. De plus, l'information de la personne concernée au sujet des finalités, risques, règles, garanties et droits liés au traitement des données doit être constamment assurée, y compris en ce qui concerne les modalités d'exercice de leurs droits relatifs au traitement, notamment le droit de s'y opposer[858]. En ce sens, le RGPD fournit, à son article 13, une liste de toutes les informations à fournir lorsque les données personnelles ont été collectées auprès de la personne concernée, et, à son article 14, une autre liste de toutes les informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée. Dans ce cadre, toute personne a le droit d'être informée de l'existence d'une opération de traitement et de ses finalités. Le responsable du traitement doit également fournir toute autre information nécessaire pour garantir un traitement

[856] Contrôleur européen de la protection des données (CEPD), Avis n° 7/2015 « Relever les défis des données massives : Un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes », du 19 novembre 2015, Bruxelles EDPS, p. 5.
[857] RGPD, Cons. 58.
[858] RGPD, Cons. 39, 50, 60 et 61, et Art. 5, 12, 13, 14, et 15.

équitable et transparent, en prenant en compte les circonstances particulières et le contexte dans lesquels les données personnelles sont traitées.

Cette obligation d'information s'étend pour inclure le droit d'être informé de l'existence d'un profilage et des conséquences de celui-ci. La transparence des décisions automatisées est de plus en plus fondamentale avec l'essor de l'analyse des Big data. Il est, dès lors, important de faire connaître, dans un langage facile et compréhensible, la logique qui sous-tend le processus décisionnel, ce qui peut aider les personnes à vérifier davantage l'exactitude et l'intégrité des conclusions tirées « *par les organisations qui traitent les données et affectent les individus* »[859]. Ainsi, il est de l'avis du CEPD que la logique sous-tendant l'analyse des données massives doit être révélée par les organisations et les institutions, qu'elle ait un effet direct ou indirect sur l'individu, et ce, de façon proactive, « *sans que les personnes concernées ne doivent prendre des mesures actives pour obtenir la divulgation* »[860]. Il existait une époque, très proche, pendant laquelle les données personnelles collectées et traitées étaient principalement composées d'informations que les personnes avaient sciemment partagées ; or, à l'ère du Big data, ce n'est plus le cas. Une grande partie des données traitées sont, désormais, observées ou déduites, à l'insu des particuliers. Comme il a pu être observé à travers cette étude, la collecte et l'enregistrement des activités en ligne, les services de localisation des smartphones et des tablettes, et les possibilités quadruplées de suivre et de tracer les activités dans l'espace réel grâce à des dispositifs intelligents et à l'Internet des Objets, accroissent la quantité massive d'informations à partir desquelles des déductions et des prédictions sont faites sur les individus. La transparence dans la transmission de l'information et dans la liberté de l'information joue bien un rôle crucial et indispensable.

Quand les données sont collectées auprès de la personne, il importe, selon les législateurs, que cette dernière sache aussi « si elle est obligée de fournir ces données », et doit être clairement informée des conséquences auxquelles elle s'expose si elle refuse de les fournir[861]. Ces informations doivent être fournies, au moment où les données ont été collectées et d'une manière à offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement

[859] CEPD, Avis n° 7/2015 « Relever les défis des données massives », *Id.*, p. 11.

[860] CEPD, Avis n° 7/2015 « Relever les défis des données massives », *Ibid.*, p. 11 ; et le contrôleur précise : *« Parmi les exemples tirés du quotidien pour lesquels «la logique sous-jacente au processus décisionnel» devrait être dévoilée, on peut citer un système d'assurance automobile personnalisé (en utilisant les données du capteur du véhicule pour juger les habitudes de conduite), des services d'évaluation de la capacité de crédit, un système de commercialisation et de tarification qui détermine quelle ristourne une personne recevra ou quel contenu média doit être recommandé à un individu* ».

[861] RGPD, Cons. 60

lisible du traitement prévu[862]. Ces exigences s'appliquent également aux informations fournies lors de la demande de consentement, qui doit être présentée sous une forme « *compréhensible et aisément accessible, et formulée en des termes clairs et simples* »[863]. La manière dont les informations sont divulguées joue, par conséquent, un rôle crucial. Toute information ou communication doit employer un langage clair et simple, compréhensible et concis, adapté au public visé, permettant à la personne concernée de comprendre les informations complexes, tout en étant aisément accessibles.

L'importance de la transparence et de l'accès facile et clair aux informations est, d'ailleurs, mise en exergue à travers les nombreuses références à ces principes dans plusieurs dispositions du RGPD. C'est le cas par exemple de toutes les informations supplémentaires prévues dans le cadre des informations à fournir lorsque des données sont collectées auprès de la personne concernée et lorsqu'elles n'ont pas été collectées auprès de celle-ci, qui sont « nécessaires pour garantir un traitement équitable et transparent »[864]. C'est aussi le cas en ce qui concerne le droit d'opposition qui doit être « explicitement porté à l'attention de la personne » et présenté « clairement et séparément de toute autre information »[865]. *Idem* en matière de communication à la personne concernée d'une violation de données, où il est requis que cette communication décrive « *[…], en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures* » visées dans le cadre des notifications à l'autorité de contrôle d'une violation[866]. Par ailleurs, ce droit à l'information et à la communication constitue une garantie appropriée pour la protection des personnes concernées, qui se caractérise par une « *[…] information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication […]* » quant à la décision prise à l'issue du traitement, et de pouvoir contester la décision[867]. Toutes ces exigences et tous ces principes s'appliquent également aux

[862] RGPD, Cons. 61 : Ainsi, « *les informations sur le traitement des données à caractère personnel relatives à la personne concernée devraient lui être fournies au moment où ces données sont collectées auprès d'elle ou, si les données à caractère personnel sont obtenues d'une autre source, dans un délai raisonnable en fonction des circonstances propres à chaque cas. Lorsque des données à caractère personnel peuvent être légitimement communiquées à un autre destinataire, il convient que la personne concernée soit informée du moment auquel ces données à caractère personnel sont communiquées pour la première fois audit destinataire. Lorsqu'il a l'intention de traiter les données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées, le responsable du traitement devrait, avant de procéder à ce traitement ultérieur, fournir à la personne concernée des informations au sujet de cette autre finalité et toute autre information nécessaire. Lorsque l'origine des données à caractère personnel n'a pas pu être communiquée à la personne concernée parce que plusieurs sources ont été utilisées, des informations générales devraient être fournies* ».

[863] RGPD, Art. 7 §2

[864] RGPD, Art. 13 §2 et 14 §2

[865] RGPD, Art. 21 §4.

[866] RGPD, Art. 34 §2.

[867] RGPD, Cons. 71 par ex.

communications relatives au droit d'accès, au droit de rectification, au droit à l'effacement, au droit à la limitation du traitement, à l'obligation de notification en ce qui concerne la rectification ou l'effacement de données ou la limitation du traitement, au droit à la portabilité des données, au droit d'opposition, au droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, ainsi qu'à l'obligation de notification en cas de violation de données à caractère personnel au titre des articles 15 à 22 et 34 du RGPD. En outre, ce droit à l'information dépasse les frontières et doit être également protégée au-delà, en particulier lorsque les données personnelles franchissent les frontières extérieures de l'Union. Cela accroît le risque pour les individus d'être dans l'ombre quant aux finalités, premières ou secondaires, du traitement, aux données collectées et à tout autre droit lié à la protection de leurs données qu'ils peuvent exercer, « *[…] notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations* »[868]. Les autorités de contrôle, dans ces cas, se trouvent être confrontées aux mêmes difficultés entraînant l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées à l'extérieur de leurs frontières[869]. Par conséquent, selon les rédacteurs du RGPD, il est fondamental pour la Commission et les autorités de contrôle d'échanger des informations sur une base réciproque, en vue de faciliter l'application des législations relatives à la protection des données personnelles.

Afin d'assurer au mieux le respect du droit à l'information, le RGPD exige que le droit des États membres opère des conciliations entre les règles régissant la liberté d'expression et d'information, « y compris l'expression journalistique, universitaire, artistique ou littéraire », et le droit à la protection des données personnelles en vertu des dispositions du Règlement[870]. Et ce dernier précise que, dans le cadre d'un traitement à des fins journalistiques ou d'expression universitaire, artistique ou littéraire, des dérogations ou des exemptions à certaines

[868] RGPD, Cons. 116.
[869] RGPD, Cons. 116 ; et le législateur européen précise que « *[…] Leurs efforts pour collaborer dans le contexte transfrontalier peuvent également être freinés par les pouvoirs insuffisants dont elles disposent en matière de prévention ou de recours, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. En conséquence, il est nécessaire de favoriser une coopération plus étroite entre les autorités de contrôle de la protection des données, pour les aider à échanger des informations et mener des enquêtes avec leurs homologues internationaux. Aux fins d'élaborer des mécanismes de coopération internationale destinés à faciliter et à mettre en place une assistance mutuelle internationale pour faire appliquer la législation relative à la protection des données à caractère personnel, la Commission et les autorités de contrôle devraient échanger des informations et coopérer dans le cadre d'activités liées à l'exercice de leurs compétences avec les autorités compétentes dans les pays tiers, sur une base réciproque et conformément au présent règlement* ».
[870] RGPD, Cons. 153 et Art. 85 §1.

dispositions du Règlement peuvent être prévues « *si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, consacré par l'article 11 de la Charte* »[871].

Conséquemment, et de façon générale, que les données soient fournies volontairement, observées, déduites, ou recueillies auprès de sources publiques, il ressort que les personnes ont incontestablement le droit d'être informées pour savoir quelles sont ces données, d'où elles viennent et auprès de qui elles ont été obtenues. Dans ce contexte, protéger le secret d'affaire ou la confidentialité commerciale ou encore le secret défense ne peut, d'une manière générale, primer sur les droits fondamentaux à la vie privée et à la protection des données des individus. Tout au contraire, il semble nécessaire de concilier les deux à travers une mise en balance des droits, d'autant que la décision de divulgation d'information n'est quasiment plus binaire, délimitée entre deux interlocuteurs ou acteurs potentiels.

Le secret, censé irriguer le respect de la vie privée des personnes physiques, devient un outil de pouvoir des institutions et grandes corporations, notamment celles de la Silicon Valley. Une logique inversée apparaît alors : les citoyens deviennent de plus en plus transparents face à un gouvernement de plus en plus opaque et au dispositif d'entreprise, l'appareil commercial. Il est vrai que tous les États suivaient une tradition consistant à combiner les préoccupations en matière de respect de la vie privée aux garanties relatives à la transparence étatique. Des garde-fous appropriés, préservant les libertés fondamentales, doivent être prévus dans l'architecture technique des services d'intelligence intérieure, mais non moins important est le fait de veiller à ce que les individus, qui ne font pas partie des services de renseignement, puissent, d'une certaine façon, traiter et comprendre les quantités de données massives que même un programme de surveillance basique (de contrôle) pourra générer[872]. Toutefois, à l'heure actuelle, ce sont également les grandes entreprises qui ont continuellement recours aux programmes de surveillance du Big data, leur permettant de générer des décisions automatisées

---

[871] RGPD, Cons. 153 « *[…] Tel devrait notamment être le cas des traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives d'actualités et bibliothèques de la presse. En conséquence, les États membres devraient adopter des dispositions législatives qui fixent les exemptions et dérogations nécessaires aux fins d'assurer un équilibre entre ces droits fondamentaux. Les États membres devraient adopter de telles exemptions et dérogations en ce qui concerne les principes généraux, les droits de la personne concernée, le responsable du traitement et le sous-traitant, le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, les autorités de contrôle indépendantes, la coopération et la cohérence, ainsi que les situations particulières de traitement des données. Lorsque ces exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre dont relève le responsable du traitement devrait s'appliquer. Pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, telles que le journalisme ».*

[872] D. K. CITRON, "Technological Due Process," Washington University Law Review, Vol. 85 Issue 6, 2008, p. 1305-1306.

et des recommandations personnalisées, comme il a été susmentionné. Or, « *automation jeopardizes the due process guarantees of meaningful notice and opportunity to be heard* »[873], affectant par conséquent la liberté d'information. Ceci dit, alors que les juridictions et les institutions publiques ont eu de nombreuses occasions, quoique sommaires, d'interroger les gouvernements et leurs services de renseignement sur des mesures ou des dispositifs de surveillance controversés, rien d'équivalent n'a été concrètement consacré afin de comprendre l'étendue de la collecte de données et de la demande d'information entreprises par les acteurs de la Silicon Valley : « *given their role as partners or pawns of the surveillance state, we deserve better* »[874].

Les entreprises recherchent constamment des informations personnelles et détaillées sur leurs consommateurs, actuels ou potentiels, et sur la vie de leurs employés, mais n'en rendent compte que de manière expéditive, en fournissant le moins d'information possible concernant leurs propres procédures et statistiques[875]. Les géants du web collectent quotidiennement des quantités massives de données sur leurs utilisateurs, mais combattent les dispositions permettant à ces mêmes utilisateurs d'exercer leur droit d'accès à l'information et leur droit de regard sur les dossiers numériques informationnels résultants. En effet, « *to scrutinize others while avoiding scrutiny oneself is one of the most important forms of power* »[876]. Un déséquilibre, et une sorte de paradoxe, au sein même des interprétations de la liberté de l'information s'observe : l'information semble être fournie de manière unidirectionnelle, éliminant peu à peu les droits et libertés fondamentales des individus ainsi que les exigences en matière d'information. Il est utile de relever que le RGPD autorise, certes, des exemptions et des dérogations, mais « dans des conditions spécifiques et moyennant des garanties appropriées pour les personnes concernées » et à des fins bien délimitées, telles que des fins archivistiques dans l'intérêt public, à des fins de recherches scientifique ou historique, ou à des fins statistiques[877].

La métaphore de la « black box », la boîte noire, telle qu'employée et analysée par le Professeur F. Pasquale, permet d'illustrer significativement l'étendue des enjeux du droit à l'information : la notion de « boîte noire » porte en soi un double sens selon l'auteur, qui peut soit renvoyer à

---

[873] D. K. CITRON, "Technological Due Process,", *Id.*, p. 1305, et l'auteur affirme que "*Both technological and legal mechanisms can secure meaningful notice, combat automation bias, and enhance the accuracy of decisions about constitutionally significant individual rights*".

[874] F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press Cambridge, USA, 2015, p. 161.

[875] G. PACKER, "Amazon and the Perils of Non-disclosure," The New Yorker, February 11, 2014; Disponible en ligne: https://www.newyorker.com/books/page-turner/amazon-and-the-perils-of-non-disclosure

[876] F. PASQUALE, *The Black Box Society*, *Id.,* p. 3-4.

[877] RGPD, Cons. 156, par ex.

un dispositif d'enregistrement, comme les systèmes de suivi et de contrôle des données trouvés dans les avions, les trains, les voitures, les smartphones etc., soit désigner un système dont le fonctionnement est opaque, et énigmatique, dans lequel il est possible d'observer les intrants et les sortants (*inputs and outputs*), mais il est impossible de déterminer comment l'un devient l'autre. Selon l'auteur, nous sommes quotidiennement confrontés à cette double interprétation: « *tracked ever more closely by firms and government, we have no clear idea of just how far much of this information can travel, how it is used, or its consequences* »[878].

§2. Droits de rectification et d'opposition

Parmi les droits de la personne prévus, certains assurant la protection de leurs données personnelles, d'une importance non négligeable, méritent d'être analysés, à savoir les droits de rectification et d'effacement (A), mais aussi les droits d'opposition et de limitation (B).

A. Les droits de rectification et d'effacement

Les droits de rectification et d'effacement sont, dorénavant, inscrits séparément dans le texte du RGPD, qui prévoit que toute personne a le droit de « faire rectifier » ses données personnelles, et de disposer d'un « droit à l'oubli » leur permettant d'obtenir que leurs informations soient effacées et ne soient plus traitées. Cette exigence n'est pas nouvelle, indiquent les anciens députés lors de l'élaboration du projet de loi de 1978, « *mais jusqu'à un passé récent, il suffisait que l'individu, naturellement jaloux de ses secrets, se garde de l'indiscrétion des autres. Les limites de l'esprit humain, le temps qui passe, l'intérêt qui retombe, tout cela constituait la meilleure des sauvegardes. Mais, aujourd'hui, voilà que l'ordinateur a brisé ces protections très anciennes. Désormais, les années qui passent n'apportent plus l'oubli. C'est là que s'enracine l'angoisse que l'informatique fait naître quelquefois et dont votre rapporteur, M. Foyer, parlait tout à l'heure en termes si éloquents. Tout est fiché, rien n'est perdu. Un élément quelconque de notre vie passée peut être à jamais fixé par une mémoire qui ne faiblira pas. Voilà qui paraît, à beaucoup d'entre nous, insupportable* »[879].

---

[878] F. PASQUALE, *The Black Box Society*, *Id.,* p. 3 ; et l'auteur ajoute : "*In philosophy, the term is also polysemic. For example, if enough people simply accept the outputs of a given process as valid, it is a quite useful black box. Some aspects of reality are simply assumed to be true, without need for further investigation. Graham Harman stated, "We have a true black box when a statement is simply presented as raw fact without any reference to its genesis or even its author. As Latour asks, 'who refers to Lavoisier's paper when writing the formula H2O for water?'" […].*"

[879] Débats parlementaires – Compte-rendu intégral, 4 oct. 1977, *op. cit.*, p. 5787.

Ce droit, qui porte une double dénomination au sein même du Règlement, est prévu à son article 17, Droit à l'effacement (« droit à l'oubli »), qui dispose que tout individu a le droit d'obtenir du responsable du traitement l'effacement des données la concernant « dans les meilleurs délais ». Partant, une obligation à la charge du responsable du traitement y est associée : celle d'effacer ces données dans les meilleurs délais sur la base d'un des motifs, limitativement énumérés, en présence duquel ce droit s'applique[880]. En outre, une obligation supplémentaire incombe au responsable du traitement étayant le droit à l'effacement, « afin de renforcer le « droit à l'oubli » numérique », qui inclut l'hypothèse où il aurait rendues publiques les données personnelles qu'il est tenu de supprimer[881]. Dans ce cas, le responsable du traitement est censé informer les autres responsables du traitement, traitant lesdites données, qu'il convient d'effacer « tout lien vers ces données, ou toute copie ou reproduction de celles-ci »[882].

Toutefois, cette obligation comporte en elle trois limitations qui risquent de réduire fortement, en pratique, l'applicabilité effective de ce droit par le responsable du traitement : le caractère « raisonnable » des mesures prises, la disponibilité des technologies et la disponibilité des moyens, des coûts de mise en œuvre. Par ailleurs, des exceptions générales au droit à l'effacement sont prévues par le Règlement, « dans la mesure où ce traitement est nécessaire » à l'exercice du droit à la liberté d'expression et d'information, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, pour des motifs d'intérêt public dans le domaine de la santé publique ou à des fins

---

[880] RGPD, Art. 17 §1 « *[…], lorsque l'un des motifs suivants s'applique :*
a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;
c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;
d) les données à caractère personnel ont fait l'objet d'un traitement illicite ;
e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1. »

[881] RGPD, Cons. 66 « *Afin de renforcer le «droit à l'oubli» numérique, le droit à l'effacement devrait également être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les responsables du traitement qui traitent ces données à caractère personnel qu'il convient d'effacer tout lien vers ces données, ou toute copie ou reproduction de celles-ci. […]* »

[882] RGPD, Cons. 66 et Art. 17 §2.

précises telles qu'énumérées par l'article 89[883], ou à la constatation, à l'exercice ou à la défense de droits en justice[884].

La loi Informatique et libertés, telle que modifiée par la loi du 20 juin 2018 précitée ainsi que par le décret et l'ordonnance pris en application[885], prévoit également le droit de rectification et le droit à l'effacement dans les conditions prévues par les dispositions du Règlement[886]. Ainsi, l'ancienne version de la loi qui prévoyait que « *toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite* »[887] fut récemment abandonnée.

---

[883] RGPD, Art. 89 - Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

[884] RGPD, Cons. 65 et Art. 17 §3 : « *Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire :*
a) à l'exercice du droit à la liberté d'expression et d'information ;
b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3 ;
d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; ou
e) à la constatation, à l'exercice ou à la défense de droits en justice. »

[885] Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF n° 0288 du 13 décembre 2018, « *[…], procède à la réécriture complète de la loi "Informatique et libertés"* » ; et Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 0125 du 30 mai 2019, « *achève l'adaptation du droit français au droit européen. Il s'agit du nouveau décret d'application de la loi de 1978.* » : La Rédaction de Vie-publique.fr, « La réécriture de la loi "Informatique et libertés" du 6 janvier 1978 », du 2 août 2019 : https://www.vie-publique.fr/eclairage/268790-la-reecriture-de-la-loi-informatique-et-libertes-du-6-janvier-1978-cnil

[886] Loi informatique et libertés de 1978, Art. 50 (modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018 – art. 1) dispose que « *Le droit de rectification s'exerce dans les conditions prévues à l'article 16 du règlement (UE) 2016/679 du 27 avril 2016.* », et Art 51 (modifié par l'ordonnance n° 2018-1125 du 12 décembre 2018 – art. 1) dispose que « *I.- Le droit à l'effacement s'exerce dans les conditions prévues à l'article 17 du règlement (UE) 2016/679 du 27 avril 2016.*
II.- En particulier, sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci.
En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation »

[887] Loi informatique et libertés de 1978, Art. 40 § I (Version en vigueur du 25 mai 2018 au 01 juin 2019).

Quant à l'obligation supplémentaire en cas de transmission de données à un tiers, elle comporte une régulation assez floue, pouvant mener à des interprétations et des inapplicabilités extensives et pénalisantes, puisque ladite loi vise l'accomplissement, par le responsable du traitement, des « diligences utiles » afin de notifier aux tiers les opérations effectuées[888].

Sans nommément le désigner, c'est la Cour de justice de l'Union qui a, en premier, consacré le droit à l'oubli numérique, sur le fondement de la directive de 1995, dans le cadre de l'affaire mettant en cause les pratiques de l'entreprise Google[889]. Elle s'est penchée, de prime abord, sur la question du juste équilibre entre le droit à l'oubli et le droit à l'information, en précisant qu'une « pondération » des droits et des intérêts opposés en cause, qui permet de « *[…] tenir compte de manière plus spécifique de toutes les circonstances entourant la situation concrète de la personne concernée* »[890], doit être effectuée, et que, dans le cadre de celle-ci, « l'importance des droits de la personne », résultant des articles 7 et 8 de la Charte, doit être également prise en compte[891]. Il semble alors que le *modus operandi* à suivre est d'opérer une « pesée des intérêts »[892] lorsqu'une personne exerce son droit à l'encontre d'un responsable du traitement qui est, dans ce cas, le moteur de recherche Google. Dans la pesée des intérêts effectuée lors de cette affaire, la Cour affirme clairement la prévalence de l'intérêt de la personne sur celui du moteur de recherche et sur celui des personnes souhaitant accéder aux informations. Cet équilibre n'est inversé, selon la Cour, que s'il apparaît, pour des raisons particulières, telles que le rôle joué par une personne dans la vie publique, que l'intérêt du public à avoir accès aux informations est « prépondérant »[893]. Elle a, dès lors, consacré un droit à l'oubli numérique, assez large, reposant sur le droit au déréférencement : « *toute personne a en*

---

[888] Loi informatique et libertés de 1978, Art. 119 : « *Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa du III.* »

[889] CJUE, Cour (Grande Ch.), Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) (Agence de protection des données) du 13 mai 2014, affaire C-131/12.

[890] CJUE, Arrêt Google Spain du 13 mai 2014, *Id.,* §76.

[891] CJUE, Arrêt Google Spain du 13 mai 2014, *Ibid.,* §74.

[892] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *op. cit.,* p. 186.

[893] CJUE, Arrêt Google Spain, *Ibid.,* §99 « *[…], il convient notamment d'examiner si la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. Cette dernière pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question.* »

principe le droit d'obtenir d'un moteur de recherche qu'il n'affiche pas certaines informations la concernant, même si ces informations ne lui sont pas préjudiciables »[894].

Il est évident que cet arrêt procède d'une triple hardiesse : premièrement, celle d'avoir inclus l'activité exercée par Google Inc., depuis les États-Unis, dans le champ d'application territorial de la directive 95/46, en se basant sur la présence sur le territoire d'un État membre, d'une succursale ou d'une filiale à vocation publicitaire[895] ; ensuite, celle d'avoir qualifié, d'une part, l'activité d'un moteur de recherche tel que Google de traitement de données et, d'autre part, les exploitants de moteur de recherche comme responsables dudit traitement[896] ; enfin, celle d'avoir dégagé un droit à l'effacement qui ressemble plus à un droit au déréférencement « paramétré de façon prétorienne »[897]. Toute personne peut donc exiger d'un exploitant d'un moteur de recherche qu'il supprime de la liste de résultats affichée, à la suite d'une recherche effectuée à partir de son nom, les liens vers des pages web publiées contenant des informations qui la concernent, y compris celles publiées et hébergées par des tiers[898]. En outre, la Cour a considéré que l'effet de l'ingérence d'un traitement de données, réalisé par un moteur de recherche, dans les droits fondamentaux de la personne « *se trouve démultiplié en raison du rôle important que jouent Internet et les moteurs de recherche dans la société moderne, lesquels confèrent aux informations contenues dans une telle liste de résultats un caractère ubiquitaire* »[899].

---

[894] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *Id.,* p. 186.

[895] CJUE, Arrêt Google Spain, *Id.,* 2° du dispositif « *L'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre.* »

[896] CJUE, Arrêt Google Spain*, Id.,* 1° du dispositif « *L'article 2, sous b) et d), de la directive 95/46/CE [...], doit être interprété en ce sens que, d'une part, l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de «traitement de données à caractère personnel», au sens de cet article 2, sous b), lorsque ces informations contiennent des données à caractère personnel et, d'autre part, l'exploitant de ce moteur de recherche doit être considéré comme le «responsable» dudit traitement, au sens dudit article 2, sous d).* »

[897] A. BRETONNEAU, « Le droit au « déréférencement » : champ territorial », Conclusions sur Conseil d'État, 19 juillet 2017, Google Inc., n° 399922, Lebon ; AJDA 2017, p. 1479, RFDA 2017, p. 972.

[898] CJUE, Arrêt Google Spain*, Id.,* 3° du dispositif « *Les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, afin de respecter les droits prévus à ces dispositions et pour autant que les conditions prévues par celles-ci sont effectivement satisfaites, l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite*. »

[899] CJUE, Arrêt Google Spain, *Ibid.,* § 80

Il est utile de noter que la double dénomination employée par les législateurs dans le RGPD, droit à l'effacement - droit à l'oubli, pour prévoir le droit à l'oubli numérique conformément à l'interprétation et à la logique suivies par la Cour, témoigne d'une hésitation quant à sa portée, et ses paramètres d'application, ainsi que d'un compromis difficile à atteindre. Avant même cet arrêt et ce nouveau Règlement, le concept et l'appellation de droit à l'oubli ne faisaient pas l'objet d'un consensus en Europe et ont reçu de nombreuses critiques, dans la mesure où ils évoqueraient, *inter alia*, « l'imposition du silence, donc la censure »[900] et pourraient porter atteinte à la liberté d'expression et d'information. Certains archivistes et historiens ont, par ailleurs, soulevé leurs inquiétudes quant aux risques que ce droit pourrait entraîner pour la recherche historique et la mémoire collective. D'autres, lors de l'élaboration du projet de Règlement sur la protection des données, se sont demandés s'il est possible de « concevoir un droit à l'oubli qui ne serait qu'un simple droit à l'effacement des données »[901]. La réponse, telle qu'il ressort des dispositions du RGPD, est celle de l'interprétation étendue fournie par la Cour dans son arrêt précité, en ce sens que le droit à l'effacement classique, se double dorénavant d'un droit à « l'oubli » permettant d'obtenir la suppression, par le responsable du traitement, des données personnelles transmises et publiées par des opérateurs tiers. Pour certains, c'est un droit « *improprement surnommé « à l'oubli », qui est en réalité un droit des individus à obtenir que, quand on tape leur nom sur un moteur de recherche en ligne, certains résultats ne sortent pas* »[902].

Il faut reconnaître que la portée accordée à ce droit par la Cour, dans son arrêt Google Spain, peut soulever des interrogations mais aussi des problèmes pratiques. Dans un premier temps, cet arrêt semble rétablir un équilibre entre la liberté d'expression et le respect de la vie privée, tel qu'il prévalait avant l'avènement d'internet, des moteurs de recherche et des nouvelles technologies. Ces nouveaux outils numériques ont, toutefois, changé la donne, l'information étant désormais essentiellement partagée et consultée sur internet et ses réseaux, engendrant un déséquilibre entre lesdits droits. Par ailleurs, il n'est pas exclu que cet arrêt soit étendu aux réseaux sociaux, qui peuvent être qualifiés de traitement de données, puisqu'ils permettent la mise en ligne d'informations personnelles et que leurs exploitants déterminent « les finalités et

[900] A. STROWEL, « Le « droit à l'oubli » : mal nommé, mal défini, mais bienvenu : À propos de l'arrêt Google de la Cour de justice », (préf.), *In* C. Castets-Renard (dir.), *Quelle protection des données personnelles en Europe ?*, Ed. Larcier, Bruxelles, 2015, p. 9-15 (Conférence Quelle protection des données personnelles en Europe ? Toulouse, 14/03/2014).
[901] I. FALQUE-PIERROTIN, Quelle protection européenne pour les données personnelles ?, Question d'Europe n° 250, publié sur le site de la Fondation Robert Schuman, septembre 2012.
[902] A. BRETONNEAU, « Le droit au « déréférencement » : champ territorial », *Id.*, p. 972.

les moyens » du traitement[903]. Par conséquent, si le même raisonnement adopté par la Cour dans ledit arrêt est suivi, les personnes disposeraient de droits d'effacement et d'opposition étendus, leurs offrant de « *larges possibilités d'obtenir l'effacement d'informations les concernant mises en ligne par des tiers ou par eux-mêmes, le consentement à un traitement de données pouvant être retiré* »[904].

En outre, se pose la question pratique du champ territorial du droit à l'oubli tel que mis en place par la Cour et repris par le RGPD, et, concurremment, la loi Informatique et libertés. Lorsqu'un moteur de recherche est tenu d'effacer, de déréférencer des données, cette obligation est-elle limitée à la zone géographique couverte par le droit de l'Union ou s'étend-elle au monde entier, compte tenu de l'indifférence d'internet aux frontières nationales, au moyen d'une forte dose d'extraterritorialité. De façon auxiliaire, il est utile de s'interroger sur le meilleur moyen de procéder à une limitation spatiale, territoriale du champ du déréférencement, de sorte que celui-ci ne soit pas aisément contourné. Dans ce contexte, lorsqu'une demande d'effacement de données est formulée, l'entreprise Google Inc. doit-elle déréférencer toutes les informations en ligne sur l'ensemble de ses terminaisons web ou l'ensemble des extensions de noms de domaine de son moteur en incluant celles mondiales (google.com), ou seulement sur ses terminaisons nationales et/ou européennes (par exemple : google.fr ou google.de). Sauf si, à ce titre, la suggestion de Google, à la suite de sa mise en demeure[905] et sa sanction par la CNIL[906], de

---

[903] RGPD, Art. 4, 7) « *«responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;* » ; Loi Informatique et libertés, Art. 2 al. 3 « Sauf dispositions contraires, dans le cadre de la présente loi s'appliquent les définitions de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016. » et Art 3 § I « *Sans préjudice, en ce qui concerne les traitements entrant dans le champ du règlement (UE) 2016/679 du 27 avril 2016, des critères prévus par l'article 3 de ce règlement, l'ensemble des dispositions de la présente loi s'appliquent aux traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire français, que le traitement ait lieu ou non en France.* ».

[904] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *Id.*, p. 188.

[905] CNIL, Décision n° 2015-047 du 21 mai 2015 mettant en demeure la société X, § II : « *Il en résulte donc que, dès lors qu'une demande de déréférencement est satisfaite conformément aux dispositions susmentionnées, elle doit nécessairement porter sur l'ensemble du moteur de recherche, quelles que soient les terminaisons utilisées. Dès lors, en l'espèce, le fait que des liens vers des sites Internet, déréférencés uniquement des noms de domaines correspondant à des extensions géographiques européennes du moteur de recherche, demeurent accessibles à tout utilisateur effectuant une recherche à partir des autres extensions du moteur de recherche constitue un manquement aux dispositions des articles 38 et 40 de la loi du 6 janvier 1978 modifiée précités.* »

[906] CNIL, Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X, § 2 : « *Une telle mesure ne permet pas de répondre aux impératifs d'efficacité, de complétude, d'effectivité et de non contournement qui s'imposent au regard de la décision précitée de la CJUE en ce que l'atteinte à la vie privée et à la protection des données à caractère personnel des personnes concernées persiste. Dès lors, seul un déréférencement sur l'ensemble du moteur de recherche est de nature à permettre une protection effective des droits des personnes. En conséquence, la formation restreinte considère que c'est à bon droit qu'il a été reproché à la société, dans la décision de mise en demeure du 21 mai*

mettre en place un système de « géoblocage », permettant de bloquer l'accès aux données déréférencées depuis le sol européen, ne soit adoptée, alors même que certains l'ont estimé insuffisante[907]. Cela dénote l'ampleur de la problématique centrale entourant le droit à l'oubli numérique et d'autres droits de la personne numériques, tels que le droit d'opposition ou de limitation, « *celle de l'adaptation des matrices juridiques traditionnelles, reposant sur une forte territorialisation du droit, à l'a-territorialité propre à l'outil numérique* »[908]. De plus, il semble que, à long terme, si le champ territorial du déréférencement s'étend en suivant les critères spécifiques au droit de l'Union, plus il y a de risques qu'interviennent des chocs de culture et de conception au-delà des frontières virtuelles de l'Europe. Par ailleurs, à la lecture de l'arrêt Google Spain, une pesée des intérêts entre l'atteinte à la vie privée et l'accès du public à l'information doit être effectuée, aussi apparaît-il raisonnable de s'interroger sur l'étendue de ce public, cible de l'information.

Cet arrêt semble, *in fine,* être émis de façon volontaire et délibérée par la Cour qui désire rendre plus effective et pertinente la protection des personnes dans le monde virtuel, en faisant tomber l'immunité rendue possible par la faculté d'exercer une activité mondiale sans devoir se soumettre aux règles nationales imposées par les États à l'intérieur de leurs territoires, faute de contrainte de localisation. Par conséquent, en assimilant avec vigueur les moteurs de recherche à des responsables de traitement et en tirant de leurs propres effets de majoration des informations une obligation *sui generis* leur imposant de mettre un terme à cet écho, la Cour a trouvé « une martingale juridique »[909] à l'effet « ubiquitaire » d'internet.

Pour la Cour, précisément, « *la mise en ligne de contenus sur un site Internet se distingue de la diffusion territorialisée d'un média tel un imprimé en ce qu'elle vise, dans son principe, à l'ubiquité desdits contenus. Ceux-ci peuvent être consultés instantanément par un nombre indéfini d'internautes partout dans le monde, indépendamment de toute intention de leur émetteur visant à leur consultation au-delà de son État membre d'établissement et en dehors de son contrôle* »[910].

2015, de ne pas procéder aux déréférencements sur toutes les extensions du nom de domaine du moteur de recherche ».

[907] Conseil d'État, Décision Google Inc., 19 juillet 2017, Requête n° 399922, §14 : « […]. *La formation restreinte de la CNIL a par ailleurs estimé insuffisante la proposition complémentaire dite de « géo-blocage » faite par la société Google Inc., après expiration du délai de mise en demeure, consistant à supprimer la possibilité d'accéder, depuis une adresse IP réputée localisée dans l'État de résidence du bénéficiaire du « droit au déréférencement », aux résultats litigieux à la suite d'une recherche effectuée à partir de son nom, ce indépendamment de la déclinaison du moteur de recherche qu'a sollicitée l'internaute.* »

[908] A. BRETONNEAU, « Le droit au « déréférencement » : champ territorial », *Id.*, p. 973.

[909] A. BRETONNEAU, « Le droit au « déréférencement » : champ territorial », *Id.*, p. 973.

[910] CJUE, Cour (Grande ch.), eDate Advertising c. X et O. M. et R.M. c. MGN Limited, du 25 octobre 2011, affaires jointes C-509/09 et C-161/10, §45.

B. Les droits d'opposition et de limitation

Complément du droit d'accès, du droit à l'information, du droit de rectification et d'effacement, le droit d'opposition exige, au même titre, la mise en place de modalités destinées à faciliter son exercice par toute personne concernée[911]. L'article 21, paragraphe 1 du Règlement prévoit ainsi le droit pour toute personne de s'opposer « *à tout moment, pour des raisons tenant à sa situation particulière* », à un traitement de données fondé sur les points e) ou f) de l'article 6 paragraphe 1, « *y compris un profilage fondé sur ces dispositions* »[912]. Les deux motifs visés par cette disposition présentent une particularité : s'ils s'appuient sur une appréciation objective des intérêts et des libertés et droits en jeu, en reconnaissant un droit d'opposition à la personne, ils impliquent également son autodétermination.

Ce droit à l'opposition ne doit pas être confondu avec le consentement envisagé par l'article 6, point a), qui doit être recueilli par le responsable du traitement afin de pouvoir traiter les données[913]. Celui-ci peut traiter les données, dans le contexte de l'article 6, point f), sous réserve de certaines conditions et garanties, à moins que ne prévalent des intérêts ou des droits fondamentaux qui exigent une protection des données personnelles, aussi longtemps que la personne ne s'y est pas opposée. Dans ce cadre, ce droit d'opposition semble plutôt se référer à une catégorie particulière de refus permettant à un individu de s'opposer ou de refuser un traitement déjà entamé, qui repose sur un fondement autre que le consentement et fait référence au droit d'opposition ou de refus d'un traitement[914]. Enfin, le Règlement précise que dans les

---

[911] RGPD, Cons. 59 « *Des modalités devraient être prévues pour faciliter l'exercice par la personne concernée des droits qui lui sont conférés par le présent règlement, y compris les moyens de demander et, le cas échéant, d'obtenir sans frais, notamment, l'accès aux données à caractère personnel, et leur rectification ou leur effacement, et l'exercice d'un droit d'opposition. Le responsable du traitement devrait également fournir les moyens de présenter des demandes par voie électronique, en particulier lorsque les données à caractère personnel font l'objet d'un traitement électronique. Le responsable du traitement devrait être tenu de répondre aux demandes émanant de la personne concernée dans les meilleurs délais et au plus tard dans un délai d'un mois et de motiver sa réponse lorsqu'il a l'intention de ne pas donner suite à de telles demandes.* »

[912] RGPD, Art. 21 – Droit d'opposition.

[913] Groupe de travail « Article 29 » sur la protection des données, Avis 15/2011 sur la définition du consentement, adopté le 13 juillet 2011, 01197/11/FR (WP 187), p. 39 : « *Il convient de ne pas confondre les situations dans lesquelles le responsable du traitement fonde le traitement des données à caractère personnel sur le consentement et celles où il s'appuie sur d'autres fondements juridiques impliquant un droit d'opposition de la personne concernée. Cela peut être le cas lorsque le traitement repose sur les «intérêts légitimes» du responsable du traitement au sens de l'article 7, point f), de la directive 95/46/CE, mais la personne concernée a néanmoins le droit de s'y opposer en vertu de l'article 14, point a), de ladite directive. […]* »

[914] Groupe de travail « Article 29 », Avis 15/2011 sur la définition du consentement, *Id.*, p. 35 : « *[…] chaque fois qu'un consentement est requis¸ il doit être obtenu avant le début du traitement des données. La possibilité d'entamer le traitement sans avoir préalablement obtenu de consentement n'est licite que lorsque la directive relative à la protection des données ou la directive «vie privée et communications électroniques», plutôt que d'exiger un consentement, prévoit un autre fondement et fait référence au droit d'opposition ou de refus du traitement. Ces mécanismes sont tout à fait distincts du consentement. Dans ces cas, le traitement peut avoir déjà commencé et la personne a le droit de s'y opposer ou de le refuser.* »

cas où l'opposition est justifiée, le traitement des données en question doit cesser, sous réserve de certaines conditions[915].

À l'instar de l'ancienne directive de 1995 sur la protection des données[916], la nouvelle législation requiert de la personne concernée de démontrer simplement qu'il existe des « raisons tenant à sa situation particulière » d'arrêter le traitement de ses données, sauf dans les cas d'activités de prospection où l'opposition n'a pas besoin d'être justifiée, « y compris au profilage dans la mesure où il est lié à une telle prospection », et ce, qu'il s'agisse d'un traitement initial ou ultérieur[917]. Ces raisons permettant d'arrêter le traitement ne doivent pas être perçues comme étant en contradiction avec la condition de mise en balance, de pesée des intérêts, visée au point f) de l'article 6 qui, pour sa part, s'applique *a priori*. Elles semblent plutôt compléter cette pesée d'intérêts dans la mesure où, lorsque le traitement est considéré comme licite à la suite d'une évaluation raisonnable et objective des différents intérêts et droits en cause, la personne jouit encore d'une possibilité additionnelle de manifester son opposition pour des motifs liés à sa situation particulière. Dans ce cas, une nouvelle appréciation doit alors être entamée, avec une prise en compte des arguments particuliers avancés par l'individu, et qui peut, par la suite, faire l'objet d'une autre appréciation soit par les tribunaux ou par les autorités chargées de la protection des données. Cette option de refus joue ainsi le rôle d'une garantie supplémentaire qui intervient, pour sa part, *a posteriori*.

Malgré le fait que le droit d'opposition est subordonné à la justification par la personne de raisons particulières à sa situation, « rien n'empêche le responsable du traitement de proposer une option de refus qui serait plus large »[918], et qui permettrait d'éviter toute démonstration supplémentaire de la part de la personne concernée. Dès lors, toute société souhaitant invoquer l'intérêt légitime visé à l'article 6, point f) du RGPD comme fondement juridique du traitement des données, doit alors accorder aux personnes un droit d'opposition tel que prévu par ledit

---

[915] RGPD, Art. 21 § 1 « *[…]. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.* »

[916] Directive 95/46/CE, Art. 14 - Droit d'opposition de la personne concernée « *Les États membres reconnaissent à la personne concernée le droit : a) au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. […]* »

[917] RGPD, Art. 21 § 2, et Cons. 70 « *Lorsque des données à caractère personnel sont traitées à des fins de prospection, la personne concernée devrait avoir le droit, à tout moment et sans frais, de s'opposer à ce traitement, y compris le profilage dans la mesure où il est lié à une telle prospection, qu'il s'agisse d'un traitement initial ou ultérieur. Ce droit devrait être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information.* »

[918] Groupe de travail « Article 29 » sur la protection des données, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, adopté le 9 avril 2014, 844/14/FR (WP 217), p. 50.

Règlement. Outre celui-ci, l'entreprise peut proposer un droit de refus et/ou de retrait plus large, inconditionnel et applicable de façon générale aux personnes sans prise en compte des situations particulières à chacune.

Actuellement très peu exercé dans la pratique, le droit de s'opposer au traitement de données a, cependant, la capacité de se « *transformer en un outil puissant dans les mains des parties prenantes lorsqu'il est appliqué comme un retrait inconditionnel « sans poser de questions »* »[919]. Ce retrait inconditionnel doit s'entendre comme le fait qu'un individu est conscient que ses données font l'objet de traitement et sait qu'il peut s'y opposer à tout moment, s'il le décide. Un consentement libre et valable n'est donc pas nécessaire, la personne étant implicitement d'accord ou non avec le fait que ses données soient traitées, et souvent, elle ne se trouve pas assez affectée négativement au point de modifier les paramètres par défaut, « *ou ne s'en donne simplement « pas la peine »* »[920]. Selon le contrôleur européen pour la protection des données, ce mécanisme « *influence subtilement la personne concernée à accepter le traitement, sans toutefois lui dénier totalement le droit de ne pas être d'accord* »[921]. En effet, surtout dans les cas douteux et ambigus, dans lesquels il est difficile de trouver un équilibre entre l'intérêt légitime du responsable du traitement et ceux des personnes, un mécanisme « bien conçu, viable et fonctionnel » permettant de refuser le traitement, sans nécessairement donner aux personnes tous les éléments requis pour un consentement valable et éclairé conformément aux dispositions du RGPD, a la capacité de contribuer prodigieusement à la préservation des droits et intérêts des personnes concernées[922].

Le choix du législateur européen de mentionner « les intérêts ou les droits et libertés fondamentaux » tend à accorder plus de protection à la personne concernée, puisqu'il requiert que ses intérêts soient aussi pris en considération en sus de ses droits et libertés fondamentaux. Ce choix paraît raisonné en ce sens que, si le responsable du traitement ou le tiers peut poursuivre n'importe quel intérêt, du moment que celui-ci est légitime, tout individu doit pouvoir raisonnablement s'attendre à ce que tous ses intérêts, collectivement et de toutes sortes ou natures, soient pris en compte et mis en balance face à ceux du responsable du traitement de façon pertinente. Ainsi, la mise en place d'un mécanisme et de garanties efficaces peuvent jouer

[919] CEPD, Avis n° 7/2015 « Relever les défis des données massives », *loc. cit.*, p. 13.
[920] CEPD, Avis n° 7/2015 « Relever les défis des données massives », *Id.*, p. 13.
[921] CEPD, Avis n° 7/2015 « Relever les défis des données massives », *Ibid.,* p. 13.
[922] Voir, en ce sens : CEPD, Avis n° 7/2015 « Relever les défis des données massives », *Ibidem.*, p. 13-14 et Groupe de travail « Article 29 », Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement, 844/14/FR (WP 217), *Id.,* p. 50-51.

un rôle primordial en vue de réduire les incidences injustifiées sur les personnes et, par là même, rétablir, voire modifier, l'équilibre des droits et intérêts.

En outre, les garanties susvisées peuvent comprendre, *inter alia*, des limitations strictes du volume de données collectées, des mesures techniques et organisationnelles visant à garantir une séparation fonctionnelle, la suppression immédiate des données après utilisation, le recours à des techniques d'anonymisation appropriées et à des technologies renforçant la protection de la vie privée, mais aussi plus de transparence et d'*accountability,* sans oublier la possibilité de s'opposer au traitement. Ceci dit, il est de l'avis du G29 que le « *recours à des garanties ne suffit bien sûr pas à justifier, à lui seul, n'importe quel traitement dans toutes les situations envisageables. Il faut en outre que les garanties en question soient adéquates et suffisantes, et qu'elles réduisent indubitablement et sensiblement les incidences sur les personnes concernées* »[923]. De plus, le RGPD prévoit une nouvelle garantie supplémentaire, à savoir, le droit pour une personne ayant exercé son droit d'opposition, *« pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée* », d'obtenir la limitation du traitement[924].

Il est donc nécessaire, en tant que société, d'adopter une approche nuancée avec sagesse afin de distinguer les cas dans lesquels il faut exiger des responsables du traitement qu'ils obtiennent un véritable consentement libre et éclairé, des cas où il est envisageable de se contenter d'une simple évaluation de la pesée des intérêts et d'un mécanisme de retrait inconditionnel. Il s'agit alors de distinguer le traitement des données dont les avantages sont à portée générale ou sociétale, de celui qui n'apporte que des avantages économiques aux entreprises qui les traitent. Et pour le contrôleur européen, « *nous devons également évaluer l'impact potentiel sur les personnes concernées et mettre soigneusement les deux en balance, tout en tenant compte d'autres facteurs pertinents* »[925].

---

[923] Groupe de travail « Article 29 », Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement, *Id.,* p. 34.

[924] RGPD, Art. 18 - Droit à la limitation du traitement « *1. La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :*
a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;
b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
c) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
d) la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée. »

[925] CEPD, Avis n° 7/2015 « Relever les défis des données massives », *Id.*, p. 14.

Cette analyse de l'impact désigne la manière dont les données sont traitées, pour évaluer l'impact des opérations envisagées sur la protection des données à caractère personnel ; ce qui peut consister, au sens large, à vérifier si les données ont été publiées ou rendues accessibles par n'importe quel moyen, ou si de larges volumes de données personnelles sont traités ou combinés avec d'autres données, en vue d'établir des profils à des fins commerciales ou judiciaires par exemple[926]. Aux termes du RGPD, l'analyse d'impact relative à la protection des données fait partie des obligations du responsable du traitement et du sous-traitant, et doit être entreprise avant le traitement[927]. Comme il a été précédemment vu, le traitement de données à grande échelle d'apparence anodine et leur combinaison avec d'autres données peuvent donner lieu à des inférences à propos d'informations sensibles. De plus, nous précise le G29, « *outre le fait qu'elle risque de permettre le traitement de données plus sensibles, ce genre d'analyse peut aussi conduire à des prévisions saugrenues, inattendues, voire inexactes concernant, par exemple, le comportement ou la personnalité des individus concernés* »[928]. En conséquence, l'intrusion dans la vie privée des individus peut s'avérer considérable et substantielle selon la nature et l'incidence de ces prévisions.

Par ailleurs, certaines mesures techniques et organisationnelles appropriées pour garantir la sécurité du traitement[929], telles qu'empêcher l'accès non autorisé à des réseaux de communications et la distribution de codes malveillants ou arrêter les attaques par « déni de service » et les dommages touchant les systèmes de communications numériques[930], sont susceptibles d'engendrer un déploiement à grande échelle d'analyse des paquets en profondeur, impactant sensiblement l'équilibre des droits[931]. Et le RGPD impose aux responsables du traitement et aux tiers d'évaluer les risques inhérents au traitement afin de garantir sa sécurité et prévenir tout traitement illicite, et exige que, dans le cadre de l'évaluation des risques pour la sécurité des donnés, il importe de prendre en compte les risques que présente le traitement « *tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non*

[926] *Cf.* p. 243.
[927] RGPD, Art. 35 – Analyse d'impact relative à la protection des données.
[928] Groupe de travail « Article 29 », Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement, *Id.,* p. 44.
[929] RGPD, Art. 32 – Sécurité du traitement.
[930] RGPD, Cons. 49.
[931] Groupe de travail « Article 29 », Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement, *Id.,* p. 44-45, et Groupe de travail « Article 29 », Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») (WP 159), Section 3.1.

autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral »[932].

Il n'empêche que, de façon générale, plus l'incidence de l'opération de traitement pourrait se révéler être négative ou équivoque, moins il est probable qu'elle sera jugée légitime au regard du critère de mise en balance des intérêts. En pratique, il s'est avéré jusqu'à présent que les différents mécanismes fonctionnels de retrait, qui peuvent être en outre facilités par des accords sectoriels, n'ont pas fourni de résultats concrets et valables conformément aux législations européennes en matière de protection des données. Ce fut le cas, par exemple, du configurateur de navigateur « *Do not Track* »[933] qui accorde la possibilité, selon ses promoteurs, de se soustraire, « *opt-out* », à la collecte de données concernant leurs habitudes en ligne grâce à un paramétrage de leurs navigateurs de recherche, sans avoir à décider au cas par cas pour chaque site. Pragmatiquement, elle s'est malheureusement avérée inefficace et a simplement contribué à la création d'un *loophole,* d'une échappatoire pour les géants d'internet rendant cette option de refus futile et caduque[934].

Ce droit d'opposition large, composante des droits de la personne, comprend par ailleurs le droit de ne pas faire l'objet de décision individuelle automatisée, y compris le profilage, sous conditions. Toute personne a le droit de ne pas faire l'objet d'une décision, y compris d'une mesure, qui implique l'évaluation de certains aspects personnels la concernant, prise sur la base d'un traitement automatisé et générant des effets juridiques à son égard ou l'affectant significativement, « *tels que le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine* »[935]. Cette forme de traitement comprend le « profilage », défini uniquement par le RGPD suivant, notamment, les recommandations du Conseil des ministres sur la protection des personnes à l'égard du traitement automatisé des données dans le cadre du profilage, et se réfère à toute forme de

[932] RGPD, Cons. 83.
[933] What is Do Not Track: https://allaboutdnt.com/#adjust-settings
[934] Par ex.: F. B. CAMPBELL Jr., "The Slow Death of 'Do Not Track'", The New York Times, du 26 décembre 2014, l'auteur souligne que "*Google, Facebook and other large companies that operate both first- and third-party businesses would be able to use data they gather through their first-party relationships to compete in the third-party ad market. Smaller ad tech companies would be at a severe competitive disadvantage and could even be driven out of the market.*": https://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html , et, K. HILL, "'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything", Gizmodo, du 15 octobre 2018: https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324
[935] RGPD, Cons. 71.

traitement automatisé de données personnelles utilisant celles-ci en vue d'évaluer les aspects personnels relatifs à une personne physique[936].

La nouvelle loi Informatique et libertés, telle que modifiée par la loi du 20 juin 2018, ne définit ni la notion de profil, ni celle de profilage, et se contente d'affirmer qu' « *aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage* », sous réserve d'exceptions tirées principalement du RGPD[937]. Ce dernier, conjointement avec la directive européenne du 27 avril 2016, ont laissé une grande marge de manœuvre aux États membres pour fixer les règles et les conditions applicables aux prises de décisions fondées sur un traitement automatisé y compris le profilage, en précisant qu'elles peuvent être permises lorsqu'elles sont « expressément » autorisées par le droit de l'Union ou le droit d'un État membre, à condition que tout traitement de ce type soit assorti de « garanties appropriées », telles que le droit de la personne d'obtenir une explication quant à la manière dont le traitement la concernant a été mis en œuvre ou son droit de contester la décision[938]. La nouvelle loi Informatique et libertés s'est, à ce stade aussi, contentée de

---

[936] RGPD, Cons. 71, Art. 4, point 4) « *«profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;* », et Art. 3, point 4) Directive UE 2016/680 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, du 27 avril 2016, JO L 119/89 (04/05/2016).

[937] Loi Informatique et libertés, Art. 47 (Modifié par l'ordonnance du 12 décembre 2018) : « *[...], à l'exception :*
1° Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande ;
2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 6 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard. »

[938] RGPD, Cons. 71 « *[...]. Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis, y compris aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale conformément aux règles, normes et recommandations des institutions de l'Union ou des organes de contrôle nationaux, et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement, ou nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou si la personne concernée a donné son consentement explicite. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine,*

souligner l'interdiction du recours à ce type de traitement dans des cas bien visés, en distinguant les décisions de justice des autres décisions. Elle affirme ainsi, dans le cadre du chapitre dédié aux dispositions applicables aux traitements relevant de la directive UE 2016/680[939], que tout traitement automatisé de données personnelles destiné « à évaluer certains aspects de la personnalité de cette personne », sur lequel se fonde une décision de justice impliquant une appréciation sur le comportement d'une personne, est interdit. De même, aucune autre décision produisant des effets juridiques à l'égard d'une personne, ou l'affectant de manière significative, ne peut être prise sur le « seul fondement » d'un traitement automatisé destiné à « prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée »[940]. Par ailleurs, en ce qui concerne le profilage pratiqué par les autorités compétentes, en application de la directive UE 2016/680, la loi précise simplement que tout profilage qui engendre une discrimination à l'égard des personnes, sur la base des catégories particulières de données personnelles visés par l'article 8, est interdit.

Au regard des différentes atteintes qu'un tel type de traitement pourrait porter à plusieurs droits et libertés fondamentales, combiné au développement constant des technologies de l'information et de la communication facilitant la collecte et le traitement de données à grande échelle dans le secteur public comme privé, à des fins aussi diverses que variées, et au développement continu de technologies convergentes soulevant de plus en plus de défis quant à la collecte et au traitement ultérieur des données, le Comité des ministres avait, dès 2010, formulé des recommandations aux États membres en vue d'assurer une meilleure protection des personnes concernant la collecte et le traitement de leurs données personnelles dans le cadre du profilage, en soulignant la nécessité pour les États de prendre des mesures « *pour que les principes contenus dans l'annexe à la présente recommandation soient reflétés dans leur droit et leur pratique* »[941]. L'annexe définit à la fois la notion de profil et celle de profilage, en précisant que « *le terme "profil" désigne un ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu* »[942], là où la notion de profilage

---

d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision. Cette mesure ne devrait pas concerner un enfant. »

[939] Loi Informatique et libertés, Titre III : Dispositions applicables aux traitements relevant de la directive UE 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/ JAI du Conseil.

[940] Loi Informatique et libertés, Art. 95 al. 2.

[941] Recommandation CM/Rec (2010)13, du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée par le Comité des Ministres le 23 novembre 2010, Recommandation n° 1, p. 3.

[942] Annexe à la Recommandation CM/Rec (2010)13, *Id.,* Art. 1, point d.

constitue « *une technique de traitement automatisé des données qui consiste à appliquer un « profil » à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels* »[943].

Dans le RGPD, un article dédié spécifiquement au profilage n'a pas été prévu, les rédacteurs ayant préféré que plusieurs articles, notamment liés aux droits de la personne, en déduisent les conséquences. C'est le cas des informations à fournir lorsque des données personnelles sont ou non collectées auprès de la personne, tel que prévu aux articles 13 et 14, le tout afin de « garantir un traitement équitable et transparent ». Ainsi, au titre de cette garantie, des informations, non seulement sur « l'existence d'une prise de décision automatisée, y compris un profilage », mais aussi « sur la logique sous-jacente, ainsi que l'importance et les conséquences que ce traitement pourrait avoir » doivent être fournies[944]. C'est également le cas du droit d'opposition permettant à toute personne concernée de s'opposer à un profilage fondé sur un tel type de traitement.

[943] Annexe à la Recommandation CM/Rec (2010)13, *Ibid.,* Art. 1, point e.
[944] RGPD, notamment, Cons. 63, et Art. 13-2, point f), 14-2, point g) et 15-1, point h).

Chapitre II. Un régime de protection transfrontalier : Une influence souveraine

> « *Le langage a alors pris sa stature souveraine ; il surgit comme venu d'ailleurs, de là où personne ne parle ; mais il n'est œuvre que si, remontant son propre discours, il parle dans la direction de cette absence.* »[945]

En sus d'être harmonisé, le droit à la protection des données ainsi analysé s'avère être transfrontalier, « *qui concerne le franchissement d'une frontière* »[946], soulignant la vocation internationale, cosmopolite, rattachée au régime de protection des données à caractère personnel nouvellement mis en œuvre, particulièrement à l'échelle européenne et française ; le numérique et les technologies de l'information et de la communication n'ayant aucune notion des frontières ou espaces délimités.

Ce régime de protection se caractérise par son aspect souverain, « qui est suprême, au plus haut degré ; qui règne en maître, l'emporte sur les autres, sur tout »[947], qui représente un « idéal » à suivre, porteur d'une « efficacité totale, assurée », dénotant, par conséquent, l'influence souveraine suscitée par le régime de protection européen au sein du corpus juridique mondial relatif à la protection des données à caractère personnel. C'est donc une influence initiée principalement par l'ère de la révolution technologique, qui a provoqué la mise en place dudit régime de protection des données, régime qui, par la suite, s'est avéré à vocation mondiale, porteur d'une autorité souveraine en la matière, et qui implique, simultanément, les concepts de souveraineté étatique et de souveraineté numérique. Cette notion de souveraineté évoque, dans son essence, le « *caractère absolu, sans limite, sans restriction (d'un droit, d'une faculté, d'une loi dans son application)* », ou encore la « *domination, suprématie (de quelqu'un, de quelque chose, sur d'autres, dans un domaine particulier)* »[948], caractérisant l'influence souveraine, dominante, désormais exercée par le régime de protection des données à l'échelle internationale et incarnant, à la fois, une souveraineté étatique et numérique.

La souveraineté étatique, nationale, une « qualité propre à l'État », désigne, en droit, « *[…] la détention de l'autorité suprême, c'est-à-dire d'un pouvoir absolu (dont tous dépendent) et*

---

[945] J. REVEL, *Le vocabulaire de Foucault, op cit.,* p. 13.
[946] Dictionnaire Larousse, « Transfrontalier » : https://www.larousse.fr/dictionnaires/francais/transfrontalier/79124
[947] Dictionnaire de l'Académie Française, 9ème Ed., « Souverain, aine » : https://www.dictionnaire-academie.fr/article/A8S1420 ; et, CNRTL, « Souverain, aine » : https://cnrtl.fr/definition/souveraine
[948] CNRTL, « Souveraineté » : https://cnrtl.fr/definition/souveraineté

inconditionné (qui ne dépend de qui que ce soit) »[949]. Autrement dit, « *le principe de toute Souveraineté réside essentiellement dans la nation. Nul corps, nul individu ne peut exercer d'autorité qui n'en émane expressément* »[950]. Quant au concept de souveraineté numérique, il s'est notamment manifesté en juin 2009, lorsque la ministre de l'Intérieur française annonce vouloir « *"garantir la souveraineté numérique" et, à cette fin, "étendre à l'espace numérique le champ de l'état de droit"* »[951].

Il faut admettre qu'avec l'avènement de la révolution numérique, la plupart des activités humaines s'opèrent en ligne, par le biais des nouvelles technologies, suscitant « un rapport de force » avec les géants du web et toute entreprise qui règne sur et dépend des réseaux numérique ; ce qui entraîne conséquemment la nécessité de « *préserver ou de reconquérir une part du pouvoir qui s'exerce dans ces nouveaux espaces, pourtant conçus pour échapper à l'emprise étatique, ce que résume la célèbre Déclaration d'indépendance du cyberespace de […] Barlow en 1996 : "Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Vous n'avez aucun droit de souveraineté sur nos lieux de rencontre. Vous n'êtes pas les bienvenus parmi nous."* »[952].

Cette notion de souveraineté numérique s'entend, toutefois, à l'heure actuelle comme « la capacité de l'État à agir dans le cyberespace »[953], ce qui représente une « condition nécessaire à la préservation de nos valeurs »[954]. De ce fait, elle implique, d'une part, « une capacité autonome d'appréciation, de décision et d'action dans le cyberespace » et, d'autre part, « une capacité de garder ou restaurer la souveraineté sur les outils numériques » facilitant la maîtrise de « nos réseaux, nos communications électroniques et nos données »[955].

Comment ce régime de protection ainsi construit se décline-t-il dans sa portée internationale, transfrontalière ? Quels sont, plus particulièrement, les droits, principes et obligations à connotation souveraine et universelle mis en œuvre ?

---

[949] F. BARON, « La Souveraineté nationale », Parole d'expert, publié le 7 juillet 2018 : https://www.vie-publique.fr/parole-dexpert/270252-la-souverainete-nationale

[950] Déclaration des droits de l'homme et du citoyen de 1789, Art. 3.

[951] Michèle Alliot-Marie, ancienne Ministre de L'intérieur de France, citée par M. UNTERSINGER, « L'incertaine mais nécessaire "souveraineté numérique" », Le Monde, publié le 20 novembre 2019 : https://www.lemonde.fr/idees/article/2019/11/20/l-incertaine-mais-necessaire-souverainete-numerique_6019810_3232.html

[952] P. TÜRK, « Définition et enjeux de la souveraineté numérique », Parole d'expert, publié le 14 septembre 2020 : https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique ; et, M. UNTERSINGER, « L'incertaine mais nécessaire "souveraineté numérique" », *Id.*

[953] Rapport n°7 de M. G. LONGUET, fait au nom de la commission d'enquête, sur la souveraineté numérique déposé le 1er octobre 2019, t. I, p. 16 ; disponible en ligne : https://www.senat.fr/rap/r19-007-1/r19-007-10.html#toc0 ; https://www.senat.fr/rap/r19-007-1/r19-007-1.html

[954] Rapport n°7 de la Commission d'enquête du Sénat sur la souveraineté numérique, *Id.*, p. 8.

[955] Rapport n°7 de la Commission d'enquête du Sénat sur la souveraineté numérique, *Ibid.*, p. 16.

Il apparaît, à travers cette étude, qu'afin d'assurer la visée mondiale du régime de protection européen, tout en prenant en compte la dimension transfrontalière des données et des nouvelles technologies, une nouvelle dynamique internationale de protection a été instaurée (Section 1), et, parallèlement, une nouvelle conception de protection numérique souveraine, d'une efficacité assurée, a vu le jour (Section 2) ; l'ensemble révélant l'influence souveraine et absolue exercée, depuis lors, par le régime de protection des données personnelles européen.

Section 1 – Une nouvelle dynamique internationale de protection

C'est une nouvelle dynamique manifestée par les dispositions légales, qui se base principalement sur une logique inversée correspondant au principe de l'*accountability*, le régime de responsabilité – de responsabilisation, dont le champ d'application s'étend à l'international, et qui se décline en un régime de responsabilité s'avérant être à connotation utilitaire avec une approche fondée sur le risque et l'*accountability* (§1), ainsi qu'en un régime à connotation répressive présentant une approche fondée sur un double système de sanction (§2).

§1. Un régime de responsabilité à connotation utilitaire : approche fondée sur le risque et l'accountability

Ce régime de responsabilité ainsi mis en place se présente comme étant à connotation utilitaire, suivant une approche fondée sur le risque et l'*accountability*, se traduisant par un système de reddition de compte d'une utilité *a posteriori* (A) et par un système d'autorégulation d'une utilité *a priori* (B).

A. Un système de reddition de compte *a posteriori*

Aux termes du RGPD, le responsable du traitement, seul ou conjointement avec d'autres en cas de multiplicité d'acteurs[956], est tenu de mettre en œuvre des « mesures techniques et organisationnelles appropriées » lui permettant de s'assurer et de démontrer qu'il répond et se conforme aux exigences du Règlement[957]. Ces mesures et garanties se justifient, aux yeux du législateur européen, en raison de la nature, de la portée, du contexte et des finalités du

[956] C'est le cas lorsque le traitement est effectué par deux responsables du traitement ou plus, c'est le cas du sous-traitant qui peut être seul acteur sur les opérations de traitement ou conjointement avec d'autres sous-traitants ou avec des responsables du traitement, c'est aussi le cas du représentant du responsable du traitement ou du sous-traitant : voir, en ce sens, RGPD, Art. 26, 27 et 28.
[957] RGPD, Chap. IV, Section I – Obligations générales, Art. 24 – Responsabilité du responsable du traitement.

traitement, de l'état des connaissances et des coûts de mise en œuvre, « *ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques* »[958].

Au titre de l'article 30, une nouvelle obligation à la charge du responsable du traitement et du sous-traitant est introduite : « *la tenue d'un registre des activités de traitement effectuées sous leur responsabilité* », mettant à l'écart la notification générale à l'autorité de contrôle exigée par l'ancienne directive 95/46/CE sur la protection des données personnelles[959], désormais abrogée. Cette obligation moins formaliste impose, par conséquent, aux responsables du traitement de tracer l'ensemble des traitements de données opérés pour s'assurer, et pouvoir éventuellement le démontrer, que ceux-ci sont en conformité avec la législation en vigueur.

Cette obligation de tenir un registre de conformité se prouve être complexe et éparse en pratique, découlant de différentes dispositions du Règlement. En premier lieu, en tant que responsable du respect des principes relatifs au traitement des données personnelles, le RGPD exige du responsable du traitement d'être en mesure de démontrer que celui-ci est respecté, en précisant que cette obligation lui incombe au regard de sa responsabilité[960]. Cette même obligation est reprise au niveau de l'article ayant trait aux responsabilités du responsable du traitement, dans lequel cette obligation générale est assortie à une mise en œuvre de mesures techniques et organisationnelles appropriées, et au recours à un code de conduite ou à des mécanismes de certification approuvés comme éléments de supports, de preuve[961].

Pour ce faire, le responsable du traitement doit, à la fois, tracer les traitements effectués, mais aussi leurs conformités à l'ensemble des exigences imposées par le RGPD. Enfin, cette obligation est visée directement par les termes de ce dernier, qui mentionne expressément la tenue d'un registre des activités de traitement effectuées sous leur responsabilité, « sous une

---

[958] RGPD, Art. 24, 25, 32.

[959] Directive 95/46/CE, Art. 18 – Obligation de notification à l'autorité de contrôle « *1. Les États membres prévoient que le responsable du traitement, ou le cas échéant son représentant, doit adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées*. »

[960] RGPD, Art. 5 §2 « *Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité)* »

[961] RGPD, Art. 24 « *1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire. [...]*

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement. »

forme écrite y compris la forme électronique »[962], et les informations que celui-ci doit comporter[963]. Une exception légale à cette dernière obligation est, par ailleurs, prévue à l'article 30 paragraphe 5 du Règlement au bénéfice des entreprises et organisations comptant moins de 250 salariés, sous certaines réserves[964].

Une lecture combinée des dispositions traitant de cette obligation montre que ce registre a un rôle fondamental, permettant de lister les traitements opérés au sein de l'organisation pour s'assurer qu'ils sont conformes aux exigences légales. En effet, exigée par diverses dispositions du Règlement, le respect de cette obligation impose que tout traitement mis en œuvre soit listé, indexé, puis audité et, enfin, enregistré dans un registre d'activités. Or, l'article 30, paragraphe 5, autorise les petites et moyennes entreprises et organisations à ne pas tenir de registre, alors que la conjugaison des articles 5 et 24 réclame, *de facto*, sa tenue, traduisant ainsi une contradiction au sein même des prescriptions du Règlement.

La dernière réforme de la loi Informatique et libertés a prévu cette nouvelle obligation exigeant la tenue d'un registre des activités de traitement dans les conditions susvisées par le Règlement, et, dans le cas des traitements relevant de la directive police-justice, « *dans les conditions prévues aux 1 à 4 de l'article 30* » du RGPD[965]. Elle a, dès lors, volontairement écarté l'exception prévue au paragraphe 5 de l'article 30 visant les établissements de moins de 250 salariés. Ce choix semble marquer la volonté du législateur français d'éviter la contradiction susmentionnée, mais risque de rendre le respect des obligations imposées par les législations en la matière, à savoir le Règlement et la nouvelle loi Informatique et libertés, un impératif ésotérique, difficultueux et énigmatique.

Selon ces législations nationale et européenne, le registre en question doit contenir, *a minima*, les informations suivantes : le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ; les finalités et les fondements du traitement ; une

---

[962] RGPD, Art. 30 §3 « *Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.* »

[963] RGPD, Art. 30 – Registre des activités de traitement « *1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes : […]*»

[964] RGPD, Art. 30 §5 « *Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.* »

[965] Loi Informatique et libertés, Art. 57 et 60 ; et Art. 100 « *Le responsable de traitement et son sous-traitant tiennent un registre des activités de traitement dans les conditions prévues aux 1 à 4 de l'article 30 du règlement (UE) 2016/679 du 27 avril 2016. […]*»

description des catégories de personnes concernées et des catégories de données à caractère personnel ; les catégories de destinataires auxquels les données ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ; le cas échéant, le recours au profilage et les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ; et enfin, dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ainsi qu'une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1[966]. Dans ce cadre, lister les traitements effectués, et suivre et contrôler leurs conformités, en prenant des mesures et techniques organisationnelles adéquates, se révèle être des minima.

Une autre forme de reddition de compte, désormais prévue par le RGPD, se manifeste à travers l'obligation de notification et celle de communication, visées respectivement par les articles 33 et 34, en cas de violation de données à caractère personnel. Une telle violation risque, « *si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important* »[967]. Par conséquent, le responsable du traitement doit notifier à l'autorité de contrôle dans les meilleurs délais, et 72 heures au plus tard si possible, la violation qui s'est produite, à moins qu'il ne puisse démontrer qu'il est peu probable que ladite violation engendre un risque pour les droits et libertés des personnes physiques[968]. Respectivement, celui-ci est tenu de communiquer à la personne concernée, « en des termes clairs et simples », la violation produite dans les meilleurs délais[969].

---

[966] RGPD, Art. 30 §1, points a) à g), et Loi Informatique et libertés, Art. 100 « *[…]. Ce registre contient aussi la description générale des mesures visant à garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel mentionnées au I de l'article 6 de la présente loi, l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées et, le cas échéant, le recours au profilage.* »

[967] RGPD, Cons. 85.

[968] RGPD, Cons. 85 et Art. 33 §1.

[969] RGPD, Art. 34 §§ 1 et 2.

Cette nouvelle obligation de notification et de communication semble s'inspirer de l'article 4, paragraphe 2, de la directive vie privée et communications électroniques qui impose au fournisseur d'un service de communications électroniques d'informer ses abonnés lorsqu'il existe un risque particulier de violation[970]. L'obligation de notification, à destinataires doubles, dorénavant imposée par le RGPD, précise les éléments devant être impérativement, et « à tout le moins », compris dans la notification : une description de la nature de la violation (uniquement dans le cas de notification à l'autorité de contrôle), nom et coordonnées de tout point de contact pouvant fournir des informations supplémentaires, une description des conséquences probables de la violation, ainsi qu'une description des mesures prises ou envisagées par le responsable du traitement pour remédier à la violation[971]. En ce qui concerne les sous-traitants, ils sont uniquement tenus de notifier au responsable du traitement toute violation de données, « dans les meilleurs délais après en avoir pris connaissance »[972].

Le Règlement a eu la bienveillance de fournir une définition de ce que représente une "violation de données", en précisant que c'est « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière,* ***ou*** *l'accès non autorisé à de telles données* ». Reprise dans la loi Informatique et libertés, cette définition et, conséquemment, l'obligation de notification rattachée s'appliquent exclusivement « *au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de*

---

[970] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), Art. 4 §2. « *Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable.* »

[971] RGPD, Art. 33 §3. « *La notification visée au paragraphe 1 doit, à tout le moins : a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ; b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ; c) décrire les conséquences probables de la violation de données à caractère personnel ; d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.* » ; et Art. 34 §2. « *La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).* »

[972] RGPD, Art. 33 §2.

données et d'identification »[973]. En ce sens, seul le fournisseur de service de communications électroniques est tenu d'avertir, « sans délai », la CNIL, en cas de violation de données personnelles, et l'intéressé « *lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique* »[974].

Il apparaît ainsi que la communication est la règle mais, comme toute règle, elle est assortie d'exceptions : elle n'est pas nécessaire « si l'une ou l'autre des conditions suivantes est remplie », à savoir, si des mesures techniques et organisationnelles appropriées ont été appliquées aux données affectées par la violation, ou si des mesures ultérieures garantissant que le risque élevé pour les droits et libertés des personnes « n'est plus susceptible de se matérialiser » ont été prises, ou encore si la communication exigerait « des efforts disproportionnés »[975]. Cette dernière exception est aussi prévue dans le cadre de l'obligation de notification en ce qui concerne la rectification ou l'effacement de données, ou la limitation du traitement. De plus, le Règlement prévoit une autre exception à cette obligation de notification en question dans le cas où une « telle communication se révèle impossible »[976].

Le RGPD prévoit, dès lors, que pour que l'exception s'applique, il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre, afin d'établir « immédiatement » si une violation s'est produite et d'informer « rapidement » l'autorité de contrôle et la personne physique[977]. Pour ce faire, des règles détaillées concernant

---

[973] Loi Informatique et libertés, Art. 83 § I (Créé par l'ordonnance n° 2018-1125 du 12 décembre 2018, entré en vigueur en même temps que le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés au 1er juin 2019).

[974] Loi Informatique et libertés, Art. 83 § II.

[975] RGPD, Art. 34 §3. « *La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :*
a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;
c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace. » ; et, Loi Informatique et libertés, Art. 83 § II. « *La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.* »

[976] RGPD, Art. 19 - Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement « *Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué conformément à l'article 16, à l'article 17, paragraphe 1, et à l'article 18, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.* »

[977] RGPD, Cons. 87.

la forme et les procédures applicables à la notification des violations doivent être fixées, en tenant « dûment compte des circonstances de cette violation », y compris du fait que les données étaient ou non protégées par les mesures de protection appropriées susvisées, « limitant efficacement la probabilité d'usurpation d'identité ou d'autres formes d'abus »[978].

Afin de respecter toutes ces exigences et ces exceptions, le RGPD et la loi Informatique et libertés commandent la tenue d'un documentaire, en ce qui concerne le premier, ou d'un inventaire « à jour », en ce qui concerne la seconde, qui précise les faits et les modalités de toute violation ainsi que leurs effets et les mesures prises pour y remédier ; documentaire ou inventaire qui doit être à la disposition de l'autorité de contrôle pour vérification, caractérisant *de facto* un système de reddition de compte[979].

Cette nouvelle double obligation de notification *a posteriori* vient remplacer l'obligation de notification générale des traitements de données aux autorités de contrôle prévue par l'ancienne directive 95/46/CE qui, selon le législateur européen, génère une charge administrative et financière « *sans pour autant avoir systématiquement contribué à améliorer la protection des données à caractère personnel* »[980]. Par conséquent, il convient de supprimer les obligations générales de notifier sans distinction, et les remplacer par des « *procédures et des mécanismes efficaces ciblant plutôt les types d'opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, du fait de leur nature, de leur portée, de leur contexte et de leurs finalités* »[981].

Par ailleurs, parmi les mesures et garanties appropriées, facilitant le respect des exigences et des obligations à la charge du responsable du traitement, et dont le Règlement fait la promotion, figurent les codes de conduite et les certifications, qui contribuent « *à la mise en œuvre de mesures appropriés et à la démonstration par le responsable du traitement ou le sous-traitant*

---

[978] RGPD, Cons. 88 qui poursuit « *[…]. Par ailleurs, ces règles et procédures devraient tenir compte des intérêts légitimes des autorités répressives lorsqu'une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation des données à caractère personnel.* »

[979] RGPD, Art. 33 §5 « *Le responsable du traitement documente toute violation de données à caractères personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.* », et, Loi Informatique et libertés, Art. 83 § III. « *Chaque fournisseur de services de communications électroniques tient à jour un inventaire des violations de données à caractères personnel, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition de la commission.* »

[980] RGPD, Cons. 89.

[981] RGPD, Cons. 89, et le législateur précise que « *Ces types d'opérations de traitement peuvent inclure ceux qui, notamment, impliquent le recours à de nouvelles technologies ou qui sont nouveaux et pour lesquels aucune analyse d'impact relative à la protection des données n'a été effectuée au préalable par le responsable du traitement, ou qui deviennent nécessaires compte tenu du temps écoulé depuis le traitement initial.* »

du respect du présent règlement »[982]. En ce sens, l'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé fournit une garantie et sert à démontrer le respect des obligations leur incombant[983], caractérisant de façon indirecte et subtile une reddition de compte inversée.

Ainsi, le Règlement encourage les associations et organismes représentant des catégories de responsables du traitement à élaborer des codes de conduite destinés à faciliter la bonne application du Règlement, en prenant en compte les besoins spécifiques des micros, petites et moyennes entreprises, mais aussi la spécificité propre aux traitements effectués dans différents secteurs[984]. Selon le législateur, ces codes fournissent des directives en définissant, notamment, les obligations incombant aux responsables du traitement et aux sous-traitants, « *compte tenu du risque que le traitement peut engendrer pour les droits et libertés des personnes physiques* »[985]. Élaborés par des acteurs professionnels (fédérations, associations ou organisations professionnelles) et modifiés ou prorogés selon les besoins[986], ces codes de conduite, équivalents à un outil de conformité, traduisent des modalités d'application concrètes de la réglementation sur la protection des données à un secteur d'activité en particulier. Ils se constituent de lignes directrices et de bonnes pratiques portant sur, *inter alia*, le traitement loyal et transparent, les intérêts légitimes poursuivis dans des contextes spécifiques, la collecte et la pseudonymisation des données à caractère personnel, les informations communiquées au public et aux personnes concernées, l'exercice des droits des personnes, les informations communiquées aux enfants et la protection spécifique dont ils bénéficient, les mesures et procédures visées dans le cadre de la responsabilité du responsable du traitement et dans le contexte de la protection des données dès la conception et par défaut, ainsi que les mesures visant à assurer la sécurité du traitement, la notification et la communication des violations de

---

[982] RGPD, Cons. 77 « *Des directives relatives à la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou le sous-traitant du respect du présent règlement, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque, pourraient être fournies notamment au moyen de codes de conduite approuvés, de certifications approuvées et de lignes directrices données par le comité ou d'indications données par un délégué à la protection des données. […]* »

[983] RGPD, Cons. 81 « *[…]. L'application par un sous-traitant d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à démontrer le respect des obligations incombant au responsable du traitement. […]* »

[984] RGPD, Cons. 98 et Art. 40 §1.

[985] RGPD, Cons. 98.

[986] RGPD, Cons. 99 « *Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations.* »

données, le transfert des données ou les voies de recours et procédures extrajudiciaires valables[987].

Pour être ensuite « approuvé » et servir de démonstration, le code de conduite doit être soumis à l'autorité de contrôle compétente, qui rend un avis sur la question de savoir si le code respecte concrètement le Règlement, et l'approuve, si elle estime qu'il offre des « garanties appropriées suffisantes »[988]. Selon la CNIL, reconnue par la loi Informatique et libertés consolidée comme étant « l'autorité de contrôle nationale au sens et pour l'application du Règlement »[989], un code de conduite ne peut se contenter de reprendre simplement les dispositions du RGPD, « *mais doit les traduire de manière opérationnelle et adaptée pour répondre aux besoins et problématiques du domaine d'activité, qui doivent être recensés, identifiés et qualifiés* »[990]. Pour répondre à ces exigences, le code de conduite doit donc fournir des propositions précises et effectives, sous forme de fiches thématiques, de modèles de mentions d'informations adaptés, de modalités pratiques d'exercice des droits ou encore de recommandations concrètes sur les mesures à appliquer[991]. D'ailleurs, le RGPD précise que ce code doit comprendre des mécanismes permettant à l'organisme chargé du suivi des codes approuvés de procéder au contrôle obligatoire du respect de ses dispositions par les organisations qui s'engagent à l'appliquer, lui conférant ainsi un caractère contraignant[992]. De plus, l'application d'un code de conduite approuvé par une organisation qui n'est pas soumise au Règlement (en vertu de l'article 3) peut servir de garanties appropriées dans le cadre d'un transfert de données vers un pays tiers ou une organisation internationale, du moment que celle-ci prend l'engagement contraignant et doté de force obligatoire, moyennant des instruments contractuels ou

---

[987] RGPD, Art. 40 §2, points a) à k).

[988] RGPD, Art. 40 §5 « *Les associations et autres organismes visés au paragraphe 2 du présent article qui ont l'intention d'élaborer un code de conduite ou de modifier ou proroger un code de conduite existant soumettent le projet de code, la modification ou la prorogation à l'autorité de contrôle qui est compétente en vertu de l'article 55. L'autorité de contrôle rend un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le présent règlement et approuve ce projet de code, cette modification ou cette prorogation si elle estime qu'il offre des garanties appropriées suffisantes.* »

[989] Loi Informatique et libertés, Art. 8 § I. 2. b) (Modifié par la l'ordonnance du 12 décembre 2018) qui dispose qu'à ce titre « *[...] Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables de traitement et à leurs sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques, notamment des mineurs. Elle homologue et publie les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel. Elle prend en compte, dans tous les domaines de son action, la situation des personnes dépourvues de compétences numériques, et les besoins spécifiques des collectivités territoriales, de leurs groupements et des microentreprises, petites entreprises et moyennes entreprises ; »*

[990] CNIL, « La certification et les codes de conduite », 19 décembre 2018 : https://www.cnil.fr/fr/la-certification-et-les-codes-de-conduite

[991] CNIL, « La certification et les codes de conduite », *Id.,* et l'autorité de contrôle précise que « *le recueil de l'avis des professionnels du secteur est indispensable pour relever les difficultés rencontrées par le secteur dans la mise en œuvre des principes informatique et libertés* ».

[992] RGPD, Art. 40 §4.

juridiquement contraignants, d'appliquer ces garanties dites appropriées[993]. L'instauration et l'élaboration de ces codes de conduite répondent ainsi aux préconisations et conditions de l'étude du Conseil d'État sur le droit souple, afin que ceux-ci soient légitimes et effectifs[994].
La loi Informatique et libertés, dans sa dernière version, ne mentionne les codes de conduite que dans le cadre de son chapitre dédié aux mesures et sanctions prises par la formation restreinte de la CNIL, lorsque le non-respect des dispositions du Règlement et celles de la loi entraîne une violation des droits et libertés visés par la loi[995], à savoir l'identité humaine, les droits de l'homme, la vie privée, les libertés individuelles ou publiques[996].

En outre, les mécanismes de certification et les labels et marques, également encouragés par le Règlement, représentent un autre outil de conformité servant à rendre des comptes, en vue de prouver limpidement le respect de la réglementation, mais aussi, de permettre aux personnes « *d'évaluer rapidement le niveau de protection des données offert par les produits et services en question* »[997]. Prévue par les articles 42 et 43 du RGPD, la certification constitue une procédure qui permet à une organisation ou un professionnel de demander à un organisme tiers de certification d'évaluer et d'attester que ses produits, services, processus ou compétences sont en conformité avec les « critères des référentiels de certification ou d'agrément »[998]. Elle sert

---

[993] RGPD, Art. 40 §3.
[994] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *op. cit*., p. 183 où le Conseil affirme ainsi que « *[…]. Conformément aux préconisations de l'étude annuelle de 2013 du conseil d'État sur Le droit souple, plusieurs conditions doivent être réunies pour que de tels codes de conduite soient légitimes et effectifs : ils doivent être élaborés de manière transparente, en associant l'ensemble des parties prenantes, notamment les consommateurs, leurs associations, les organisations de défense des droits de l'homme et les autorités de protection des données ; ils doivent prévoir des mécanismes d'évaluations de leur mise en œuvre. Il pourrait être envisagé que l'autorité de protection des données homologue les codes de conduite professionnels lorsqu'ils sont conformes à ces conditions*. »
[995] Loi Informatique et libertés, Art. 21 (Modifié par l'ordonnance du 12 décembre 2018) « *I. - Lorsque le non-respect des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi entraîne une violation des droits et libertés mentionnés à l'article 1er de la présente loi et que le président de la commission considère qu'il est urgent d'intervenir, il saisit la formation restreinte, qui peut, dans le cadre d'une procédure d'urgence contradictoire définie par décret en Conseil d'État, adopter l'une des mesures suivantes : […] 4° La suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite ; […]*»
[996] Loi Informatique et libertés, Art. 1er (Modifié par la loi du 7 octobre 2016).
[997] RGPD, Cons. 100 « *Afin de favoriser la transparence et le respect du présent règlement, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.* »
[998] Loi Informatique et libertés, Art. 8, § I, 2°, h) « *Elle peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et à la présente loi. Elle prend en considération, à cette fin, les besoins spécifiques des collectivités territoriales, de leurs groupements et des micro- entreprises, petites entreprises et moyennes entreprises. Elle agrée, aux mêmes fins, des organismes certificateurs, sur la base, le cas échéant, de leur accréditation par l'organisme national d'accréditation mentionné au b du 1 de l'article 43 du même règlement ou décide, conjointement avec cet organisme, que ce*

donc à démontrer que l'opération de traitement de données concernée par la certification respecte ledit Règlement[999], attestant ainsi d'une reddition de compte *a contrario*. L'organisme de certification, nommé parfois tiers certificateur, doit démontrer son indépendance et son expertise au regard de l'objet de certification[1000], mettre en place des services et structures pour mener à bien ses missions et objectifs[1001], et justifier de son impartialité[1002]. Pour ce faire, le RGPD prévoit soit l'obtention d'un agrément par l'autorité de contrôle qui établit un référentiel, soit l'obtention d'une accréditation par un organisme national d'accréditation, conformément au règlement européen du 9 juillet 2008[1003] ainsi qu'au référentiel d'accréditation composé des exigences de la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle[1004].

La lecture combinée du RGPD et de la loi Informatique et libertés dévoile deux types de référentiels : le référentiel d'agrément ou d'accréditation employé par la CNIL ou le Comité français de l'accréditation (COFRAC) pour évaluer les organismes de certification, et, le référentiel de certification utilisé par les tiers certificateurs permettant d'évaluer des produits, des services, des procédés, des techniques et même des personnes. La législation prévoit ainsi que la CNIL peut directement certifier des organismes et agréer des organismes de certification ou encore choisir de collaborer avec le COFRAC. Il faut, enfin, noter que la certification est contraignante, et donne lieu à des contrôles réguliers du respect du référentiel et des exigences par les organismes *via* des audits et des examens. Elle est volontaire et accessible grâce à un

---

dernier procède à leur agrément, dans des conditions précisées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. La commission élabore ou approuve les critères des référentiels de certification et d'agrément ; »

[999] RGPD, Art. 42 – Certification « *1. Les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération.* »

[1000] RGPD, Art. 43 – Organismes de certification – 2. « *a) démontré, à la satisfaction de l'autorité de contrôle compétente, leur indépendance et leur expertise au regard de l'objet de la certification;* »

[1001] RGPD, Art. 43 §2. « *b) pris l'engagement de respecter les critères visés à l'article 42, paragraphe 5, et approuvés par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ou par le comité, en vertu de l'article 63 ;*
c) mis en place des procédures en vue de la délivrance, de l'examen périodique et du retrait d'une certification, de labels et de marques en matière de protection des données ;
d) établi des procédures et des structures pour traiter les réclamations relatives aux violations de la certification ou à la manière dont la certification a été ou est appliquée par un responsable du traitement ou un sous-traitant, et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public ; »

[1002] RGPD, Art. 43 §2. « *e) démontré, à la satisfaction de l'autorité de contrôle compétente, que leurs tâches et leurs missions n'entraînent pas de conflit d'intérêts.* »

[1003] Règlement (CE) no 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) no 339/93 du Conseil, JO L 218 du 13.8.2008, p. 30.

[1004] RGPD, Art. 43 §1.

processus transparent et doit être renouvelée[1005]. Comme pour les codes de conduite, la loi Informatique et libertés récemment modifiée envisage la certification dans le cadre des mesures et sanctions prévoyant, d'une part, le « *retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée* », lorsque celui-ci ne respecte pas les obligations résultant du RGPD et de la loi[1006]. Et, d'autre part, elle prévoit la suspension provisoire de la certification délivrée, ou de l'agrément délivré à un organisme, lorsque le non-respect desdites législations entraîne une violation de l'identité humaine, des droits de l'homme, de la vie privée, des libertés individuelles ou publiques[1007].

B. Un système d'autorégulation *a priori*

Une des mises en œuvres concrètes du principe de responsabilisation, l'*accountability*, visé par l'Union repose notamment sur la réalisation d'une analyse d'impact relative à la protection des données (AIPD ou PIA pour *Privacy Impact Assessment*) dans les cas où le traitement envisagé par le responsable du traitement, en particulier « *par le recours à de nouvelles technologies et compte tenu de la nature, de la portée, du contexte et des finalités du traitement* », risque d'engendrer un risque élevé pour les droits et libertés des individus[1008]. La loi Informatique et libertés, uniquement dans le cadre des dispositions applicables aux traitements de données par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données[1009], ainsi que la directive 2016/680 relative à la protection des

[1005] RGPD, Art. 42 et 43, et, CNIL, « La certification et les codes de conduite », 19 décembre 2018 : https://www.cnil.fr/fr/la-certification-et-les-codes-de-conduite

[1006] Loi Informatique et libertés, Art. 20, § III. « *Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou après avoir prononcé à son encontre une ou plusieurs des mesures correctrices prévues au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : [...] 4° Le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;* »

[1007] Loi Informatique et libertés, Art. 21, § I, 3° et 4° ; et Art. 23.

[1008] RGPD, Art. 35 §1 - Analyse d'impact relative à la protection des données.

[1009] Loi Informatique et libertés, Titre III : Dispositions applicables aux traitements relevant de la directive UE 2016/680 du Parlement européen et du Conseil du 27 avril 2016, Art. 90 (Modifié par l'ordonnance du 12 décembre 2018) « *Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 8, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.* »

personnes à l'égard desdits traitements[1010] introduisent, *a pari*, la réalisation d'une analyse d'impact préalablement aux traitements présentant des risques élevés.

Nommée également analyse d'impact sur la vie privée, la notion d'AIPD n'est pas formellement définie en tant que telle par les législations susmentionnées. Néanmoins, le Règlement précise que l'analyse doit tout au moins contenir : une description systématique des opérations de traitement envisagées et des finalités du traitement ; une évaluation de la nécessité et de la proportionnalité des opérations de traitement ; une évaluation des risques pour les droits et libertés des personnes concernées ; et, les mesures de protection envisagées pour, *primo*, faire face aux risques et, *secundo*, apporter la preuve du respect des dispositions légales[1011]. C'est un processus de description et d'évaluation itératif, dont « le responsable du traitement devrait assumer la responsabilité », visant à augmenter le niveau de protection des données et la sécurité des traitements en évaluant, « en particulier, l'origine, la nature, la particularité et la gravité » du risque[1012]. Les codes de conduite approuvés, les certifications labels et marques ainsi que les règles d'entreprises contraignantes en matière de transfert de données doivent être dûment pris en compte lors des évaluations démontrant que des mesures ou garanties appropriées ont été choisies ou mises en place[1013]. Il s'avère que l'AIPD représente un outil majeur comportant une double utilité : l'analyse en soi permet au responsable du traitement de respecter les exigences légales, mais elle sert aussi à démontrer que le traitement respecte le Règlement et que des mesures efficaces ont été prises afin d'assurer la conformité au Règlement, en tenant compte, notamment, des risques pour les droits et libertés[1014]. Autrement dit, « *une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve* »[1015].

[1010] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, Art. 27 Analyse d'impact relative à la protection des données « *1. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* »

[1011] RGPD, Cons. 84 et 90, Art. 35 §7.

[1012] RGPD, Cons. 84.

[1013] *Cf.* p. 232 et s., 271 et s.

[1014] RGPD, Cons. 84 et 90, Art. 24, §1.

[1015] Groupe de travail « Article 29 », « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 », 4 avril 2017 (modifiées et adoptées en dernier lieu le 4 octobre 2017), 17/FR WP 248 rév. 01, p. 4.

Aux termes du RGPD, une AIPD caractérise une véritable évaluation de risques, ayant pour objectif une aide à la gestion des risques pour les droits et libertés des personnes[1016]. Le RGPD mentionne ainsi certains éléments qui recouvrent des composantes bien connues de la gestion de risque, notamment de la norme ISO 31000[1017]. De ce fait, une analyse d'impact permet de gérer le risque en établissant un contexte, « compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque », en appréciant le risque, « en vue d'évaluer la probabilité et la gravité particulières du risque élevé », et, en traitant le risque, « pour atténuer ce risque, assurer la protection des données à caractère personnel et démontrer le respect du présent règlement »[1018]. Le G29 encourage de ce fait le développement de « cadres sectoriels » pour les AIPD qui, dans la mesure où ils se fondent sur des connaissances spécifiques au secteur donné, permettent à l'analyse de prendre en compte les spécificités d'un type particulier de traitement[1019]. La CNIL a, en ce sens, fournit des « Guides PIA » décrivant la méthode et la démarche à suivre[1020], les modèles utiles pour formaliser l'étude[1021] et les bases de connaissances utiles[1022] ; puis, elle a appliqué ces guides aux objets connectés[1023], et a entrepris une étude de cas[1024]. Ceci dit, selon la Commission, quelle que soit la méthode choisie pour mener une analyse d'impact, celle-ci « doit permettre de

[1016] RGPD, Cons. 90 « *Dans de tels cas, une analyse d'impact relative à la protection des données devrait être effectuée par le responsable du traitement, préalablement au traitement, en vue d'évaluer la probabilité et la gravité particulières du risque élevé, compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque. Cette analyse d'impact devrait comprendre, notamment, les mesures, garanties et mécanismes envisagés pour atténuer ce risque, assurer la protection des données à caractère personnel et démontrer le respect du présent règlement.* » ; voir aussi, G29, « Lignes directrices sur l'AIPD », *Id.,* p. 20 ainsi que les Guides PIA de la CNIL qui sont « *des catalogues de bonnes pratiques destinées à traiter les risques que les traitements de données personnelles peuvent faire peser sur les libertés et la vie privée des personnes concernées* » : https://www.cnil.fr/fr/PIA-privacy-impact-assessment

[1017] ISO 31000 :2018 Management du risque – Lignes directrices, Art. 3 - Termes et définitions - ainsi que la table des matières de l'Art. 6 - Processus - dans l'aperçu de la norme : communication et consultation, périmètre d'application - contexte, appréciation du risque, traitement du risque, suivi, évaluation et enregistrement » : https://www.iso.org/obp/ui/fr/#iso:std:iso:31000:ed-2:v1:fr ; Voir également, G29, « Lignes directrices sur l'AIPD », *Id.,* p. 20.

[1018] RGPD, Cons. 90.

[1019] G29, « Lignes directrices sur l'AIPD », *Id.,* p. 21.

[1020] CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – La méthode », édition février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf

[1021] CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Les modèles », édition février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf

[1022] CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Les bases de connaissances », édition février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf

[1023] CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Application aux objets connectés », édition février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-fr.pdf

[1024] CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Étude de cas « CAPTOO » », édition février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-captoo-fr.pdf

satisfaire »[1025] aux critères d'acceptabilité dégagés par le G29 et son successeur, le Comité Européen de la Protection des Données (CEPD ou EDPB pour *European Data Protection Board*)[1026], dans leurs lignes directrices[1027].

En pratique, l'AIPD doit être effectuée préalablement au lancement du traitement présentant un risque élevé[1028], ce qui s'articule de manière cohérente avec les principes de protection des données dès la conception et par défaut, prévus également par le Règlement dans le contexte des obligations générales du responsable du traitement de gérer de manière appropriée les risques[1029]. L'analyse d'impact sur la vie privée peut, donc, être envisagée comme un « outil d'aide à la prise de décisions »[1030] en matière de traitement de données. Elle doit être mise en œuvre le plus tôt possible, revue de manière régulière et mise à jour, « en tout état de cause tous les trois ans », afin d'examiner et de s'assurer que le niveau de risque reste acceptable[1031]. Dans cette perspective, la réalisation d'une AIPD correspond à un processus continu et itératif. Par ailleurs, le RGPD prévoit qu' « *une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires* »[1032] manifestant des risques élevés similaires, « *en termes de nature, périmètre, contexte, finalité et risques présentés pour les droits et libertés des personnes concernées* »[1033]. En ce sens, une seule et même AIPD peut être employée pour évaluer plusieurs traitements analogues, puisqu'une nouvelle analyse serait inutile et économiquement déraisonnable pour les cas déjà étudiés et analysés[1034].

[1025] CNIL, Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD), JORF n° 0256 du 6 novembre 2018, texte n° 81, Art. 2 – Conditions de réalisation d'une AIPD.

[1026] Institué par le RGPD à la section 3 – Comité européen de la protection des données – du Chapitre VII (Art. 68 à 76), il a vocation à prendre la suite du groupe de travail « article 29 » qui était l'enceinte informelle d'échanges et d'élaboration de doctrine commune mise en place par l'ancienne directive 95/46/CE. Ses missions sont listées à l'art. 70 du règlement, et ses modalités de travail sont détaillées dans le cadre des « *EDPB Rules of procedure* » adoptées le 25 mai 2018 :
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop_adopted_en.pdf

[1027] G29, « Lignes directrices sur l'AIPD », *Id.,* Annexe 2 – Critères d'acceptabilité d'une AIPD, p. 26-27.

[1028] RGPD, Cons. 90 et 93, et Art. 35 §§ 1 et 10 ; Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, *Id.,* Art. 27 ; CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Id.,* Art. 2.

[1029] RGPD, Cons. 78 et Section I – Obligations générales – Art. 24 (Responsabilité du responsable du traitement) et 25 (Protection des données dès la conception et protection des données par défaut).

[1030] G29, « Lignes directrices sur l'AIPD », *Id.,* p. 17.

[1031] RGPD, Art. 35 §§ 1 et 11 ; CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Id.,* Art. 2.

[1032] RGPD, Art. 35 § 1.

[1033] CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Ibid.,* Art. 2.

[1034] RGPD, Cons. 92 *« Il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.* »

La responsabilité de mettre en œuvre une analyse d'impact incombe au responsable du traitement concerné, et, dans les cas où elle est réalisée par un tiers, elle doit être menée sous son autorité puisqu'il reste seul responsable du respect de cette obligation[1035]. Celui-ci doit aussi demander conseil auprès du délégué à la protection des données (DPD – DPO pour *Data Protection Officers*), « si un tel délégué a été désigné »[1036], ce dernier ayant également, selon le RGPD, pour mission de vérifier l'exécution de l'analyse d'impact[1037]. L'exécution d'une AIPD doit, en outre, impliquer tous les acteurs du traitement envisagé. Par conséquent, le Règlement ainsi que les lignes directrices de la CNIL sur les AIPD citent quelques acteurs de manière non exhaustive. C'est le cas du DPO mais aussi, selon la CNIL, du responsable de la sécurité des systèmes d'information (RSSI), cité également par le G29[1038]. C'est le cas aussi du sous-traitant qui, dans la mesure où il opère partiellement ou entièrement le traitement, est tenu d'aider le responsable du traitement à effectuer l'analyse, et coopérer en lui fournissant toutes les informations nécessaires[1039]. En outre, le responsable du traitement demande, « le cas échéant », l'avis des personnes concernées ou de leurs représentants au sujet du traitement considéré, « dont la consultation peut, dans certains cas, être pertinente pour évaluer les risques », sous réserve de la protection des « intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement »[1040]. Le G29 a apporté quelques précisions en ce qui concerne cette dernière disposition, et considère que ces avis peuvent être recueillis « par divers moyens, selon le contexte », en soulignant toutefois que « *demander le consentement au traitement n'est évidemment pas un moyen de recueillir l'avis des personnes concernées* »[1041].

Enfin, toutes les législations et les lignes directrices en la matière recommandent de documenter les apports, avis et conseils des acteurs sollicités, y compris, le choix, à l'inverse, de ne pas en solliciter un en particulier, ainsi que les décisions prises par le responsable du traitement ; une documentation servant, *in fine*, à rendre des comptes. Et la CNIL estime, à

[1035] RGPD, Art. 35 § 2 ; CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Ibid.,* Art. 2.
[1036] RGPD, Art. 35 § 2.
[1037] RGPD, Art. 39 §1 « *c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 ;* »
[1038] G29, « Lignes directrices sur l'AIPD », *Id.,* p. 18, qui précise qu' « il est de bonne pratique de définir et de documenter les autres rôles et responsabilités spécifiques, en fonction de la politique interne et des processus et règles en jeu. »
[1039] RGPD, Art. 28 §3 « *f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;* »
[1040] RGPD, Art. 35 §9, et CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Id.,* Art. 2.
[1041] G29, « Lignes directrices sur l'AIPD », *Id.,* p. 17-18, et le groupe relève aussi que « *le responsable du traitement doit également justifier toute décision de ne pas recueillir l'avis des personnes concernées s'il juge la démarche inappropriée, en estimant par exemple que cela compromettrait la confidentialité de plans d'affaires ou serait disproportionné ou irréalisable.* »

cet égard, qu'un responsable de traitement ayant effectué une analyse peut « *utilement produire un rapport ou un résumé ayant vocation à être publié afin de créer un climat de confiance et de transparence entre les parties concernées par un traitement* »[1042]. En vertu des dispositions du Règlement, le fait de ne pas entreprendre une AIPD alors que le traitement y est soumis[1043], ou de réaliser l'analyse d'impact de façon incorrecte[1044], ou encore de ne pas consulter l'autorité de contrôle quand la situation l'exige[1045] est passible de sanctions administratives. Une AIPD doit donc être obligatoirement effectuée lorsque le traitement considéré est « susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques » conformément à l'approche fondée sur le risque préconisée par le RGPD, et dans la mesure où « il convient de déterminer la probabilité et la gravité du risque » pour ces droits et libertés en fonction de la nature, de la portée, du contexte et des finalités du traitement[1046].

Le Règlement ne fournit pas de définition propre à la notion de risque et ce, selon certains auteurs, afin de « *préserver la neutralité technologique du texte et une souplesse dans la mise en œuvre* »[1047]. Néanmoins, plusieurs exemples et références à des opérations de traitement « susceptibles d'engendrer un risque élevé » ont été mentionné dans différentes dispositions du RGPD. Celui-ci cite « en particulier » trois cas où la réalisation d'une AIPD est requise mais cette liste n'est pas exhaustive. Le G29 a proposé une définition de la notion de « risque » et de celle de « gestion du risque »[1048], et a fourni neuf critères permettant d'évaluer concrètement si un traitement nécessite une analyse d'impact en raison d'un risque élevé ; critères repris par le CEPD et la CNIL dans ses lignes directrices en matière d'AIPD précitées. Il a, par ailleurs, rappelé sa déclaration sur le rôle d'une approche fondée sur les risques dans les cadres juridiques de protection des données, où le groupe indiquait que la portée des « droits et libertés » visés est large, comprenant essentiellement le droit à la protection des données et le droit à la vie privée, mais pouvant aussi impliquer, le cas échéant, d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation,

[1042] CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Ibid.,* Art. 2.
[1043] RGPD, Art. 35 §§ 1, 3 et 4.
[1044] RGPD, Art. 35 §§ 2 et 7 à 9.
[1045] RGPD, Art. 36 § 3 e).
[1046] RGPD, Cons. 76.
[1047] E. BRUNET, « Règlement général sur la protection des données à caractère personnel – genèse de la réforme et présentation globale », Dalloz IP/IT 2016, p. 567.
[1048] G29, « Lignes directrices sur l'AIPD », *Ibid.,* p. 7 : « *Un «risque» est un scénario qui décrit un évènement et ses effets, estimés en termes de gravité et de probabilité. La «gestion du risque» peut, quant à elle, se définir comme un ensemble d'activités coordonnées dans le but de diriger et de piloter un organisme vis-à-vis du risque.* »

l'interdiction de toute discrimination, le droit à la liberté ou à la liberté de conscience et de religion[1049].

Il en découle que la réalisation d'une AIPD n'est pas obligatoire pour toute opération de traitement qui pourrait générer un risque pour les droits et libertés des personnes. Elle n'est exigée par les dispositions légales que lorsque le type de traitement est susceptible d'engendrer un « risque élevé », en particulier en cas de « recours à de nouvelles technologies »[1050]. Le risque, selon le législateur européen, « *devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé* »[1051]. Le RGPD cite trois cas en particulier où il est requis d'effectuer une AIPD, mais fournit également d'autres références de traitements « susceptibles d'engendrer un risque élevé » dans plusieurs de ses dispositions. Une lecture combinée de ces dernières, complétée par les critères fournis par le G29[1052] et les lignes directrices de la CNIL[1053] font ressortir plusieurs éléments, facteurs et catégories permettant d'évaluer et de déterminer si le type de traitement envisagé est susceptible d'entraîner un risque élevé pour les droits et libertés et requière, à ce titre, une AIPD.

L' « évaluation systématique et approfondie d'aspects personnels »[1054] ou notation, *scoring*, y compris les techniques de profilages et de prédiction, portant sur « *les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements* »[1055], représente le premier cas spécifiquement mentionné par le texte du RGPD. Celui-ci comprend aussi la prise de décisions automatisées « *produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative de façon similaire* »[1056], critérium ayant fait l'objet d'explications complémentaires dans les lignes

[1049] Groupe de travail « Article 29 », "Statement on the role of a risk-based approach in data protection legal frameworks", WP218, du 30 mai 2014, p. 4: " *8/ In the context referred to above, the scope of "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.*"
[1050] RGPD, Art. 35 §1, illustré et complété par les §§ 3 et 4 ainsi que les Cons. 89, 90 et 91.
[1051] RGPD, Cons. 76.
[1052] G29, « Lignes directrices sur l'AIPD », *Id.,* p. 9 à 13.
[1053] CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Id.,* Art. 1.1.
[1054] RGPD, Art. 35 §3, point a).
[1055] RGPD, Cons. 71.
[1056] RGPD, Art. 35 §3, point a).

directrices du G29 relatives au profilage[1057] afin de définir les expressions « effets juridiques » et « de manière significative de façon similaire », absentes du RGPD. Selon le groupe de travail, un effet juridique implique que la décision prise, fondée exclusivement sur un traitement automatisé, « affecte les droits juridiques d'une personne », tels que la liberté de s'associer, de voter ou d'intenter une action en justice, ou affecte « le statut juridique d'une personne ou ses droits en vertu d'un contrat »[1058]. Un traitement peut également produire des effets équivalents sur les personnes ou les affecter « de manière significative » et, rajoute les rédacteurs du RGPD à l'instar de ceux de l'ancienne directive sur la protection des données[1059], « de façon similaire », sous-entendant, par conséquent, que le niveau d'importance des effets produits par la décision doit être « *similaire à celui d'une décision produisant un effet juridique* »[1060]. Et le législateur européen en fournit des exemples pratiques dans les dispositions du RGPD, comme « *le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine* »[1061], ou, précise-t-il, lorsque le traitement peut donner lieu « *à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important [...]* »[1062].

La « surveillance systématique d'une zone accessible au public »[1063], correspondant au deuxième cas cité expressément par le RGPD, implique un traitement automatisé pour observer, surveiller ou contrôler des personnes incluant la collecte de données *via* des réseaux ou *via* une zone accessible au public. Cet élément suppose donc un « suivi régulier et systématique »[1064], terme mentionné mais non défini par le Règlement qui fournit uniquement des précisions sur la notion particulière de « suivi du comportement », en soulignant que pour déterminer si une

---

[1057] G29, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, Adoptées le 3 octobre 2017 - Version révisée et adoptée le 6 février 2018, WP251rev.01.

[1058] G29, Lignes directrices relatives au profilage du 6 février 2018, *Id.,* p. 23 ; et le groupe de travail donne des exemples de ce type d'effet en soulignant qu' « *il convient de mentionner les décisions automatisées au sujet d'une personne qui se traduisent par : l'annulation d'un contrat ; le droit ou le refus d'un avantage social particulier accordé par la loi, comme l'allocation familiale ou l'allocation de logement ; le refus d'admission dans un pays ou le refus de citoyenneté.* »

[1059] Directive 95/46/CE relative à la protection des données, Art. 15 - Décisions individuelles automatisées « *1. [...] décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.* »

[1060] G29, Lignes directrices relatives au profilage du 6 février 2018, *Id.,* p. 24.

[1061] RGPD, Cons. 71.

[1062] RGPD, Cons. 75.

[1063] RGPD, Art. 35 §3, point c).

[1064] RGPD, Cons. 97 ou Art. 37 §1, point b), par ex.

activité de traitement peut être considérée comme un suivi du comportement des personnes, il y a lieu d'établir si celles-ci sont suivies sur internet, « *ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit* »[1065]. Dans ses lignes directrices concernant les DPD, le G29 interprète les termes « régulier » et « systématique » comme recouvrant, pour le premier, une ou plusieurs des significations suivantes : « *continu ou se produisant à intervalles réguliers au cours d'une période donnée ; récurrent ou se répétant à des moments fixes ; ayant lieu de manière constante ou périodique* »[1066], et, pour le second, une ou plusieurs des suivantes : *« se produisant conformément à un système ; préétabli, organisé ou méthodique ; ayant lieu dans le cadre d'un programme général de collecte de données ; effectué dans le cadre d'une stratégie* »[1067]. Quant à la surveillance de « zones accessibles au public », le RGPD note simplement « en particulier lorsque des dispositifs optoélectroniques sont utilisés »[1068] sans fournir de définition quant aux périmètres d'une zone accessible au public. Selon le G29, s'entend comme une zone accessible au public « *tout lieu, quel qu'il soit, ouvert à tout un chacun, tel qu'une place, un centre commercial, une rue, un marché, une gare ou encore une bibliothèque publique, par exemple* »[1069].

Les « données traitées à grande échelle »[1070], correspondant au dernier cas mentionné par les rédacteurs du Règlement, se réfère à une activité de traitement portant sur un « volume important de données » et touchant « un nombre important de personne »[1071]. Le Règlement ne définit pas la notion de traitement à « grande échelle », mais apporte quelques orientations en soulignant que doivent être incluses dans celle-ci les opérations de traitement « *qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé* »[1072]. Quant au G29, il recommande, en tout état

[1065] RGPD, Cons. 24.
[1066] G29, Lignes directrices concernant les délégués à la protection des données (DPD), Adoptées le 13 décembre 2016 - Version révisée et adoptée le 5 avril 2017, 16/FR WP 243 rev.01, p. 10.
[1067] G29, Lignes directrices relatives aux DPD, du 5 avril 2017, *Id.*, p. 10-11.
[1068] RGPD, Cons. 91.
[1069] G29, Lignes directrices sur l'AIPD, *Id.,* p. 11.
[1070] RGPD, Art. 35 §3, points b) et c).
[1071] RGPD, Cons. 75.
[1072] RGPD, Cons. 91, et le législateur souligne « *par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ainsi qu'à d'autres opérations de traitement qui engendrent un risque élevé pour les droits et libertés des personnes concernées* ». Il précise par ailleurs que « *le traitement de données à caractère personnel ne devrait*

de cause, que les facteurs suivants soient particulièrement pris en considération pour mesurer si le traitement est effectué à grande échelle : « *le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée ; le volume de données et/ou le spectre des données traitées ; la durée, ou la permanence, des activités de traitement des données ; l'étendue géographique de l'activité de traitement* »[1073].

Les « données sensibles » ou les « données à caractère hautement personnel », représentent, par ailleurs, des catégories particulières de données, visées aux articles 9 et 10 du RGPD[1074], incluses dans le cas du « traitement à grande échelle » nécessitant obligatoirement une analyse d'impact, ainsi que prévu par ledit texte. Celui-ci ainsi que les lignes directrices de la CNIL précisent la notion de « données sensibles » qui comprend l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques ou de santé, les données biométriques, les données concernant la vie ou l'orientation sexuelle, les données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes[1075]. Ces dispositions apportent, également, des indications quant à l'expression « données à caractère hautement personnel » qui suppose les données relatives à des communications électroniques, les données de localisation, ou encore les données financières[1076] ; en d'autres termes, « *lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels* »[1077].

De même, une AIPD est requise dans le cas des « données concernant des personnes vulnérables », élément mentionné par le législateur européen et la CNIL en citant, essentiellement, les enfants, les patients ou les personnes âgées[1078]. C'est aussi le cas en ce qui concerne le « croisement ou la combinaison de données », critère nécessaire dans la mesure où le RGPD définit le terme de « traitement » comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que [...] le rapprochement ou*

pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. »

[1073] G29, Lignes directrices relatives aux DPD, du 5 avril 2017, *Id.*, p. 9.
[1074] RGPD, Art. 35 §3, point b).
[1075] RGPD, Cons. 75, Art. 9 §1 et Art. 10 ; CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Id.,* Art. 1.1.
[1076] CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Id.,* Art. 1.1.
[1077] RGPD, Cons. 75.
[1078] RGPD, Cons. 75 ; CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Ibid.,* Art. 1.1.

l'interconnexion ». En effet, de telles interconnexions et combinaisons pourraient dépasser les attentes raisonnables des personnes concernées dans le cas d'un traitement effectué à des fins différentes et/ou par différents responsables du traitement par exemple[1079]. *Idem* pour le « traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat » puisque ces opérations empêchent en elles-mêmes les personnes « d'exercer un droit ou de bénéficier d'un service ou d'un contrat »[1080]. Ce type de traitement est susceptible d'engendrer un risque élevé « *lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leur données [...]* »[1081]. Ces traitements comprennent notamment, selon le G29, les activités « *visant à autoriser, modifier ou refuser l'accès à un service ou la conclusion d'un contrat* »[1082].

L' « utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles »[1083] représente un critère qui ressort clairement des dispositions du RGPD, puisque le recours à de nouvelles technologies, entendues « en conformité avec l'état des connaissances technologiques »[1084], peut générer un risque élevé pour les droits et libertés et nécessite donc une AIPD « *dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication et des pratiques commerciales* »[1085]. Le Règlement insère, par ailleurs, le suivi des évolutions pertinentes, notamment dans le domaine précité, dans le cadre des missions de l'autorité de contrôle compétente[1086]. En effet, indique le G29, « *les conséquences personnelles et sociales du déploiement d'une nouvelle technologie peuvent être inconnues, et une AIPD aidera le responsable du traitement à comprendre et à traiter de tels risques* », et cite les applications de l'Internet des objets en guise d'exemple de traitement nécessitant une analyse d'impact[1087].

De nombreux exemples sont enfin fournis par les lignes directrices du G29 et de la CNIL, y compris des exemples de cadres référentiels existants pour la réalisation d'une AIPD[1088],

---

[1079] G29, Opinion 03/2013 on purpose limitation (Avis relatif à la limitation des finalités), Adopté le 2 avril 2013, 13/EN WP 203, p. 24-25: "*b) the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use*"
[1080] RGPD, Cons. 91 et Art. 22 §§ 1 et 2.
[1081] RGPD, Cons. 75.
[1082] G29, Lignes directrices sur l'AIPD, *Id.,* p. 12.
[1083] RGPD, Cons. 89 et 91, et Art. 35 §1.
[1084] RGPD, Cons. 91.
[1085] RGPD, Art. 57 §1, point i).
[1086] RGPD, Art. 57 - Missions.
[1087] G29, Lignes directrices sur l'AIPD, *Id.,* p. 12.
[1088] Par ex., G29, Lignes directrices sur l'AIPD, Annexe 1 — Exemples de cadres européens existants pour la réalisation d'une AIPD, *Ibid.,* p. 24-25.

particulièrement en ce qui concerne des types de traitements pour lesquels il est requis d'entreprendre une AIPD[1089]. Celle-ci, comme il a été vu, présente plusieurs utilités : elle permet en soi de respecter une obligation, elle permet d'identifier les mesures et garanties techniques et organisationnelles nécessaires à mettre en place menant, *in fine*, à un respect de toutes les dispositions légales combinées, et sert à démontrer le respect des exigences légales. Les AIPD sont donc « *avant tout l'occasion de mener une réflexion interne, spécifique à chaque traitement, de nature à garantir de manière opérationnelle le respect des principes relatifs à la protection des données et de pouvoir, le cas échéant, le démontrer* »[1090].

Les mesures et les garanties visées sont nombreuses, tel qu'il a été constaté, allant de la désignation d'un DPD, à la consultation préalable de l'autorité compétente, à l'obligation de sécurité du traitement ou de protection des données dès la conception ou par défaut. Il est important de noter que le simple fait que les critères ou les conditions, suscitant l'obligation d'effectuer une AIPD, ne soient pas remplis ne restreint aucunement l'obligation générale à la charge des responsables du traitement de mettre en œuvre des mesures et garanties appropriées permettant de gérer les risques pour les droits et libertés des personnes. Concrètement, « *cela signifie que les responsables du traitement sont tenus d'évaluer de manière continue les risques créés par leurs activités de traitement dans le but d'identifier quand un type de traitement est susceptible d'engendrer un risque élevé* »[1091].

§2. Un régime de responsabilité à connotation répressive : approche fondée sur un double système de sanctions

Ce régime de responsabilité à connotation répressive se décline principalement en un système de réparation d'initiative individuelle (A), d'une part, et, d'autre part, en un système de sanction d'initiative institutionnelle (B), en vue d'assurer et d'imposer la protection des données et des personnes et la réparation des atteintes subies.

[1089] Par ex., CNIL, Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, JORF n° 0256 du 6 novembre 2018, texte n° 82.
[1090] CNIL, Délibération n° 2018-326 du 11 octobre 2018, *Id.,* Propos liminaires.
[1091] G29, Lignes directrices sur l'AIPD, *Ibid.,* p. 7.

A. Un système de réparation d'initiative individuelle

Le RGPD, à l'image de la directive 95/46/CE, conçoit un système de responsabilité ouvrant droit à des voies de recours et à des réparations au bénéfice des individus. Aux termes du Règlement, toute personne, qui estime que ses droits et libertés ont été violés, devrait avoir le droit d'introduire une réclamation auprès d'une autorité de contrôle et de disposer d'un droit à un recours juridictionnel effectif conformément à l'article 47 de la Charte[1092], sans préjudice de tout autre recours administratif ou juridictionnel[1093]. C'est une composante des droits de la personne concernée par une violation de données par une activité de traitement, prévue par le RGPD et qui est d'initiative individuelle.

Dans cette perspective, tout individu a le droit d'introduire une réclamation auprès d'une autorité de contrôle ainsi que le droit à un recours juridictionnel effectif contre une autorité de contrôle, sans préjudice de toute autre voie de recours possible. Par conséquent, si une personne considère qu'un traitement de données personnelles la concernant constitue une violation des dispositions du Règlement, elle a le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente, en l'occurrence la CNIL en France, ou de mandater « un organisme, une organisation ou une association à but non lucratif » pour l'introduire[1094]. L'autorité de contrôle en question « *informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 78* »[1095]. Ce dernier dispose que toute personne « physique ou morale » a le droit à un recours juridictionnel effectif contre une autorité de contrôle et sans préjudice de toute autre recours administratif ou extrajudiciaire[1096].

Dès lors, une personne physique ou morale peut former un recours devant la juridiction nationale compétente contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne et qui produit des effets juridiques à son égard ; et le Règlement précise qu' « *une telle décision concerne en particulier l'exercice, par l'autorité de contrôle, de pouvoirs d'enquête, d'adoption de mesures correctrices et d'autorisation ou le refus ou le*

[1092] Charte des droits fondamentaux, Art. 47 - Droit à un recours effectif et à accéder à un tribunal impartial « *Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article.*
Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter. »
[1093] RGPD, Cons. 141 et Art. 77 – Droit d'introduire une réclamation auprès d'une autorité de contrôle.
[1094] RGPD, Cons. 142 et Art. 80 – Représentation des personnes concernées.
[1095] RGPD, Art. 77.
[1096] RGPD, Art. 78 – Droit à un recours juridictionnel effectif contre une autorité de contrôle.

rejet de réclamations »[1097]. De plus, le RGPD prévoit la possibilité pour une personne physique ou morale de former un recours en annulation des décisions du Comité devant la Cour de justice[1098] dans les conditions prévues à l'article 263 du traité sur le fonctionnement de l'Union européenne[1099].

En outre, toute personne concernée a le droit d'intenter une action devant les juridictions nationales lorsque l'autorité de contrôle compétente ne traite pas une réclamation ou ne l'informe pas, « dans un délai de trois mois », de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite[1100]. Et dans le cas où une réclamation a été rejetée ou refusée par une autorité de contrôle, la personne concernée peut également exercer son droit à un recours juridictionnel effectif à son encontre[1101].

La loi Informatique et libertés, dans sa dernière version, prévoit le droit pour une personne concernée d'introduire une réclamation auprès de la CNIL, désignée simultanément autorité de contrôle concernée et autorité de contrôle chef de file[1102], notamment « *en cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande* »[1103]. La loi précise, par ailleurs, que dans la mesure où, saisie d'une réclamation dirigée contre un responsable de traitement ou son sous-traitant, la CNIL estime fondés les griefs avancés concernant la protection des droits et libertés d'une personne à l'égard de ses données ou, en vue d'assurer, de manière générale, la protection desdits droits dans le cadre de sa mission, elle peut « *demander au Conseil d'État d'ordonner la suspension d'un transfert de données, le cas échéant sous astreinte* », et doit alors assortir ses conclusions d'une demande de question préjudicielle à la CJUE « *en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE)*

[1097] RGPD, Cons. 143.
[1098] RGPD, Cons. 143.
[1099] TFUE (Version consolidée), JO n° C 326 du 26/10/2012, Art. 263 « *La Cour de justice de l'Union européenne contrôle la légalité des actes législatifs, des actes du Conseil, de la Commission et de la Banque centrale européenne, autres que les recommandations et les avis, et des actes du Parlement européen et du Conseil européen destinés à produire des effets juridiques à l'égard des tiers. Elle contrôle aussi la légalité des actes des organes ou organismes de l'Union destinés à produire des effets juridiques à l'égard des tiers. À cet effet, la Cour est compétente pour se prononcer sur les recours pour incompétence, violation des formes substantielles, violation des traités ou de toute règle de droit relative à leur application, ou détournement de pouvoir, formés par un État membre, le Parlement européen, le Conseil ou la Commission. [...]. Toute personne physique ou morale peut former, dans les conditions prévues aux premier et deuxième alinéas, un recours contre les actes dont elle est le destinataire ou qui la concernent directement et individuellement, ainsi que contre les actes réglementaires qui la concernent directement et qui ne comportent pas de mesures d'exécution* »
[1100] RGPD, Art. 78 §2.
[1101] RGPD, Cons. 143 et Art. 77 et 78.
[1102] Loi Informatique et libertés, Art. 24, Art. 25 ou Art. 27 par ex.
[1103] Loi Informatique et libertés, Art. 51, § II, al. 2.

2016/679 du 27 avril 2016 ainsi que de tous les actes pris par la Commission européenne relativement aux garanties appropriées dans le cadre des transferts de données »[1104]. Et, rajoute la loi, si le transfert de données en cause ne constitue pas un traitement effectué devant une juridiction dans l'exercice de sa fonction juridictionnelle, la CNIL peut saisir le Conseil d'État dans les mêmes conditions « *aux fins d'ordonner soit la suspension du transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, soit la prolongation de la suspension de ce transfert qu'elle aurait elle-même déjà ordonnée* », dans l'attente de l'appréciation par la Cour de la validité de la décision en cause[1105].

À côté des recours devant l'autorité compétente et à l'encontre de celle-ci, et sans préjudice de tout autre recours administratif ou extrajudiciaire qui lui est ouvert, le Règlement stipule que « *chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement* »[1106]. Par conséquent, et là réside l'innovation introduite par le RGPD en matière de responsabilité et de réparation, toute personne concernée peut intenter une action en justice contre le responsable du traitement ou contre le sous-traitant ; l'ancienne directive ne prévoyant que la responsabilité du responsable du traitement[1107].

De même que pour l'introduction d'une réclamation, toute personne qui estime que les droits que lui confèrent le Règlement sont violés par une opération de traitement a le droit d'intenter une action contre le responsable du traitement ou le sous-traitant s'il a effectué le traitement incriminé. Elle a aussi le droit de mandater les mêmes entités, à savoir « un organisme, une organisation ou une association à but non lucratif », valablement constituées, actives dans le domaine de la protection des droits et libertés des personnes et dont les objectifs statutaires sont d'intérêt public, pour exercer, en son nom, les mêmes voies de recours qui lui sont ouvertes ainsi que le droit d'obtenir réparation[1108]. S'observe donc « *une forme de délégation offerte à la société civile, l'invitant à s'organiser pour assurer avec les États et les*

[1104] Loi Informatique et libertés, Art. 39, al. 1 (Modifié par l'ordonnance du 12 décembre 2018).
[1105] Loi Informatique et libertés, Art. 39, al. 2.
[1106] RGPD, Art. 79 – Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant.
[1107] Directive 95/46/CE, Art. 23 – Responsabilité « *1. Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi.* »
[1108] RGPD, Cons. 142 et Art. 80 §1.

organismes de contrôle paraétatique la pleine exécution des normes règlementaires »[1109]. La loi Informatique et libertés ouvre également la possibilité pour la personne concernée de mandater « une association ou une organisation mentionnée au IV de l'article 37 »[1110] aux fins d'exercer, en son nom, les droits à un recours prévus par le Règlement, ou d'agir devant la CNIL, contre celle-ci ou contre le responsable de traitement ou son sous-traitant devant une juridiction, lorsqu'est en cause un traitement relevant du Titre III[1111] de la présente loi[1112].

À ce titre, ces voies de recours d'initiative individuelle ouvrent le droit à réparation de « tout dommage qu'une personne peut subir du fait d'un traitement » opéré en violation des dispositions légales[1113]. Le législateur européen proclame, en effet, que « *toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi* »[1114]. Il détermine l'étendue de la responsabilité des acteurs ayant causé un dommage par le traitement qui constitue une violation des dispositions règlementaires. Ainsi, « tout responsable du traitement » ayant participé au traitement illégal est, de manière conjointe et solidaire, responsable du dommage matériel ou moral causé par celui-ci[1115]. Et, précise-t-il, « *lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement* »[1116]. Ces derniers doivent alors définir de manière transparente, et par voie d'accord entre eux, leurs obligations respectives en vue d'assurer le respect des exigences du Règlement.

[1109] A. BASDEVANT, J.-P. MIGNARD, *L'empire des données*, *op. cit.*, p. 170.
[1110] Loi Informatique et libertés, Art. 37 § IV « *Peuvent seules exercer cette action :*
1° Les associations régulièrement déclarées depuis cinq ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel ;
2° Les associations de défense des consommateurs représentatives au niveau national et agréées en application de l'article L. 811-1 du code de la consommation, lorsque le traitement de données à caractère personnel affecte des consommateurs ;
3° Les organisations syndicales de salariés ou de fonctionnaires représentatives au sens des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du code du travail ou du III de l'article 8 bis de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ou les syndicats représentatifs de magistrats de l'ordre judiciaire, lorsque le traitement affecte les intérêts des personnes que les statuts de ces organisations les chargent de défendre. »
[1111] Loi Informatique et libertés, Titre III - Dispositions applicables aux traitements relevant de la directive UE 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/ JAI du Conseil
[1112] Loi Informatique et libertés, Art. 38 (Modifié par l'ordonnance du 12 décembre 2018).
[1113] RGPD, Cons. 146.
[1114] RGPD, Art. 82 §1 – Droit à réparation et responsabilité.
[1115] RGPD, Art. 82 §2.
[1116] RGPD, Art. 26 §1 – Responsables conjoints du traitement.

En effet, celui-ci indique que, par principe, « *la protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et des sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par celles-ci, exige une répartition claire des responsabilités au titre du présent règlement, y compris lorsque le responsable du traitement détermine les finalités et les moyens du traitement conjointement avec d'autres responsables du traitement, ou lorsqu'une opération de traitement est effectuée pour le compte d'un responsable du traitement* »[1117]. L'accord défini par les responsables conjoints ne prive pas pour autant la personne concernée de la possibilité d'exercer ses droits « à l'égard de et contre chacun des responsables du traitement »[1118]. De même, en cas de désignation d'un représentant par le responsable du traitement ou le sous-traitant, le Règlement stipule que cette désignation est « *sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement ou le sous-traitant lui-même* »[1119].

Toutefois, le RGPD, en précisant la responsabilité particulière des sous-traitants, révèle le caractère subsidiaire de celle-ci comparée à l'obligation principale des responsables du traitement. Un sous-traitant n'est tenu pour responsable que s'il n'a pas respecté les obligations légales règlementaires « qui incombent spécifiquement aux sous-traitants », ou s'il a agi « en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci »[1120]. Et, une exonération de responsabilité est également prévue lorsqu'un responsable du traitement ou un sous-traitant prouve que ce qui a causé le dommage ne lui est nullement imputable[1121].

Le Règlement indique, par ailleurs, que dans le cas où plusieurs acteurs sont responsables d'un dommage provoqué par le traitement, « *chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective* »[1122], soulignant ainsi leur responsabilité solidaire. Il est important de relever que le législateur a, en quelque sorte, fournit des indications quant à la notion de dommage, qui doit être interprétée largement « à la lumière

[1117] RGPD, Cons. 79.
[1118] RGPD, Art. 26 §3.
[1119] RGPD, Art. 27 §5 – Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union.
[1120] RGPD, Art. 82 §2.
[1121] RGPD, Cons. 146 et Art. 82 §3.
[1122] RGPD, Cons. 146 et Art. 82 §4.

de la jurisprudence de la Cour de justice »[1123], en prévoyant expressément la réparation « complète et effective » du dommage « matériel ou moral » subi.

Dans le cas de la loi Informatique et libertés, une action en justice en application des dispositions de la loi sur la modernisation de la justice et celles du Code de justice administrative est ouverte aux personnes physiques[1124]. Et le législateur français souligne que cette action « *peut être exercée en vue soit de faire cesser le manquement* [aux dispositions du RGPD et de la présente loi], *soit d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis, soit de ces deux fins* »[1125]. Toutefois, il a conditionné le début de cet engagement de responsabilité d'un terme à échoir, l'alignant à la date d'entrée en application du RGPD en affirmant explicitement que « *la responsabilité de la personne ayant causé le dommage ne peut être engagée que si le fait générateur est postérieur au 24 mai 2018* »[1126]. Il est important de noter dans ce cadre, qu'à l'instar du RGPD, la loi Informatique et libertés a employé l'expression de « personne ayant causé le dommage » sans délimitation ou précision particulière, caractérisant ainsi son souhait d'y inclure toute personne physique ou morale responsable du dommage provoqué.

La volonté manifestée par ces nouvelles règlementations est bien celle d'un engagement de responsabilité en vue de garantir une réparation effective et complète du préjudice subi, aspirant *in fine* à combler les vides juridiques repérés dans l'ancienne législation.

Mais ce système de responsabilisation semble être, en quelque sorte, limité et entaché de subsidiarité, puisqu'il ne prend pas concrètement en compte les autres acteurs pouvant intervenir dans le traitement des données et jouant donc un rôle dans la mise en œuvre de leur protection[1127]. Ce furent pourtant les préconisations du Conseil d'État dans son étude annuelle sur « Le numérique et le droits fondamentaux » dans laquelle il confirmait que, pour éviter une dilution de responsabilité, il est important de maintenir la place centrale du responsable du traitement dans la protection des données, tout en précisant néanmoins que les obligations de celui-ci « *devraient être complétées par la définition d'une « chaîne de responsabilités », allant*

[1123] RGPD, Cons. 146.
[1124] Loi Informatique et libertés, Art. 37 § I (modifié par l'ordonnance du 12 décembre 2018) « *Sous réserve du présent article, le chapitre Ier du titre V de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle et le chapitre X du titre VII du livre VII du code de justice administrative s'appliquent à l'action ouverte sur le fondement du présent article.* »
[1125] Loi Informatique et libertés, Art. 37 §III.
[1126] Loi Informatique et libertés, Art. 37 §III.
[1127] *Cf.* p. 135.

des éditeurs de logiciels et des fabricants d'objets connectés en amont aux particuliers en aval »[1128].

Par conséquent, les fabricants et éditeurs de logiciels devraient incorporer au sein même de leurs activités le souci de la protection des données, tel que visé notamment par le principe de protection des données dès la conception prévu par le RGPD ; les sous-traitants doivent, activement et conjointement, collaborer et coopérer avec les responsables du traitement pour s'acquitter de leurs obligations, et les particuliers doivent mesurer les implications du principe de responsabilité puisque, selon le Conseil, « *en matière de données personnelles comme en tout autre domaine, la liberté consiste à faire ce qui ne nuit pas à autrui* », mais aussi, indique-t-il, « *la co-régulation peut contribuer à la responsabilisation des acteurs professionnels* », l'exemple américain montrant les limites de l'autorégulation[1129].

Cette chaîne de responsabilité n'est pas explicitement prévue par le RGPD, ou par la loi Informatique et libertés qui, dans le cas de cette dernière, se contente de citer « la personne ayant causé le dommage ». Quant au Règlement, il indique qu'il « convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données » lors de l'élaboration de la conception de produits, services et applications, qui reposent sur le traitement de données ou traitent des données personnelles, pour remplir leurs fonctions, comme notamment la prise en considération des principes de protection des données dès la conception et de protection des données par défaut[1130]. Il convient en outre de les inciter, « compte dûment tenu de l'état des connaissances », à s'assurer que les responsables du traitement et sous-traitants sont en mesure de s'acquitter de leurs obligations et exigences en ce qui concerne la protection des données[1131].

Ce système de responsabilité et de réparation mis en place s'inscrit, dès lors, dans l'optique adoptée par les juridictions de l'Union, particulièrement en ce qui concerne le droit à la vie privée tel qu'il a été précédemment vu. En contrôlant les atteintes à ce droit, elles vérifient les marges d'appréciation laissées aux États et aspirent, notamment, à repérer un juste équilibre entre les intérêts en cause, afin de se prononcer sur la responsabilité ou la réparation du préjudice subi, et à assurer, de manière concrète, un droit à un recours effectif tel que

[1128] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 183.
[1129] Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux*, *Id.*, p. 183.
[1130] RGPD, Cons. 78 et Art. 25 – Protection des données dès la conception et protection des données par défaut.
[1131] RGPD, Cons. 78.

prévu, également, par l'article 13 de la Convention[1132]. Le fait de reconnaître une violation peut constituer en soi, dans certain cas, une réparation suffisante et adéquate pour le dommage moral subi par une victime[1133]. C'est bien une étude au cas par cas, en fonction des contextes propres à chaque circonstance, qu'il faut entreprendre pour déterminer, *in concreto*, la responsabilité et la réparation adéquate et effective à accorder.

B. Un système de sanction d'initiative institutionnelle

Le système répressif conçu par le RGPD fait principalement la promotion des amendes administratives pouvant être imposées par les autorités de contrôle qui veillent à ce que celles-ci « soient, dans chaque cas, effectives, proportionnées et dissuasives »[1134]. Selon le Règlement, ce système comprend deux grandes catégories de sanctions : des sanctions administratives harmonisées et déterminées à l'initiative des autorités de contrôle, et des sanctions administratives ou pénales à l'initiative des États membres, « en particulier pour les violations qui ne font pas l'objet des amendes administratives » prévues par le RGPD[1135], ou lorsque celui-ci « n'harmonise pas les sanctions administratives ou, si nécessaire dans d'autres circonstances, par exemple en cas de violation grave » dudit Règlement[1136] ; le tout régi par un « mécanisme de contrôle de la cohérence »[1137].

Ainsi, le Règlement énumère des violations qui font l'objet d'amendes administratives pouvant s'élever, d'une part, jusqu'à dix millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, ou, d'autre part, jusqu'à vingt millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu[1138]. Dans le premier cas, les sanctions fixées[1139] concernent la violation des obligations incombant au responsable du traitement et au sous-traitant en vertu des dispositions

[1132] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Art. 13 – Droit à un recours effectif : « *Toute personne dont les droits et libertés reconnus dans la présente Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles.* »
[1133] CEDH (2ème Section), Affaire Egill Einarsson c. Iceland, Requête N° 24703/15, du 7 novembre 2017, points 32 à 34, et 55 à 57 ; la Cour juge ainsi que « *The Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage that may have been sustained by the applicant.* »
[1134] RGPD, Art. 83 §1 – Conditions générales pour imposer des amendes administratives.
[1135] RGPD, Art. 84 §1 – Sanctions.
[1136] RGPD, Cons. 152.
[1137] RGPD, Art. 63 – Mécanisme de contrôle de la cohérence : « *Afin de contribuer à l'application cohérente du présent règlement dans l'ensemble de l'Union, les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission dans le cadre du mécanisme de contrôle de la cohérence établi dans la présente section* ».
[1138] RGPD, Art. 83 §§ 4 et 5.
[1139] RGPD, Art. 83 §4 points a) à c).

relatives aux conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information[1140], des dispositions relatives aux traitements ne nécessitant pas l'identification[1141], des dispositions relatives aux exigences et missions dans le cadre du respect des obligations dans le traitement des données[1142], ou des dispositions relatives aux certifications et organismes de certification[1143]. Ces sanctions concernent aussi la violation des obligations incombant à l'organisme de certification[1144], ou celles incombant à l'organisme chargé du suivi des codes de conduite[1145]. Dans l'autre cas, les sanctions administratives fixées[1146], à caractère encore plus dissuasif, concernent la violation des principes de base d'un traitement, y compris les conditions applicables au consentement, en vertu des dispositions relatives aux principes en matière de traitement des données personnelles[1147], à la licéité du traitement[1148], aux conditions applicables au consentement[1149] et au traitement portant sur des catégories particulières de données[1150] ; la violation des droits dont bénéficient les personnes concernées[1151] ; la violation des dispositions relatives aux transferts des données[1152] ; ou la violation des obligations découlant du droit des États membres adoptées dans le cadre des situations particulières de traitement[1153]. Les sanctions en question concernent, enfin, le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement, ou de la suspension des flux de données ordonnée par l'autorité de contrôle[1154], ou le fait de ne pas accorder l'accès prévu[1155].

Il ressort des termes de ces dispositions, et à la lumière des définitions fournies par le Règlement[1156], que ces sanctions s'appliquent à toute structure, que celle-ci soit responsable du

[1140] RGPD, Art. 8.
[1141] RGPD, Art. 11.
[1142] RGPD, Art. 25 à 39.
[1143] RGPD, Art. 42 et 43.
[1144] RGPD, Art. 42 et 43.
[1145] RGPD, Art. 41 §4.
[1146] RGPD, Art. 83 §5 points a) à e).
[1147] RGPD, Art. 5.
[1148] RGPD, Art. 6.
[1149] RGPD, Art. 7.
[1150] RGPD, Art. 9.
[1151] RGPD, Art. 12 à 22 : informations à recevoir, accès aux données personnelles, droit de rectification ; droit à l'effacement, droit à la limitation du traitement ; notification des mesures prises s'agissant de ces trois derniers droits, droit à la portabilité des données, droit d'opposition, y compris dans le cas du profilage.
[1152] RGPD, Art. 44 à 49
[1153] RGPD, Art. 85 à 91 : traitement et liberté d'expression et d'information ; traitement et accès du public aux documents officiels ; traitement du numéro d'identification national ; traitement de données dans le cadre des relations de travail ; garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ; obligation de secret ; et règles existantes des églises et associations religieuses en matière de protection des données.
[1154] RGPD, Art. 58 §2.
[1155] RGPD, Art. 58 §1.
[1156] RGPD, Art. 4, points 7), 8), 10) et 16) à 19).

traitement, sous-traitant ou ayant un représentant dans l'Union, ou qu'elle propose une offre de biens ou de services visant des individus qui se trouvent sur le territoire de l'Union. Les activités de profilage visant ces derniers sont, en outre, également concernées. Dans ce contexte, il apparaît qu' « *il n'y a pas de critère de taille d'entreprise, de lieu de stockage des données ou encore de secteur d'activité : toute entreprise qui cible le territoire européen et effectue des traitements de données à caractère personnel est concernée par ce règlement* »[1157].

Quant aux autres sanctions à l'initiative des institutions nationales, le Règlement indique que les États membres peuvent déterminer le régime de sanctions pénales applicables en cas de violation des dispositions règlementaires ou nationales, en plus des amendes administratives prévues[1158]. Cependant, l'application de sanctions pénales et l'application de sanctions administratives ne devraient pas entraîner, selon le RGPD, « la violation du principe *ne bis in idem* tel qu'il a été interprété par la Cour de justice ». Par conséquent, il convient de se référer aux critères employés par la Cour pour déterminer la nature de l'infraction et son degré de gravité, en vue d'établir la « possibilité d'option, voire de cumul » entre sanction pénale et sanction disciplinaire[1159].

La loi Informatique et libertés établit, à cet égard, des sanctions administratives que peuvent prononcer l'autorité de contrôle, en l'occurrence la CNIL, en cas de violation des dispositions européennes ou nationales. Ainsi, la formation restreinte de la CNIL peut, en plus des procédures de mises en demeure, prononcer un rappel à l'ordre, enjoindre de mettre le traitement en conformité avec les dispositions juridiques, y compris sous astreinte, limiter temporairement ou définitivement un traitement, retirer une certification ou enjoindre l'organisme de certification de refuser une certification ou de retirer la certification accordée, suspendre les flux de données, suspendre partiellement ou totalement la décision d'approbation des règles d'entreprise contraignante, ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte, et/ou prononcer une amende administrative[1160]. Par ailleurs, ladite loi prévoit des mesures répressives particulières en cas de violation des droits et libertés mentionnés à l'article 1er de celle-ci, à savoir l'identité humaine, les droits de l'homme, la vie privée, les libertés individuelles ou publiques[1161]. Et, en cas d'atteinte grave et immédiate

[1157] J.-L. SAURON et M. QUÉMÉNER, « Le régime de sanction du RGPD : quand la complétude l'emporte sur la cohérence », Dalloz IP/IT 2018, p. 23.
[1158] RGPD, Cons. 149 et Art. 84.
[1159] CJUE (Grande ch.), décision préjudicielle « Łukasz Marcin Bonda », affaire C-489/10 du 5 juin 2012, §37 ; et, CEDH (Cour Plénière), affaire Engel et autres c. Pays-Bas du 8 juin 1976, série A n° 22, Pourvois nos 5100/71 et autres, § 80 à 82.
[1160] Loi Informatique et libertés, Art. 20 § III (Modifié par la loi n° 2022-52 du 24 janvier 2022), et CNIL, « La procédure de sanction » : https://www.cnil.fr/fr/la-procedure-de-sanction
[1161] Loi Informatique et libertés, Art. 21 § I points 1) à 8) (Modifié par l'ordonnance du 12 décembre 2018).

à ceux-ci, le président de la CNIL « *peut en outre demander, par la voie du référé, à la juridiction compétente, d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés* »[1162].

Par ailleurs, le Règlement fournit une liste de critères, permettant aux autorités de contrôle de décider s'il y a lieu d'imposer une amende administrative et du montant de celle-ci, qui doit être dûment prise en compte dans chaque cas d'espèce. L'application des sanctions administratives s'avère être, en ce sens, encadrée par les dispositions réglementaires qui déterminent également les violations réprimées et le montant maximal des sanctions imposé. Par conséquent, dans un souci de renforcer et d'harmoniser les sanctions administratives applicables en cas de violation, toute autorité de contrôle compétente a le pouvoir d'imposer, dans chaque cas d'espèce, une amende administrative « en prenant en considération toutes les caractéristiques propres à chaque cas » et en tenant dûment compte, notamment, « de la nature, de la gravité et de la durée de la violation et de ses conséquences, ainsi que des mesures prises pour garantir le respect des obligations découlant du règlement et pour prévenir ou atténuer les conséquences de la violation »[1163]. Le RGPD indique que ces sanctions peuvent être infligées « en complément ou à la place des mesures appropriées » imposées par l'autorité de contrôle, en explicitant qu' « *en cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende* »[1164].

Cela dit, le choix laissé à l'autorité de contrôle entre les sanctions administratives harmonisées et les mesures alternatives appropriées risque de la mener vers une appréciation assez complexe des circonstances, pouvant la conduire à adopter l'une des deux voies. En réalisant cette appréciation, il convient, selon le Règlement, de « tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante »[1165]. De plus, lorsque l'amende est imposée à une personne ne constituant pas une entreprise, l'autorité de contrôle devrait également « *tenir compte, lorsqu'elle examine quel*

[1162] Loi Informatique et libertés, Art. 21 § IV.
[1163] RGPD, Cons. 148 et 150, et Art. 83 § 2 points a) à k).
[1164] RGPD, Cons. 148.
[1165] RGPD, Cons. 148 et Art. 83 §2.

serait le montant approprié de l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause »[1166].

En tout état de cause, le Règlement conçoit le recours au mécanisme de contrôle de la cohérence « pour favoriser une application cohérente » du système de sanction mis en place[1167]. De manière générale, il est prévu que, « *afin de contribuer à l'application cohérente du règlement dans l'ensemble de l'Union, les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission dans le cadre du mécanisme de contrôle de la cohérence établi* »[1168]. Au regard des nombreux renvois aux droits nationaux opérés par les dispositions même du Règlement et des différentes obligations imposées par celles-ci, il semble utile de se pencher sur la notion de « cohérence »[1169] ainsi envisagée par le législateur européen, notamment en raison de l'inclusion du secteur public dans le champ d'application du RGPD.

Une des originalités de ce Règlement européen, d'applicabilité directe, est d'avoir ouvert la possibilité pour les États membres « d'intégrer des éléments » de celui-ci dans leur droit, « dans la mesure nécessaire pour garantir la cohérence »[1170]. De plus, et afin « d'assurer la cohérence » avec le Règlement, la modification de la directive « vie privée et communications électroniques »[1171] est déjà anticipée et attendue[1172]. La loi Informatique et libertés, dans sa dernière version, fait une seule fois référence au « contrôle de la cohérence » qui peut être mis en œuvre par le bureau de la commission, chargé de le faire par la CNIL, lorsque celle-ci adopte un projet de décision en tant qu'autorité chef de file ou autorité compétente[1173].

Le législateur européen conçoit l'instauration de ce mécanisme de contrôle de la cohérence « pour la coopération entre les autorités de contrôle » et fournit quelques cas où il est prescrit d'y recourir, tels que lorsqu'une autorité de contrôle entend adopter une mesure destinée à produire des effets juridiques en ce qui concerne des activités de traitement affectant sensiblement un nombre important de personnes dans plusieurs États membres, ou encore lorsqu'une autorité de contrôle concernée ou la Commission « demande que cette question soit traitée dans le cadre du mécanisme de contrôle de la cohérence »[1174]. En outre, plusieurs

[1166] RGPD, Cons. 150.
[1167] RGPD, Cons. 150.
[1168] RGPD, Art. 63 – Mécanisme de contrôle de la cohérence.
[1169] RGPD, Chap. VII. *Coopération et cohérence*, Section 2 – Cohérence.
[1170] RGPD, Cons. 8.
[1171] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31 juillet 2002, p. 37).
[1172] RGPD, Cons. 173.
[1173] Loi Informatique et libertés, Art. 24, 3ème al., point 2°.
[1174] RGPD, Cons. 135.

dispositions du Règlement requièrent l'application de ce mécanisme[1175] conformément au cadre établi par celui-ci, et dans lequel il est prévu que le comité émet un avis, dans un délai déterminé, si une majorité de ses membres le décide ou s'il est saisi d'une demande en ce sens par une autorité de contrôle concernée ou par la Commission[1176]. Il est aussi prévu que le Comité est habilité à adopter des décisions juridiquement contraignantes en cas de litiges entre autorités de contrôle[1177]. Cela dit, le Règlement prévoit, en parallèle, plusieurs dérogations à ce mécanisme, comme dans le cadre d'une procédure d'urgence[1178] ou dans un cas présentant une dimension transfrontalière, dans lequel le mécanisme de coopération devrait être appliqué et l'assistance mutuelle ainsi que des opérations conjointes pourraient être mises en œuvre entre les autorités de contrôle, « sur une base bilatérale ou multilatérale, sans faire jouer le mécanisme de la cohérence »[1179].

La sphère publique est incluse dans le champ d'application du RGPD, qui s'applique à tout traitement automatisé de données personnelles, alors qu'il ressort de ses dispositions que les « autorités publiques » n'en sont pas les cibles principales et que plusieurs mesures protectrices, marges de manœuvre et dérogations spécifiques sont prévues à leurs bénéfices[1180], rompant *ipso facto* la cohérence aspirée par ce texte. Après avoir annoncé qu'il convient d'assurer une « application cohérente et homogène des règles de protection des libertés et droits fondamentaux » des personnes à l'égard du traitement des données personnelles dans l'ensemble de l'Union, le Règlement affirme qu'en ce qui concerne le traitement de données « nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement », les États peuvent maintenir ou introduire des législations nationales particulières, « y compris en ce concerne le traitement de catégories particulières de données à caractère personnel » (données sensibles)[1181].

Alors qu'il y fait souvent référence, le RGPD ne précise pas ce qu'il faut entendre par « autorité publique », à l'exception du seul contexte d'accès du public aux documents officiels où il « *convient d'entendre par « autorités publiques et organismes publics », toutes les autorités ou*

[1175] RGPD, Art. 41 §3, 46 §4, 51 §3, par ex.
[1176] RGPD, Cons. 136, Art. 64 – Avis du comité, et Art. 70 §1 point t).
[1177] RGPD, Cons. 136 et Art. 65 – Règlement des litiges par le Comité.
[1178] RGPD, Art. 66 – Procédure d'urgence
[1179] RGPD, Cons. 138.
[1180] RGPD, Cons. 6, 19, 31, 43, 45, 47, 50, 51, 55, 65, 68, 80, 128, 145, 158 ; Art. 1, 2, 4 points 7), 8) et 9) pour ne citer que quelques exemples.
[1181] RGPD, Cons. 10.

autres organismes relevant du droit d'un État membre en matière d'accès du public aux documents »[1182]. Pourtant, le Règlement vise cette notion dans plusieurs des termes définis, tel que dans la définition de « responsable du traitement »[1183], « sous-traitant »[1184], « destinataire »[1185], « tiers »[1186] ou « autorité de contrôle »[1187], sans jamais cerner les contours de la notion en soi. Il se contente d'avancer qu'il « *devrait appartenir au droit de l'Union ou au droit d'un État membre de déterminer si le responsable du traitement exécutant une mission d'intérêt public ou relevant de l'exercice de l'autorité publique devrait être une autorité publique ou une autre personne physique ou morale de droit public ou, lorsque l'intérêt public le commande, y compris à des fins de santé, telles que la santé publique, la protection sociale et la gestion des services de soins de santé, de droit privé, telle qu'une association professionnelle* »[1188].

De même, la notion d'entreprise[1189] est définie, mais celle d'entreprise publique est absente du texte du Règlement. Il semble alors que, mis à part quelques dispositions visant les PME, l'ensemble des entreprises sont sur un pied d'égalité en ce qui concerne ce texte règlementaire qui relève, en propos liminaire, que « *les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités* »[1190].

Par ailleurs, plusieurs dispositions conservent « *un statut « à part », relativement protecteur pour les autorités publiques* »[1191]. Concernant la licéité du traitement, le RGPD affirme que le

---

[1182] RGPD, Cons. 154.

[1183] RGPD, Art. 4 point 7) « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; [...]* »

[1184] RGPD, Art. 4 point 8) « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;* »

[1185] RGPD, Art. 4 point 9) « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ;* »

[1186] RGPD, Art. 4 point 10) « *une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ;* »

[1187] RGPD, Art. 4 point 21) « *une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51 ;* »

[1188] RGPD, Cons. 45.

[1189] RGPD, Art. 4 point 18) « *une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique ;* »

[1190] RGPD, Cons. 6.

[1191] J.-L. SAURON et M. QUÉMÉNER, « Le régime de sanction du RGPD : quand la complétude l'emporte sur la cohérence », *Id.,* p. 25.

traitement n'est licite que s'il est, entre autres, « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement », ou s'il est « nécessaire aux fins des intérêts légitimes poursuivi par le responsable du traitement ou par un tiers », mais souligne que ce dernier point « ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions »[1192] étant donné « qu'il appartient au législateur de prévoir par la loi la base juridique » pour le traitement des données par les autorités publiques[1193]. La directive 95/46/CE, désormais abrogée, ne prévoyait pas cette exclusion de l'intérêt légitime en tant que fondement licite d'un traitement effectué par une autorité publique[1194], caractérisant, *ipso facto*, l'aspect plus protecteur du RGPD vis-à-vis de celle-ci. Eu égard à la jurisprudence en la matière[1195], la base juridique d'un traitement opéré par un responsable du traitement appartenant à une autorité publique est, dans la plupart des cas, la loi, plus protectrice que le consentement ou l'intérêt légitime sur lequel se fonde un responsable du traitement appartenant au secteur privé.

En effet, le Règlement annonce, de manière globale, que lorsque le traitement est effectué conformément à une obligation légale à laquelle le responsable du traitement est soumis, ou lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, le traitement devrait avoir un fondement légal en indiquant qu'une seule disposition légale « peut suffire pour fonder plusieurs opérations de traitement » de ce genre[1196].

En matière de conservation de données, la règle est la limitation de la conservation « *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* »[1197]. Toutefois, précise le texte du RGPD, la conservation ultérieure des données devrait être licite lorsqu'elle est « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique »[1198].

[1192] RGPD, Art. 6 §1, points e) et f), et, dernier al.
[1193] RGPD, Cons. 47.
[1194] Directive 95/46/CE, Section II – Principes relatifs à la légitimation des traitements de données, Art. 7.
[1195] *Cf.* p. 168 et s.
[1196] RGPD, Cons. 45 « *[...]. Le présent règlement ne requiert pas de disposition légale spécifique pour chaque traitement individuel. Une disposition légale peut suffire pour fonder plusieurs opérations de traitement basées sur une obligation légale à laquelle le responsable du traitement est soumis ou lorsque le traitement est nécessaire pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique. Il devrait également appartenir au droit de l'Union ou au droit d'un État membre de déterminer la finalité du traitement. Par ailleurs, ce droit pourrait préciser les conditions générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. [...]* »
[1197] RGPD, Art. 5 §1, point e).
[1198] RGPD, Cons. 65.

En ce qui concerne les droits des personnes, une dérogation au droit à l'effacement (droit à l'oubli) est prévue en faveur des autorités publiques, dans la mesure où ce traitement est nécessaire « pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »[1199]. Quant au droit à la portabilité des données, « de par sa nature même » clarifie le Règlement, il ne devrait pas être exercé à l'encontre de responsables du traitement qui traitent des données « dans l'exercice de leurs missions publiques »[1200]. De même, le RGPD établit des limitations « à la portée des obligations et des droits » qu'il a conçues au bénéfice des autorités publiques pour garantir, *inter alia*, la sécurité nationale, la défense nationale, la sécurité publique, la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, ou encore d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale[1201]. *Idem* en matière de transferts de données et de coopération internationale où le Règlement prend en compte les contraintes et les exigences liées aux missions publiques, et prévoit en conséquent des dérogations pour les activités des autorités publiques[1202]. C'est également le cas concernant la désignation d'un représentant, nécessaire lorsque le responsable du traitement ou le sous-traitant qui n'est pas établi dans l'Union traite des données de personnes qui se trouvent dans l'Union, et que ses activités de traitement sont liées à l'offre de biens ou de services (à ces personnes), qu'un paiement leur soit demandé ou non, ou au suivi de leurs comportements, sauf si le responsable du traitement est « une autorité publique ou un organisme public »[1203].

Ce statut « à part » se manifeste aussi dans des dispositions traitant de droits procéduraux, tels que dans le cadre des règles relatives aux autorités de contrôle[1204] ou celles relatives au droit à un recours juridictionnel effectif[1205]. Il se manifeste, enfin, dans la possibilité offerte par le RGPD auxdites autorités d'échapper aux sanctions disciplinaires puisqu'il « devrait appartenir

[1199] RGPD, Art. 17 §3, point b).
[1200] RGPD, Cons. 68 « *[...]. Il ne devrait dès lors pas s'appliquer lorsque le traitement des données à caractère personnel est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. »*, et Art. 20 §3.
[1201] RGPD, Art. 23 §1, points a) à j).
[1202] RGPD, Art. 48 à 50.
[1203] RGPD, Cons. 80 et Art. 27 §2, point b).
[1204] RGPD, Cons. 128 et Art. 55 §2.
[1205] RGPD, Cons. 145 et Art. 79 §2.

aux États membres de déterminer si, et dans quelle mesure, les autorités publiques devraient faire l'objet d'amendes administratives »[1206]. Il est donc envisageable qu'aucune amende administrative ne soit prévue à l'encontre d'une autorité publique portant atteinte à certaines dispositions du Règlement, comme c'est le cas au Danemark et en Estonie, y compris à l'encontre des entreprises[1207]. La nouvelle loi Informatique et libertés prévoit ainsi le prononcé d'une amende administrative suivant les mêmes règles et modalités établies par le RGPD, « *à l'exception des cas où le traitement est mis en œuvre par l'État* »[1208].

Comme l'avaient souligné les anciens députés lors des débats parlementaires relatifs au projet de loi Informatique et libertés en 1977, « *certes, en ce qui concerne la collecte des informations, des interdictions sont prévues, […]. Mais cette garantie connaît une restriction très grave du fait qu'il est possible de passer outre à cette interdiction pour des motifs d'intérêt public, comme pour ce qui concerne la sûreté de l'État, la défense et la sécurité publique ; il serait possible de procéder à des traitements informatiques, sans publication de l'acte règlementaire d'autorisation, des partis politiques, des minorités* » ; en effet, « *l'informatique peut être une arme de premier plan au service d'un État policier* »[1209].

Section 2 – Une nouvelle conception de protection numérique souveraine

Les dispositions légales, ainsi mises en place, élaborent une nouvelle conception de protection numérique envisagée de manière souveraine, se caractérisant par une politique de liberté de circulation des données à connotation internationale (§1), ainsi que par des principes et valeurs numériques européens, établis et renouvelés, ayant une visée mondiale (§2).

§1. Une politique de liberté de circulation des données à connotation internationale

Cette politique de liberté de circulation mise en œuvre et élargie, se démarquant des limitations territoriales et aspirant à une applicabilité internationale, se traduit par l'instauration de dispositions particulières visant, d'une part, le transfert des données (A), et d'autre part, la portabilité des données (B).

[1206] RGPD, Cons. 150 et Art. 83 §7.
[1207] RGPD, Cons. 151 et Art. 83 §9.
[1208] Loi Informatique et libertés, Art. 20 §III, point 7°.
[1209] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit.*, p. 5786-5787.

A. Le transfert des données

Apprenant des erreurs et des manquements manifestés par son prédécesseur, le RGPD consacre tout un chapitre dédié à la régulation renouvelée des transferts de données personnelles[1210]. Tout en annonçant que « *les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union et d'organisations internationales sont nécessaires au développement du commerce international et de la coopération internationale* », il reconnaît que « *l'augmentation de ces flux a créé de nouveaux enjeux et de nouvelles préoccupations en ce qui concerne la protection des données* »[1211]. Le Règlement souligne ainsi la nécessité de s'assurer que la protection des données des citoyens et résidents européens s'étende au-delà des frontières européennes, ce qui ne constitue pas, en pratique, une tâche facile.

À une époque où tout devient numérisé et hyper-connecté, un nombre de plus en plus croissant de données et de métadonnées est généré grâce aux nombreuses ressources et techniques informatiques développées, et en développement, qui ne connaissent pas, pour leur part, la notion de « frontière », de « secteur déterminé/d'activité » ou d' « espace déterminé ». Il s'agit donc de trouver un équilibre subtil entre une « protection adéquate » des personnes et leurs données, dont la protection en Europe relève d'un droit fondamental, et « *une régulation pragmatique suscitant la confiance des acteurs et le développement de l'économie numérique* »[1212].

Suivant les prémisses posées par la directive de 1995[1213], le principe général applicable en matière de transfert au-delà des frontières de l'Union reste celui de l'interdiction, « *sauf à tomber sous le coup d'exceptions parfois juridiquement instables* »[1214]. Mais ni la directive ni le Règlement ne donnent de définition claire de ce qu'il faut entendre par « transfert ». L'OCDE, dans ses les lignes directrices relatives à la protection de la vie privée et les flux transfrontières de données personnelles, définit ces flux comme étant « la circulation de données de caractère personnel à travers les frontières nationales »[1215]. Il faut souligner que l'affaire Schrems contre Facebook précitée, très médiatisée, cristallisant l'un des enjeux majeurs en matière de protection des données et invalidant l'ancien accord transatlantique « *Safe Harbor* » entre l'Union européenne et les États-Unis, a fourni la feuille de route

[1210] RGPD, Chap. V – Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales, Art. 44 à 50.
[1211] RGPD, Cons. 101.
[1212] N. LANERET et S. HAMON, « Quel avenir pour les transferts internationaux ? », Dalloz IP/IT 2018, p. 31.
[1213] Directive 95/46/CE, Chap. IV – Transfert de données à caractère personnel vers des pays tiers, Art. 25-26.
[1214] N. LANERET et S. HAMON, « Quel avenir pour les transferts internationaux ? », *Id.*, p. 31.
[1215] OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, Annexe à la recommandation du Conseil, du 23 septembre 1980, Art. 1 point c).

nécessaire pour respecter le droit applicable en matière de protection des données personnelles et de respect de la vie privée.

À ce titre, le RGPD réaffirme le principe selon lequel un transfert vers un pays tiers ou une organisation internationale de données personnelles, « qui font ou sont destinées à faire l'objet d'un traitement après ce transfert », ne peut avoir lieu que si les conditions définies par les dispositions légales sont respectées par le responsable du traitement et le sous-traitant[1216]. Ce principe comprend également « les transferts ultérieurs » de données « *au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale* »[1217]. Cette dernière disposition confirme la volonté de ce texte d'étendre son champ d'application au-delà des frontières de l'Union de manière à ce que « le niveau de protection des personnes physiques » qu'il garantit ne soit pas « compromis ». À l'image de son prédécesseur, le RGPD prévoit des dérogations à ce principe général d'interdiction de transfert « pour des situations particulières »[1218] en introduisant, cependant, une nouvelle dérogation fondée sur les « intérêts légitimes poursuivis par le responsable du traitement », sous conditions[1219].

Le G29, dans ses lignes directrices relatives aux transferts de données hors UE, recommande d'abord de recourir aux mécanismes prévus par le Règlement en matière de transferts, et de ne s'appuyer sur les dérogations prévues qu'en l'absence de tels mécanismes conformément « *au principe de droit inhérent à l'ordre juridique européen qui consiste à interpréter les clauses d'exception de manière restrictive afin que l'exception ne devienne pas la règle* »[1220]. Il est opportun de se demander si ces dérogations, de manière pragmatique, continueront à faire l'objet d'interprétation stricte ou si, à l'inverse, elles fourniront une alternative séduisante exploitable par les exportateurs de données personnelles en cas d'invalidation des mécanismes réglementaires autorisant le transfert.

En outre, et à l'instar de la directive de 1995, le Règlement multiplie les mécanismes et les fondements légaux permettant au responsable du traitement de démontrer qu'il offre des garanties appropriées autorisant le transfert extra-européen des données, leur accordant ainsi

---

[1216] RGPD, Cons. 101, 103, 107 à 109, 111 à 113 et Art. 44 – Principe général applicable aux transferts.
[1217] RGPD, Cons. 101 et Art. 44.
[1218] RGPD, Cons. 111 et 112 ; Art. 49 – Dérogations pour des situations particulières.
[1219] RGPD, Cons. 113 et Art. 49 §1, al. 2.
[1220] Groupe de travail « Article 29 », Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005, WP 114, 2093-01/05/FR, p. 9. Et la Cour de justice de l'Union a souligné à plusieurs reprises que « *s'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaires* », arrêts Digital Rights Ireland de 2014, *op. cit.,* point 52 ou Tele2 Sverige AB de 2016, *op. cit.,* point 96, par exemple.

plus de souplesse et plus de choix. Autrement dit, « *si l'architecture reste substantiellement la même que celle de la directive de 1995, la réforme des règles relatives aux transferts internationaux clarifie et simplifie leur usage et introduit de nouveaux outils pour les transferts* »[1221]. Le plus simple pour un responsable du traitement souhaitant transférer des données demeure l'option, reprise par le RGPD, fondée sur une décision d'adéquation, dans laquelle la Commission a constaté « *que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat* »[1222]. En effet, une telle décision facilite la liberté de circulation des données sans que l'exportateur de celles-ci n'ait à fournir de garanties supplémentaires ou à obtenir une autorisation spécifique.

La Commission, seule compétente pour prononcer un constat d'adéquation, a l'obligation de prévoir dans celui-ci un « mécanisme d'examen périodique » de leur fonctionnement, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale[1223]. À ce titre, elle a désormais l'obligation de « surveiller le fonctionnement des décisions » adoptées sous le RGPD, et celle de « surveiller le fonctionnement des décisions » adoptées sous la directive 95/46/CE[1224]. Et le RGPD prévoit ainsi, qu'eu égard aux « valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme », la Commission devrait dans son évaluation « prendre en considération la manière dont un pays tiers déterminé respecte l'état de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal »[1225]. Par ailleurs, le RGPD prévoit, explicitement, une évaluation du niveau adéquat de protection offert sur un « territoire particulier » d'un pays tiers ou dans « un ou plusieurs secteurs déterminés », caractérisant dès lors la possibilité d'adopter une décision d'adéquation « partielle »[1226], sans devoir y inclure la totalité du pays.

Cette décision sert ainsi à établir qu'un pays tiers ou une organisation internationale fournit un niveau de protection des données « *substantiellement équivalent à celui garanti au sein de*

[1221] Communication de la Commission au parlement européen et au Conseil, Échange et protection de données à caractère personnel à l'ère de la mondialisation, Bruxelles, du 10 janvier 2017, COM(2017) 7 final, p. 4.
[1222] RGPD, Art. 45 – Transferts fondés sur une décision d'adéquation, §1.
[1223] RGPD, Cons. 106 et Art. 45 §3.
[1224] RGPD, Cons. 106 et Art. 45 §4.
[1225] RGPD, Cons. 104 et Art. 45 §2, points a) à c).
[1226] RGPD, Art. 45 §1 ; et Communication de la Commission, Échange et protection de données à caractère personnel à l'ère de la mondialisation, *loc. cit.,* p. 5.

l'Union »[1227]. Suivant les préconisations de la Cour de justice européenne, la Commission, dans sa communication sur l'échange et la protection des données à l'ère de la mondialisation, réaffirme que le principe d'adéquation « n'exige pas que l'on reproduise à l'identique les règles de l'UE », mais qu'il s'agit plutôt de déterminer si le système étranger « offre, dans son ensemble, par l'essence de ses droits et leur mise en œuvre effective, leur opposabilité et le contrôle de leur application, le niveau élevé requis de protection » [1228]. Elle considère qu'il y a lieu de prendre en compte, lors de son évaluation, « l'étendue des relations commerciales (existantes ou potentielles) de l'UE avec un pays tiers donné », ou « la relation politique globale avec le pays tiers concerné » par exemple[1229]. Dans cette communication, la Commission semble manifester un enthousiasme prononcé vis-à-vis des constats d'adéquation et une forte inclinaison à y recourir en observant, notamment, que « *bien que les approches et le niveau d'avancement législatif varient d'un pays à l'autre, il existe des indices d'une plus grande convergence vers d'importants principes en matière de protection des données, en particulier dans certaines régions du monde* »[1230].

En plus des décisions d'adéquation adoptées jusqu'à présent par la Commission[1231], elle a annoncé qu'elle entretiendra un « dialogue actif avec des partenaires commerciaux importants d'Asie de l'Est et du Sud-Est », à commencer par le Japon et la Corée en 2017[1232], et avec l'Inde, ainsi qu'avec des pays d'Amérique latine, en particulier du Mercosur[1233], et « du

---

[1227] CJUE, arrêt Schrems de 2015, *loc. cit.,* points 73, 74 et 96 ; RGPD, Cons. 104.

[1228] CJUE, arrêt Schrems de 2015, *Id.,* point 74, et Communication de la Commission, Échange et protection de données à caractère personnel à l'ère de la mondialisation, *Id.,* p. 7.

[1229] Communication de la Commission, Échange et protection de données à caractère personnel à l'ère de la mondialisation, *Ibid.,* p. 8 et 9.

[1230] Communication de la Commission, Échange et protection de données à caractère personnel à l'ère de la mondialisation, *Ibid.,* p. 2.

[1231] Communication de la Commission, Échange et protection de données à caractère personnel à l'ère de la mondialisation, *Ibidem.,* p. 7 : « *Ces décisions concernent des pays qui sont étroitement intégrés dans l'Union européenne et ses États membres (Suisse, Andorre, Îles Féroé, Guernesey, Jersey, Île de Man), d'importants partenaires commerciaux (Argentine, Canada, Israël, États-Unis) et des pays jouant un rôle précurseur dans l'élaboration de lois en matière de protection des données dans leurs régions respectives (Nouvelle Zélande, Uruguay)* »

[1232] Commission européenne - Communiqué de presse, « La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde », Bruxelles, le 23 janvier 2019 « *Il s'agit là de la dernière étape de la procédure lancée en septembre 2018, qui comportait l'avis du comité européen de la protection des données et l'accord d'un comité composé de représentants des États membres de l'UE. Elle entre en vigueur aujourd'hui, au même titre que la décision équivalente adoptée aujourd'hui par le Japon.* » ; Disponible en ligne : http://europa.eu/rapid/press-release_IP-19-421_fr.htm

[1233] Mercosur (*Mercado Común del Sur*) – Marché commun de l'Amérique du Sud : Communauté économique regroupant des pays d'Amérique du Sud, créée en 1991 par le traité d'Asunción. Ses membres permanents sont l'Argentine, le Brésil, le Paraguay et l'Uruguay, le Venezuela (adhérent depuis 2012 puis suspendu en 2017). La Colombie, le Chili, le Pérou, la Bolivie et l'Équateur, le Guyana et le Suriname ont le statut de membres associés. Pour plus d'informations : https://www.mercosur.int/en/ & http://ec.europa.eu/trade/policy/countries-and-regions/regions/mercosur/

voisinage européen » qui se sont montrés désireux d'obtenir un « constat d'adéquation »[1234]. Aux termes des dispositions du Règlement, il y a lieu également de compter le Sénégal et la Tunisie, adhérents depuis 2016 pour le premier et depuis 2017 pour le second[1235], à la Convention 108 qui devrait être, « en particulier », prise en considération par la Commission lors de l'évaluation du niveau de protection[1236]. De plus, à la suite de l'invalidation de l'accord dit *Safe Harbor* par la Cour, un nouvel accord dit *Privacy Shield* (Bouclier de protection des données UE-EU) a été mis en place entre l'Union et les États-Unis le 1er août 2016[1237]. Faisant dès son balbutiement l'objet de nombreuses contestations[1238], cet accord a finalement été déclaré invalide en 2020 par la Cour de Justice de l'Union[1239]. La conséquence pour tous ces pays et ces exportateurs est majeure, puisque les transferts de données personnelles vers des pays tiers constatés et certifiés « adéquats », par voie de décision, par la Commission représentent, *de facto*, des transferts licites.

Toutefois, au regard de l'arrêt rendu dans l'affaire Schrems précitée ayant conduit à la mise en place de cette architecture de transfert renouvelée et ses mécanismes innovants, il s'avère raisonnable de s'interroger sur le risque de remise en cause de certaines des décisions d'adéquation adoptées ou éventuellement de certaines des dispositions du Règlement en question, notamment à la lumière de ce qui a été précédemment analysé dans le cadre de cette étude[1240]. En effet, la Cour avait, en particulier, souligné qu'une « *réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications*

[1234] Communication de la Commission, Échange et protection de données à caractère personnel à l'ère de la mondialisation, *Id.,* p. 9.

[1235] Conseil de l'Europe, État des signatures et ratifications du traité 108 - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Situation au 02/03/2019 : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures

[1236] RGPD, Cons. 105 « *[…]. Il y a lieu, en particulier, de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel. […]* »

[1237] https://www.cnil.fr/fr/le-privacy-shield & https://www.privacyshield.gov/welcome

[1238] W. ASHFORD, « Les députés européens appellent à suspendre le Privacy Shield », LeMagIT, du 6 juillet 2018 : https://www.lemagit.fr/actualites/252444356/Les-deputes-europeens-appellent-a-suspendre-le-Privacy-Shield ; L'Homme Numérique, « Le Privacy Shield remis en cause », du 13 juin 2018 : https://lhommenumerique.wordpress.com/2018/06/13/le-privacy-shield-remis-en-cause/ ; La Quadrature du Net, « Privacy Shield : Un « bouclier » troué à refuser ! », du 8 juillet 2016 : https://www.laquadrature.net/2016/07/08/privacy-shield-bouclier-a-refuser/, et, « Lettre ouverte internationale des ONG demandant la suspension du Privacy Shield », du 3 mars 2017 : https://www.laquadrature.net/2017/03/03/appel_suspension_privacy_shield/ ; J. LAUSSON, « Privacy Shield : Le Parlement européen appelle les USA à protéger correctement ses citoyens », Numerama, du 12 juin 2018 : https://www.numerama.com/politique/384867-privacy-shield-le-parlement-europeen-appelle-les-usa-a-proteger-correctement-ses-citoyens.html

[1239] CJUE, arrêt de la Cour (Grande ch.), Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems du 16 juillet 2020, Affaire C-311/18 (Arrêt Schrems II).

[1240] *Cf.* p. 167 et s., 230 et s.

électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée »[1241].

En outre, le RGPD conçoit un autre mécanisme de transfert moyennant des garanties appropriées, « sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle »[1242]. Ainsi, en l'absence de décision d'adéquation, un responsable du traitement ou un sous-traitant peut transférer des données personnelles en fournissant des garanties appropriées, telles qu'un instrument juridiquement contraignant et exécutoire, ou des clauses types de protection adoptées par la Commission ou par une autorité de contrôle et approuvées par la Commission[1243]. De plus, le recours à un code de conduite approuvé ou à un mécanisme de certification approuvé sont, dorénavant, également inclus parmi les garanties appropriées visées par les dispositions du Règlement. Pour ce faire, chacun de ces outils doit être assorti « de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées »[1244], alors même que le responsable du traitement ou le sous-traitant en question n'est pas soumis au RGPD.

Les responsables du traitement ou les sous-traitants pourraient donc se reposer sur l'ensemble de ces outils pour, à la fois, se mettre en conformité au Règlement et pouvoir en rendre compte ainsi que pour des transferts extra-européen, sous réserve d'y inclure des instruments les rendant juridiquement contraignants et exécutoires pour les importateurs non soumis au RGPD. D'autres garanties appropriées peuvent aussi être fournies, notamment par des clauses contractuelles ou par des dispositions à intégrer dans des arrangements administratifs, sous réserve, dans ce cadre, de « l'autorisation de l'autorité de contrôle compétente »[1245].

Une des garanties appropriées visées, nouvellement introduite par le Règlement, constitue les « règles d'entreprise contraignantes » (*Binding Corporate Rules* – BCR), alternative aux clauses contractuelles types, qui doivent être approuvées par l'autorité de contrôle compétente, conformément au mécanisme de contrôle de la cohérence susmentionné[1246]. Celles-ci sont définies comme étant « *les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire*

[1241] CJUE, arrêt Schrems de 2015, *Ibid.,* point 94.
[1242] RGPD, Art. 46 – Transferts moyennant des garanties appropriées, §2.
[1243] RGPD, Cons. 107 et 108 ; Art. 46 §2, points a), c) et d).
[1244] RGPD, Art. 40 §3, 42 §2 et 46 §2, points e) et f).
[1245] RGPD, Cons. 109 et Art. 46 §3, points a) et b).
[1246] RGPD, Cons. 107, 108 et 110 ; Art. 46 §2, point b), et Art. 47 – Règles d'entreprise contraignantes

d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe »[1247]. Cette pratique a été initialement formalisée par le G29 dans son document de travail relatif aux transferts de données vers des pays tiers de 2003, et dans lequel il avait souligné que « *les règles d'entreprise contraignantes ne doivent pas être considérées comme la panacée dans le cadre des transferts internationaux, mais uniquement comme un instrument supplémentaire à utiliser là où les instruments existants semblent particulièrement poser problème* »[1248].

Réservées au départ aux seuls groupes d'entreprises, le Règlement, en les introduisant, étend le champ d'application de ces règles d'entreprise contraignantes en y incluant les « groupes d'entreprises engagées dans une activité économique conjointe », un groupe d'entreprise désignant « une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle »[1249]. Cette extension offre, par conséquent, la possibilité à différents groupes de sociétés ayant une « activité économique conjointe » de recourir à cet outil pour effectuer des transferts hors UE, ouvrant potentiellement la voie vers l'introduction de nouveaux « risques », et vers une remise en cause de la part des juridictions européennes. Les conditions et les exigences imposées par le RGPD en matière de règles d'entreprise contraignantes, telles que s'assurer que ces règles sont juridiquement contraignantes ou qu'elles confèrent expressément aux personnes des droits opposables, sont certes exigeantes mais pas insurmontables, comme le montrent les nombreuses décisions de la CNIL approuvant des BCR[1250].

[1247] RGPD, Art. 4, point 20).

[1248] Groupe de travail « Article 29 », Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, adopté le 3 juin 2003, 11639/02/FR, WP 74, p. 5.

[1249] RGPD, Art. 4, point 19), et une « entreprise » (point 18) est définie comme étant « *une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique* ».

[1250] RGPD, Art. 47 §§ 1 et 2, CNIL, Approbation des BCR : les différentes étapes, https://www.cnil.fr/sites/default/files/atoms/files/bcr-etapes_de_la_procedure_dapprobation.pdf , Délibération n° 2017-165 du 1 juin 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » et « sous-traitant » du groupe BOX. (BCR-040) : https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000034985104 ; Délibération n° 2017-239 du 7 septembre 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » du groupe UTC (BCR n° 045) : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000035571825&fastReqId=1526559154&fastPos=10 ; Délibération n° 2017-273 du 12 octobre 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » du groupe Merck & Co (MSD) (BCR n° 046) :

Enfin, le RGPD recommande, dans le cadre de ce chapitre consacré aux transferts hors l'UE, d'élaborer des « mécanismes de coopération internationale » destinés à faciliter et à mettre en place une « assistance mutuelle internationale » pour faire appliquer la législation relative à la protection des données personnelles[1251].

En ce sens, le G29, désireux d'identifier les possibilités de synergie entre les « règles d'entreprises contraignantes » (BCR) soumises à une autorisation d'une autorité de contrôle et les « Cross Border Privacy Rules » (CBPR) de l'APEC soumises à un contrôle de ses agents, a mis en place en 2014 un référentiel de critères et d'exigences pour les entreprises souhaitant recourir aux BCR et/ou aux CBPR. Ce référentiel facilite par conséquent, selon le groupe de travail, « *the design and adoption of personal data protection policies compliant with each of the systems* » et peut servir également comme fondement pour une « double certification »[1252].

Dans le cadre de l'APEC[1253], la Coopération économique pour l'Asie-Pacifique, les pays adhérents[1254] à ce mécanisme de coopération s'engagent à respecter des règles et principes, nommés « APEC *Privacy framework* », permettant de fournir des garanties pour les transferts, dont le respect des *Cross Border Privacy Rules*. Il serait alors concevable de voir naître une interopérabilité entre les outils et mécanismes du RGPD et ceux du CBPR ainsi que, plus largement, un partenariat entre les États de l'Union et ceux de l'APEC autorisant, *in fine*, les entreprises à effectuer des transferts internationaux vers ces derniers.

---

https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000035936633&fastReqId=1526559154&fastPos=9; ou encore, Délibération n° 2017-306 du 7 décembre 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » du groupe DANFOSS. (BCR n° 047): https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000036670925&fastReqId=1526559154&fastPos=6 ; Groupe de travail « Article 29 », Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (mis à jour), adopté le 29 novembre 2017, 17/EN, WP 256, et Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopté le 11 avril 2018, 17/EN WP264.

[1251] RGPD, Cons. 116 et Art. 50 – Coopération internationale dans le domaine de la protection des données à caractère personnel.

[1252] Groupe de travail « Article 29 », Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, adopté le 27 février 2014, 538/14/EN WP 212, p. 2.

[1253] Asian-Pacific Economic Cooperation : https://www.apec.org ; France diplomatie - Dossiers, L'APEC « *Créée en 1989 à l'initiative des États-Unis et de l'Australie, l'APEC est le principal forum économique intergouvernemental dans la région Asie-Pacifique. Ne reposant sur aucun traité fondateur, l'APEC est fondée sur le consensus et la libre coopération entre membres : ses décisions ne sont ainsi pas contraignantes juridiquement et les engagements des membres sont pris sur une base volontaire* » : https://www.diplomatie.gouv.fr/fr/dossiers-pays/asie-oceanie/les-dynamiques-d-integration-regionale/les-enceintes-de-cooperation-economique/article/l-apec

[1254] France diplomatie - Dossiers, L'APEC, *Id.*, « *L'APEC compte 21 « économies membres » riverains du Pacifique : Canada, États-Unis, Chili, Mexique, Pérou, Chine, Corée du Sud, Hong Kong (Chine), Japon, Russie, Taiwan (Chine), Brunei, Indonésie, Malaisie, Philippines, Singapour, Thaïlande, Vietnam, Australie, Nouvelle-Zélande, Papouasie-Nouvelle-Guinée. […]. Si la France n'est pas membre de l'APEC, elle est devenue en 1997, membre associé du PECC - Pacific Economic Cooperation Council -, organisme consultatif non gouvernemental fort de 21 membres, qui joue, de fait, le rôle de conseil économique de l'APEC.* »

Ainsi mis en œuvre, ce système relatif aux transferts internationaux de données « européennes » souhaite poursuivre le même double objectif précité, « assurer un équilibre subtil entre protection adéquate des données personnelles et accompagnement stratégique du développement de l'économie numérique », objectifs également poursuivis par la directive de 1995 remise en question par la Cour dans la fameuse affaire Schrems ; et ce panorama montre déjà, indique certains auteurs, « *l'influence de l'initiative européenne en matière de protection des données personnelles sur les législations à travers le monde. Certes à des stades et niveaux différents, mais on décèle bien une dynamique internationale vers une législation en ligne avec les dispositions du RGPD* »[1255].

B. La portabilité des données

Introduit dans le cadre des droits de la personne concernée, le « droit à la portabilité des données » représente un nouveau droit instauré par le Règlement, repris par la loi Informatique et libertés dans sa dernière version[1256], étroitement lié au droit d'accès et se complétant mutuellement, tout en étant différent et, désormais, autonome. Ce droit confère aux personnes concernées le « *droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* », sous réserves de conditions cumulatives[1257].

Le droit à la portabilité semble alors avoir pour objectif de responsabiliser les individus et leur accorder plus de contrôle sur leurs données. Ne prévoyant pas explicitement ce droit, la directive 95/46/CE disposait malgré tout que, en matière de droit d'accès aux données, toute personne a le droit d'obtenir du responsable du traitement, « *sans contrainte à des intervalles raisonnables et sans délais ou frais excessifs : [...] la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données* »[1258].

La portabilité des données représente, d'une part, le droit pour une personne de « recevoir ses données » personnelles traitées par un responsable du traitement et de les sauvegarder, en vue

[1255] N. LANERET et S. HAMON, « Quel avenir pour les transferts internationaux ? », *loc. cit.*, p. 32-33.
[1256] Loi Informatique et libertés, Art. 55 (Modifié par l'ordonnance du 12 décembre 2018) : « *Le droit à la portabilité des données s'exerce dans les conditions prévues à l'article 20 du règlement (UE) 2016/679 du 27 avril 2016* ».
[1257] RGPD, Art. 20 §1 – Droit à la portabilité des données.
[1258] Directive 95/46/CE, Art. 12, point a) – Droit d'accès.

d'un usage personnel ultérieur ou de les transmettre à un autre responsable du traitement. Dans ce contexte, ce droit complète efficacement le droit d'accès susmentionné. Cela dit, la portabilité offre, en plus, aux personnes concernées un moyen destiné à leur permettre de gérer et de réutiliser elles-mêmes aisément leurs données à caractère personnel, dans la mesure où le Règlement précise que celles-ci doivent être reçues « dans un format structuré, couramment utilisé et lisible par machine »[1259]. D'autre part, la portabilité des données représente le droit pour une personne de « transmettre ses données » d'un responsable du traitement à un autre responsable du traitement, sans que le premier « y fasse obstacle »[1260]. Et le Règlement prévoit le droit pour une personne d'obtenir que ses données soient « transmises directement » d'un responsable du traitement à un autre, « lorsque cela est techniquement possible »[1261]. Pour ce faire, le législateur européen encourage les responsables du traitement « à mettre au point des formats interopérables permettant la portabilité des données » en précisant que cela ne devrait pas cependant leur créer « d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles »[1262]. Le RGPD interdit cependant aux responsables du traitement d'entraver la transmission sollicitée par une personne concernée.

Le droit à la portabilité des données tend ainsi à dessiner une nouvelle voie : « *l'empowerment des individus à l'aide de leurs propres données* » en leur accordant les moyens de devenir les propres acteurs de leurs données[1263]. Cette nouvelle voie est aujourd'hui connue sous le nom de « Self Data », définie par ses promoteurs comme étant « *la production, l'exploitation et le partage de données personnelles par les individus, sous leur contrôle et à leurs propres fins* »[1264]. Les initiatives et outils liés ne manquent pas[1265] et devraient permettre, au fur et à mesure, de rétablir la confiance, « qui est en crise », entre les individus et les organisations : le « Self Data » promeut de multiples bénéfices pour les individus, tels que le contrôle de ses

[1259] RGPD, Cons. 68 et Art. 20 §1.
[1260] RGPD, Cons. 68 et Art. 20 §1.
[1261] RGPD, Art. 20 §2.
[1262] RGPD, Cons. 68.
[1263] MesInfos – SelfData (porté par Fing) : http://mesinfos.fing.org/selfdata-2/, et RGPD, Cons. 68 « *Pour renforcer encore le contrôle qu'elles exercent sur leurs propres données [...]* ».
[1264] MesInfos – SelfData, *Id.*
[1265] Par ex. : Self Data en France, Mydata en Finlande (https://mydata.org/finland/), My Data Choices en Angleterre (https://www.mydatachoices.co.uk), Smart Disclosure and consumer decision-making aux États-Unis (https://www.data.gov/consumer/smart-disclosure-policy & https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/report_of_the_task_force_on_smart_disclosure.pdf), Vendor RelationShip Management (VRM) (http://www.enrichedcloud.com/ECC/jsp/VRM.jsp), Cloud Personnel (https://www.lemondeinformatique.fr/actualites/lire-un-petit-cloud-personnel-avec-lima-ultra-67887.html & https://www.seagate.com/fr/fr/do-more/what-is-personal-cloud-master-dm/), Quantified Self (http://quantifiedself.com), Personal Data Store (PDS) (https://pds.mydex.org/what-personal-data-store-0 & http://pde.cc/tags/pds/), Personal Information Management System (PIMS) (https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en).

données, la gestion de ses informations, documents, contrats, identifiants ou autre, ou encore la possibilité de mieux se connaître et faire ses propres choix de consommation, et semble également profiter aux entreprises « en retrouvant la confiance et la fidélité de leurs clients, en améliorant la qualité des données dont elles disposent lorsque les individus partagent avec elles leurs données, et en gagnant en compétitivité »[1266]. Plusieurs projets découlent ainsi de cette nouvelle voie, comme le projet « Dataccess »[1267], réunissant plusieurs entreprises afin de concevoir des lignes directrices facilitant la mise en œuvre de la portabilité pour les individus et les entreprises, et l'émergence éventuelle, à terme, d'un « label Dataccess, celui des « entreprises data-responsables »[1268].

La portabilité des données paraît dès lors encourager, de manière contrôlée et limitée, le partage de données entre entreprises et, en conséquence, enrichir les expériences et les services clients. Plusieurs acteurs dans le domaine ont entrepris des études pour montrer les avantages et les risques liés à la mise en relation et à l'analyse de données personnelles provenant de différents aspects de la vie d'une personne en vue d'établir une image plus complète de son profil et une « mesure de soi » plus exhaustive (pratique du *Quantified Self*)[1269].

Ce droit à la portabilité des données contribue alors, à la fois, à la responsabilisation des individus et à la responsabilisation des responsables du traitement ; ces derniers devant mettre en œuvre toutes les procédures nécessaires pour répondre au mieux aux demandes de portabilité, y compris les procédures et mesures spécifiques en coopération avec les sous-traitants. De plus, le responsable du traitement destinataire des données se doit d'être en conformité avec les principes et les obligations énoncés par le RGPD, et est tenu de garantir que les données portables transmises sont pertinentes et non excessives au regard du nouveau traitement de données envisagé. En d'autres termes, « *les données acceptées et conservées*

[1266] MesInfos – SelfData, *Id.*

[1267] MesInfos – Fing « *MesInfos, c'est un peu « la portabilité avant la portabilité ». Ce projet réunit de nombreux partenaires pour explorer ensemble la notion de Self Data : permettre aux individus de devenir maîtres de leurs données en les récupérant depuis le système d'information des organisations avec lesquelles ils sont en relation, en les stockant dans des espaces sécurisés où ils peuvent administrer leurs données et surtout en tirant de celles-ci une valeur d'usage grâce à des services tiers* » : http://mesinfos.fing.org/dataccess-pour-une-portabilite-des-donnees-personnelles-coherente-et-positive-rgpd/

[1268] MesInfos – Fing, « Dataccess – Data-responsible Enterprises: User Experience and Technical Specifications » (En Anglais) – V.1 - February, 2018, Fing: http://mesinfos.fing.org/wp-content/uploads/2018/03/PrezDataccess_EN_V1.21.pdf

[1269] CNIL, Quantified Self (https://www.cnil.fr/fr/definition/quantified-self), Le Quantified Self, c'est quoi ? (https://www.cnil.fr/fr/cnil-direct/question/le-quantified-self-cest-quoi), Le corps, Nouvel objet connecté – Du Quantified Self à la M-Santé : les nouveaux territoires de la mise en données du monde, Cahier IP Innovation & Prospective N° 02, Mai 2014 (https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf), Agence française de la santé numérique, AsipSanté (https://esante.gouv.fr/interoperabilite), Université Paris-Est Marne-la-Vallée (UFR Sciences humaines et sociales), « Le Quantified self », Les mondes numériques, 18 février 2017 (https://lesmondesnumeriques.wordpress.com/2017/02/18/le-quantified-self/); et *Cf.* p. 156.

devraient se limiter à celles qui sont nécessaires et pertinentes au service fourni par le responsable du traitement destinataire »[1270]. À cet égard, celui-ci doit indiquer « clairement et directement » la finalité du nouveau traitement avant toute demande de portabilité de données, conformément au principe de transparence tel qu'établi par le Règlement[1271], et, partant, le traitement sera sous sa seule responsabilité[1272].

Il est utile de noter que l'exercice du droit à la portabilité des données doit s'opérer sans affecter les autres droits prévus par le Règlement, tel que le droit d'accès ou de rectification, et, plus particulièrement, sans porter préjudice au droit à l'effacement[1273]. En ce sens, une personne peut continuer à utiliser et à bénéficier du service d'un responsable du traitement même après la demande de portabilité de ses données puisque celle-ci, comme il est indiqué par les dispositions règlementaires, n'entraîne pas automatiquement l'effacement des données[1274]. De même, il est prévu qu'une personne souhaitant exercer son droit à l'effacement ne peut voir sa demande reportée ou refusée par le responsable du traitement sous le prétexte de la demande de portabilité.

Aux termes des dispositions du RGPD, ce nouveau droit à la portabilité des données s'applique lorsque le traitement est fondé soit sur le « consentement » de la personne ou sur un « contrat », et lorsqu'il est effectué « à l'aide de procédés automatisés », excluant, par conséquent, tous les dossiers papiers[1275]. Le Règlement écarte, par ailleurs, expressément du champ d'application de ce droit tout « traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement », et soutient que ce droit « ne devrait pas s'appliquer lorsque le traitement est fondé sur un motif légal autre que le consentement ou l'exécution d'un contrat » [1276].

[1270] Groupe de travail « Article 29 », Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016 - Version révisée et adoptée le 5 avril 2017, 16/FR WP 242 rev.01, p. 8.

[1271] RGPD, Chap. III, Section 1 – Transparence et modalités, et en particulier Art. 14 – Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée.

[1272] G29, Lignes directrices relatives au droit à la portabilité des données, *Id.,* p. 7-8, et le groupe souligne que « *le nouveau responsable du traitement ne doit pas traiter de données à caractère personnel qui ne sont pas pertinentes et le traitement doit être limité à ce qui est nécessaires au regard des nouvelles finalités, même si les données à caractère personnel font partie d'une série de données plus globale transmise au moyen d'un processus de portabilité. Les données à caractère personnel qui ne sont pas nécessaires pour réaliser la finalité du nouveau traitement doivent être supprimées dans les meilleurs délais* », p. 8 (note de bas de page n° 12).

[1273] RGPD, Art. 20 §3.

[1274] RGPD, Cons. 78, Art. 20 §3 et Art. 17 – Droit à l'effacement.

[1275] RGPD, Art. 20 §1 *« a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b) ; et, b) le traitement est effectué à l'aide de procédés automatisés*. »

[1276] RGPD, Art. 20 §3 et Cons. 68 « *[…]. De par sa nature même, ce droit ne devrait pas être exercé à l'encontre de responsables du traitement qui traitent des données à caractère personnel dans l'exercice de leurs missions publiques. Il ne devrait dès lors pas s'appliquer lorsque le traitement des données à caractères personnel est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à l'exécution*

En outre, dans le cadre de l'exercice de ce droit à la portabilité, les personnes ont le droit de recevoir les données à caractère personnel « les concernant » et qu'elles ont « fournies » à un responsable du traitement, restreignant *de facto* la nature des données transmises[1277]. À l'image du Règlement, son champ d'application se limite aux données personnelles relatives à la personne exerçant ce droit, excluant, de ce fait, les données anonymisées mais pas celles pseudonymisées, et comprend, pour sa part, uniquement les données « fournies » par celle-ci. Selon le G29 et la CNIL, cette dernière expression couvre, à la fois, les données « activement et consciemment fournies » par la personne, telles que l'adresse postal, l'âge, ou le nom d'utilisateur, ainsi que les données « générées » découlant de « l'observation » de l'activité d'une personne lorsqu'elle utilise un service ou un dispositif, ce qui peut inclure, par exemple, l'historique de recherche, les relevés de compte bancaire, les courriels envoyés ou reçus, des données brutes, comme le rythme cardiaque, collectées par des compteurs intelligents ou d'autres types d'objets connectés, ou les achats enregistrés sur une carte de fidélité[1278].

À l'inverse, selon ces mêmes institutions, cette dernière catégorie de données découlant de l'observation d'activités ne comprend pas les données qui sont « dérivées, calculées ou inférées » à partir des données fournies par la personne, tel qu'un « profil d'utilisateur créé par l'analyse des données brutes collectées à partir d'un compteur intelligent »[1279], et ce, en raison même du fait qu'elles sont générées par le responsable du traitement à la suite d'un traitement, donc créées, et non par la personne à la suite d'une observation. Le G29 observe ainsi que « *l'expression « fournies par » englobe les données qui se rapportent à l'activité de la personne concernée ou qui résultent de l'observation du comportement d'une personne, mais exclut les données résultant d'une analyse subséquente de ce comportement. En revanche, les données qui ont été créées par le responsable du traitement dans le cadre du traitement des données,*

---

d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. […]. ». Le G29, Lignes directrices relatives au droit à la portabilité des données, *Ibid.,* p. 10, affirme cependant : « *Dès lors, les responsables du traitement ne sont pas obligés de prévoir la portabilité dans ces cas. Toutefois, une bonne pratique consiste à mettre au point des processus visant à répondre automatiquement à des demandes de portabilité, en suivant les principes régissant le droit à la portabilité des données. Un exemple serait un service public fournissant un service de téléchargement facile des précédentes déclarations des revenus des particuliers. Concernant la portabilité des données en tant que bonne pratique dans le cas d'un traitement fondé sur la base juridique de la nécessité d'un intérêt légitime et de régimes volontaires existants, voir les pages 53 et 54 de l'avis 6/2014 du groupe de travail «Article 29» concernant les intérêts légitimes (WP 217).* » (Note de bas de p. n° 16)

[1277] RGPD, Art. 20 §1.

[1278] G29, Lignes directrices relatives au droit à la portabilité des données, *Ibid.,* p. 11-12, et, CNIL, Le droit à la portabilité en questions, 22 mai 2017 : https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions

[1279] G29, Lignes directrices relatives au droit à la portabilité des données, *Ibidem.,* p. 12, et, CNIL, Le droit à la portabilité en questions, 22 mai 2017, *Id.*

par un processus de personnalisation ou de recommandation, par catégorisation ou profilage des utilisateurs par exemple, sont des données qui sont dérivées ou déduites des données à caractère personnel fournies par la personne concernée et elles ne sont pas couvertes par le droit à la portabilité des données », et pourraient donc être conservées par le responsable du traitement[1280].

Néanmoins, la personne concernée conserve son droit « d'obtenir du responsable du traitement la confirmation » que des données la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données, ainsi que des informations sur « l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée »[1281]. Il est intéressant de noter que, à la suite de l'exercice de ce droit, une fois reçues par le responsable du traitement, les données envoyées dans le cadre de l'exercice du droit à la portabilité peuvent être considérées comme ayant été « fournies » par la personne et, par conséquent, retransmises conformément audit droit[1282].

Le RGPD pose, enfin, une dernière condition à ce droit, à savoir ne pas porter atteinte aux « droits et libertés de tiers »[1283]. Cette condition vise, selon le G29, à « empêcher l'extraction et la transmission » de données contenant les données personnelles d'autres personnes (non consentantes) à un nouveau responsable du traitement dans le cas où ces données sont « susceptibles d'être traitées d'une manière qui porterait atteinte » aux droits et libertés des autres personnes concernées[1284]. À cet égard, le groupe de travail indique qu' « un « nouveau » responsable du traitement destinataire ne peut pas utiliser les données de tiers qui lui sont transmises à des fins qui lui sont propres, comme pour proposer des produits et services de marketing à ces autres tierces personnes », et souligne que « *ces informations ne doivent pas être utilisées pour enrichir le profil de la tierce personne concernée et reconstruire son environnement social, sans qu'elle en soit informée et qu'elle y ait consenti* »[1285].

[1280] G29, Lignes directrices relatives au droit à la portabilité des données, *Ibidem,* p. 13.
[1281] RGPD, 15 §1, point h) ; Voir également Art. 13 §2 et 14 §2.
[1282] G29, Lignes directrices relatives au droit à la portabilité des données, *Id.,* p. 8, et, CNIL, Le droit à la portabilité en questions, 22 mai 2017, *Id.*
[1283] RGPD, Art. 20 §4 et Cons. 68 « *[…]. Lorsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres personnes concernées conformément au présent règlement. […].* »
[1284] G29, Lignes directrices relatives au droit à la portabilité des données, *Id.,* pp. 12 à 14.
[1285] G29, Lignes directrices relatives au droit à la portabilité des données, *Ibid.,* p. 14, et le groupe observe ainsi qu' « *un service de réseaux sociaux ne doit pas enrichir le profil de ses membres en utilisant des données à caractère personnel transmises par une personne concernée dans le cadre de son droit à la portabilité des données sans respecter le principe de transparence et veiller à ce que ce traitement spécifique repose sur une base juridique appropriée.* » (Note de bas de p. n° 23).

Par ailleurs, le RGPD précise que le droit de transmettre les données, dans le contexte du droit à la portabilité, implique que la transmission doit se faire sans que le responsable du traitement, à qui la demande a été faite, n'y « fasse obstacle »[1286]. Il peut s'agir, indique le groupe de travail, « d'entraves juridiques, techniques ou financières » agencées par le responsable du traitement afin d'empêcher ou de ralentir « l'accès aux données, leur transmission ou leur réutilisation » par la personne concernée et/ou un autre responsable du traitement, telles qu'un « manque d'interopérabilité ou l'absence d'accès à un format de données ou à une interface de programme d'application ou le format fourni », ou encore « l'obscurcissement délibéré de l'ensemble de données » par exemple[1287].

De plus, le Règlement envisage la possibilité d'une transmission directe entre responsables du traitement, à la demande de la personne exerçant son droit à la portabilité, « lorsque cela est techniquement possible »[1288]. Et les dispositions du Règlement viennent préciser les contours de ce qui est « techniquement possible » en affirmant que le droit de la personne concernée de transmettre ou de recevoir des données la concernant « *ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles* »[1289]. À ce titre, le Règlement encourage les responsables du traitement à transmettre les données dans des « formats interopérables », mais sans que cela n'oblige les autres à prendre en charge ces formats[1290]. Une transmission directe entre responsables du traitement peut, par conséquent, avoir lieu, selon le G29, « *lorsque la communication entre deux systèmes est possible, de manière sécurisée (par une communication authentifiée présentant le niveau de chiffrement des données nécessaire), et lorsque le système récepteur est techniquement en mesure de recevoir les données entrantes* »[1291]. En outre, le RGPD stipule que les données reçues par la personne ayant exercé son droit à la portabilité doivent être dans un format permettant leur réutilisation, plus précisément, dans un format « structuré, couramment utilisé, lisible par machine et interopérable »[1292].

L'interopérabilité est définie dans le droit de l'Union européenne comme étant « *l'aptitude d'organisations disparates et diverses à interagir en vue de la réalisation d'objectifs communs mutuellement avantageux, arrêtés d'un commun accord, impliquant le partage d'informations et de connaissances entre ces organisations à travers les processus métiers qu'elles prennent*

[1286] RGPD, Art. 20 §1.
[1287] G29, Lignes directrices relatives au droit à la portabilité des données, *Ibid.,* p. 18-19.
[1288] RGPD, Art. 20 §2.
[1289] RGPD, Cons. 68.
[1290] RGPD, Cons. 68.
[1291] G29 », Lignes directrices relatives au droit à la portabilité des données, *Ibid.,* p. 19.
[1292] RGPD, Cons. 68 et Art. 20 §1.

en charge, grâce à l'échange de données entre leurs systèmes de TIC respectifs »[1293]. La description du format par les dispositions règlementaires, « structuré, couramment utilisé, lisible par machine », caractérise ainsi les exigences minimales en vue de faciliter l'interopérabilité des formats transmis et reçus. Et, selon le droit de l'Union, un format « lisible par machine » représente « *un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne* »[1294].

Dans ce contexte, les termes susvisés décrivant le format semblent apporter des précisions sur les moyens, « *[…] tandis que l'interopérabilité est le résultat escompté* » indique le G29[1295].

Au regard des précisions apportées par les dispositions du RGPD combinées aux définitions susmentionnées fournies par le droit de l'UE, le droit à la portabilité vise, *in fine*, à mettre en place des systèmes « interopérables » et non des systèmes techniquement « compatibles », d'autant que le manque d'interopérabilité constitue, comme il a été vu plus haut, une « entrave » à la transmission, pratique explicitement interdite par le RGPD.

§2. Les principes et valeurs numériques européens à visée mondiale

Ces principes et valeurs numériques européens visant à être appliqués mondialement, selon les aspirations des dispositions légales européennes, se composent principalement du consentement, de la licéité et de la transparence (A), mais aussi des principes de légalité, de nécessité et de proportionnalité (B).

[1293] Décision n° 922/2009/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant des solutions d'interopérabilité pour les administrations publiques européennes (ISA), Plus en vigueur (Date de fin de validité : 31/12/2015), Art. 2 point a) ; et, Glossaire de l'UE, « Interoperability » : https://eur-lex.europa.eu/eli-register/glossary.html?locale=fr

[1294] Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, Texte présentant de l'intérêt pour l'EEE, Art. 1er §2), point 6 ; et Cons. 21 qui précise « *Un document devrait être considéré comme présenté sous un format lisible par machine s'il se présente dans un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier et reconnaître des données spécifiques qu'il contient et les en extraire. Les données encodées présentes dans des fichiers qui sont structurés dans un format lisible par machine sont des données lisibles par machine. Les formats lisibles par machine peuvent être ouverts ou propriétaires ; il peut s'agir de normes formelles ou non. Les documents encodés dans un format de fichier qui limite le traitement automatique, en raison du fait que les données ne peuvent pas, ou ne peuvent pas facilement, être extraites de ces documents, ne devraient pas être considérés comme des documents dans des formats lisibles par machine. Les États membres devraient, le cas échéant, encourager l'utilisation de formats ouverts, lisibles par machine.* » ; Glossaire de l'UE, « Machine-readable », *Id. ;* et, Open Data Handbook Glossary, « Machine readable » : http://opendatahandbook.org/glossary/en/terms/machine-readable/

[1295] G29, Lignes directrices relatives au droit à la portabilité des données, *Ibid.,* p. 20.

A. Consentement, licéité et transparence

Le droit à l'information, composante des droits de la personne et des garanties appropriées, implique le principe du « consentement libre spécifique, éclairé et univoque », mais aussi le principe de transparence susmentionné[1296].

Le consentement, tel que défini et employé jusqu'à présent par la directive de 1995 et la directive vie privée et communications électroniques[1297], s'est transformé avec les nouvelles règlementations adoptées. Aux termes du RGPD, il représente une des six bases juridiques permettant un « traitement licite » des données à caractère personnel[1298]. En ce sens, le traitement n'est licite que si « la personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques »[1299]. Et le Règlement prévoit plusieurs dérogations au principe d'interdiction générale de « traitement portant sur des catégories particulières de données », qui comprend le cas où « *la personne concernée a donné son consentement explicite au traitement de ces données* »[1300]. Le concept du consentement joue ainsi un double rôle, similaire à ce qui était établi dans l'ancienne directive[1301] : il est employé comme condition générale de licéité du traitement et comme condition spécifique dans certains cas particuliers, permettant des traitements qui seraient autrement considérés illicites.

De façon générale, le consentement ne s'applique comme condition de licéité du traitement que si la personne dispose d'un contrôle effectif et d'une « véritable liberté de choix » en ce qui concerne l'acceptation ou le refus des conditions du traitement, y compris la possibilité de « refuser ou de retirer son consentement sans subir de préjudice »[1302]. Autrement dit, il doit être « *aussi simple de retirer que de donner son consentement* »[1303]. Par conséquent, si le consentement est retiré, toutes les activités de traitement fondées sur celui-ci, et ayant eu lieu

[1296] *Cf.* p. 198 et 205.
[1297] Directive 2002/58/CE du parlement européen et du conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), Art. 2 point f), 6 §§ 3 et 4, 9 §§ 1 et 2.
[1298] RGPD, Cons. 40 et 42 ; Art. 5 (Principes relatifs au traitement des données à caractère personnel), 6 (Licéité du traitement) et 7 (Conditions applicables au consentement).
[1299] RGPD, Art. 6 §1, point a).
[1300] RGPD, Art. 9 – Traitement portant sur des catégories particulières de données à caractère personnel, §1 « *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.* » et §2, point a).
[1301] Directive 95/46/CE, Art. 7 point a) et 8 §2, point a).
[1302] RGPD, Cons. 42 et Art. 7 §§ 2 et 3 ; Groupe de travail « Article 29 », Avis 15/2011 sur la définition du consentement, Adopté le 13 juillet 2011, 01197/11/FR WP 187, p. 14-15 et 37-38 ; et, Lignes directrices sur le consentement au sens du règlement 2016/679, Adoptées le 28 novembre 2017 - Version révisée et adoptée le 10 avril 2018, 17/FR WP259 rév.01, p. 24 à 26.
[1303] RGPD, Art. 7 §3.

avant son retrait, demeurent licites, conformément au Règlement, mais le responsable du traitement est, toutefois, tenu de cesser les traitements en question. Et lorsqu'il n'existe aucun autre fondement juridique au traitement, le responsable du traitement a « l'obligation d'effacer » les données « dans les meilleurs délais », sous réserve d'exceptions « dans la mesure où le traitement est nécessaire » dans certains cas particuliers[1304]. Si le consentement a été obtenu en respectant toutes les conditions et obligations énoncées par le Règlement, il représente un outil conférant aux individus un contrôle sur le ou les traitements potentiels de leurs données, mais, « dans le cas contraire, le contrôle de la personne concernée devient illusoire et le consentement ne constituera pas une base valable pour le traitement des données », rendant, *ipso facto*, l'activité de traitement illicite[1305].

Selon le RGPD, le consentement désigne *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »[1306]. Cette définition reste fidèle à celle fournie par l'ancienne directive, tout en introduisant un critère et des orientations supplémentaires dans la mesure où, avec les nouvelles dispositions du Règlement, le consentement doit être donné par un acte positif clair « par lequel la personne manifeste de façon libre, spécifique, éclairée et univoque son accord » au traitement des données la concernant, au moyen d'une « déclaration écrite » par exemple, « y compris par voie électronique », ou d'une « déclaration orale »[1307]. De plus, le RGPD souligne qu'il ne « *saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité* »[1308].

En outre, il apparaît désormais nécessaire de détailler le consentement en ce sens que, s'il est donné, il devrait valoir pour « toutes les activités de traitement ayant la ou les mêmes finalités » et lorsque le traitement envisage plusieurs finalités, « il devrait être donné pour l'ensemble d'entre elles »[1309]. La demande de consentement doit ainsi être présentée « sous une forme

[1304] RGPD, Art. 17 §1, point b) et §3, points a) à e).
[1305] G29, Avis 15/2011 sur la définition du consentement, *Id.*, p. 6 à 9 ; Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, Adopté le 9 avril 2014, 844/14/FR WP 217, p. 10 à 15 ; et, Lignes directrices sur le consentement au sens du règlement 2016/679, *Id.*, p. 3 à 5.
[1306] RGPD, Art. 4 point 11).
[1307] RGPD, Cons. 32 où le législateur souligne « *[…]. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. […].* »
[1308] RGPD, Cons. 32.
[1309] RGPD, Cons. 32 et Art. 9 §2.

compréhensible et aisément accessible », formulée en des termes « clairs et concis », et elle ne doit pas contenir de « clauses abusives » ou « inutilement perturber l'utilisation du service » pour lequel elle est accordée[1310], respectant *in fine* le principe de transparence. Ces exigences se trouvent encore plus justifiées compte tenu des dispositions du Règlement qui autorisent le responsable du traitement « *à effectuer un traitement ultérieur des données à caractère personnel indépendamment de la compatibilité des finalités* » lorsque, entre autres, la personne concernée a donné son consentement[1311].

Reconnaissant qu'il ne soit pas possible dans certains cas de « cerner entièrement la finalité du traitement », le Règlement charge le responsable du traitement d'être en mesure « de démontrer » que ladite personne a consenti valablement à l'opération de traitement, et des garanties devraient en particulier exister « afin de garantir que la personne concernée est consciente du consentement donné et de sa portée »[1312]. Cette charge de la preuve reflète et correspond, à la fois, au régime de responsabilité[1313] ainsi qu'aux principes de transparence et de licéité omniprésents dans les dispositions du RGPD.

Le consentement représente, *primo*, une manifestation de volonté libre impliquant une liberté de choix ainsi qu'un contrôle réel pour les personnes concernées. Et le Règlement fournit des précisions et des orientations afin de « garantir que le consentement est donné librement »[1314]. Ainsi, le consentement ne doit pas constituer « un fondement juridique valable » pour le traitement de données « dans un cas particulier lorsqu'il existe un déséquilibre manifeste » des rapports de force entre la personne concernée et le responsable du traitement, « *en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière* »[1315]. Le consentement, dans n'importe quelle situation, ne doit donc pas être forcé et émaner d'un déséquilibre de rapports manifeste, comme ça peut être le cas par exemple avec les autorités publiques ou les employeurs. Pour être valable, le consentement doit être donné par une personne qui est véritablement en mesure d'exercer un choix, et ce, en l'absence de risques de tromperie, d'intimidation, de coercition ou de conséquences négatives dans les cas

---

[1310] RGPD, Cons. 32, 42 (où il est fait référence à la directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs) et 58 qui dispose « *Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. […]* », et Art. 7 §2.
[1311] RGPD, Cons. 50.
[1312] RGPD, Cons. 33 et 42, et Art. 7 §1.
[1313] *Cf.* p. 232 et s.
[1314] RGPD, Cons. 43 et Art. 7 §4.
[1315] RGPD, Cons. 43.

où elle refuse de consentir. Autrement dit, « *le consentement ne sera pas libre lorsque tout élément de contrainte, de pression ou d'incapacité d'exercer un véritable choix sera présent* »[1316].

Par ailleurs, le RGPD indique que le consentement est « présumé ne pas avoir été donné librement » s'il est, entre autres, associé à l'acceptation de conditions générales, sans qu'un « consentement distinct » ne soit donné aux différentes opérations de traitement, « bien que cela soit approprié » dans certains cas, ou si « l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution »[1317]. En ce sens, ces dispositions aspirent à garantir que la finalité du traitement des données ne soit pas « dissimulée ou associée » à l'exécution d'un contrat ou à la fourniture d'un service pour lesquels le traitement de ces données, basé sur le consentement, n'est pas nécessaire[1318], témoignant par là même de l'importance du principe de transparence. Ces deux bases juridiques du traitement de données, précise le G29, « *à savoir le consentement et le contrat, ne peuvent pas être fusionnées et amalgamées* »[1319]. En effet, le choix du législateur de recourir à l'expression « tenir le plus grand compte » marque le caractère conditionnel de la liberté du consentement qui doit être prudemment évalué par le responsable du traitement, notamment si le contrat, y compris pour la fourniture d'un service, comprend une demande de consentement au traitement des données[1320].

En outre, un consentement libre implique, d'une part, la nécessité de détailler ce pourquoi le consentement est sollicité, puisque le Règlement souligne que « lorsque le traitement a plusieurs finalités, un consentement distinct devrait être donné pour l'ensemble d'entre elles »[1321] sous l'égide du principe de transparence qui vaut, notamment, « *pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les*

[1316] G29, Lignes directrices sur le consentement au sens du règlement 2016/679, *Id.*, p. 8.
[1317] RGPD, Cons. 43 et Art. 7 §4.
[1318] G29, Lignes directrices sur le consentement au sens du règlement 2016/679, *Id.*, p. 8 à 11, et, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, *Id.*, p. 18-19.
[1319] G29, Lignes directrices sur le consentement au sens du règlement 2016/679, *Ibid.*, p. 9.
[1320] RGPD, Art. 7 §4.
[1321] RGPD, Cons. 32 et 42.

concernant qui font l'objet d'un traitement »[1322]. D'autre part, cette liberté du consentement suppose de la part du responsable du traitement la faculté de démontrer qu'il est possible pour la personne concernée de refuser ou de retirer son consentement « sans subir de préjudice »[1323]. En effet, le consentement ne devrait pas être considéré comme ayant été donné librement, précise le législateur européen, « *si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* »[1324].

La nécessité susmentionnée de détailler les raisons pour lesquelles le consentement est sollicité, pour qu'il soit considéré comme « libre », est étroitement liée à l'exigence selon laquelle le consentement doit être, selon le RGPD, « *une manifestation de volonté spécifique* »[1325]. Et les dispositions portant sur la licéité du traitement des données viennent confirmer cette obligation, puisque le traitement n'est licite que si, *inter alia*, « la personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques »[1326]. Cette nécessité d'un consentement « spécifique » vise à fournir les mêmes garanties soulignées précédemment, à savoir garantir un certain degré de contrôle et de transparence pour les personnes concernées. Par conséquent, selon le G29, pour se conformer au caractère « spécifique » du consentement, le responsable du traitement doit garantir : la « spécification des finalités » en tant que garantie contre tout détournement d'usage[1327], le « caractère détaillé » des demandes de consentement, ainsi que la « séparation claire » des informations liées à l'obtention du consentement de celles liées à d'autres sujets[1328]. Cette optique a été confirmée par le Règlement qui précise que les « finalités spécifiques » du traitement des données devraient être « *explicites et légitimes, et déterminées lors de la collecte* » des données[1329].

[1322] RGPD, Cons. 39 qui dispose également que « *[…]. Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement. […].* »

[1323] RGPD, Cons. 42 et Art. 7 §§ 1 et 3.

[1324] RGPD, Cons. 42.

[1325] RGPD, Art. 4 point 11).

[1326] RGPD, Art. 6 §1, point a).

[1327] Groupe de travail « Article 29 », Opinion 03/2013 on purpose limitation, Adopté le 2 avril 2013, 00569/13/EN WP 203, p. 16 : « *For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'. […]*»

[1328] G29, Lignes directrices sur le consentement au sens du règlement 2016/679, *Id.*, p. 13-14 ; Et, RGPD, Cons. 32, 42, 43 et Art. 7.

[1329] RGPD, Cons. 39.

L'exigence d'un consentement spécifique, identique à celle imposée par l'ancienne directive de 1995[1330], est également fortement liée à la nécessité d'un consentement « *éclairé* ». Et pour que le consentement soit considéré comme « éclairé », indique le législateur européen, « la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel »[1331]. Intervient alors le droit à l'information dans la mesure où il est indispensable de fournir des informations aux personnes avant d'obtenir leur consentement, de manière à leur permettre de choisir et de décider en toute connaissance de cause, de comprendre clairement ce à quoi ils consentent, mais aussi d'exercer leur droit de refuser ou de retirer leur consentement, et ce, sans subir de conséquences négatives. Inversement, si le responsable du traitement ne fournit pas d'informations « aisément accessibles, faciles à comprendre et formulées en des termes clairs et simples », le contrôle de la personne concernée devient illusoire et le consentement ne sera pas considéré comme étant un fondement valable pour le traitement[1332]. Il en ressort ainsi que les dispositions du RGPD renforcent l'exigence selon laquelle le consentement doit être « une manifestation de volonté éclairée », l'un de ses principes fondamentaux étant, selon ces mêmes dispositions, le principe de transparence, étroitement lié pour sa part aux principes de loyauté et de licéité[1333]. En effet, « *le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées* »[1334].

Enfin, pour que le consentement soit valable, le RGPD exige « une manifestation de volonté univoque » à travers « une déclaration ou un acte positif clair »[1335]. Le consentement doit donc toujours être donné par une déclaration ou par un acte positif clair qui sous-entend, en ce qui concerne ce geste actif, que la personne concernée a effectué un « acte délibéré » pour consentir au traitement spécifique[1336]. Comme il a été précédemment indiqué, le silence, le recours à des

---

[1330] Directive 95/46/CE, Art. 2 point h) « *«consentement de la personne concernée»: toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*. »

[1331] RGPD, Cons. 42 et Art. 7 §2.

[1332] RGPD, Cons. 39 et 42 ; Art. 7 §§ 2 et 3.

[1333] RGPD, Cons. 39 et Art. 5 § 1, point a).

[1334] RGPD, Cons. 39.

[1335] RGPD, Art. 4 point 11).

[1336] G29, Lignes directrices sur le consentement au sens du règlement 2016/679, *Id.*, p. 18, et le groupe de travail cite le document de travail des services de la Commission, Analyse d'impact, Annexe 2, p. 20 et p. 105-106: « *Comme le souligne également l'avis du G29 sur le consentement, il semble essentiel de préciser que l'obtention d'un consentement valable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement, tout en expliquant que – dans le contexte de l'environnement en ligne – l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement*

cases cochées par défaut ou l'inactivité de l'individu, y compris le simple fait qu'elle continue à utiliser un service, ne manifestant pas un acte positif clair, ne peuvent *de jure* constituer un consentement valable[1337].

Dans certaines situations particulières, un consentement « explicite » est requis car le contexte dans lequel les données, « par nature particulièrement sensibles », sont traitées « pourrait engendrer des risques importants pour ces droits et libertés » et méritent, par conséquent, une « protection spécifique »[1338]. Ces données comprennent les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques ou biométriques, ainsi que les données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne[1339]. Aux termes du RGPD, « des dérogations à l'interdiction générale de traiter ces catégories particulières de donnés » sont explicitement prévues, « entre autres lorsque la personne concernée donne son consentement explicite »[1340]. Ainsi, selon le Règlement, le consentement « explicite » doit être recueilli dans le cadre d'un traitement portant sur des catégories particulières de données, mais aussi dans le contexte d'un transfert ou d'un ensemble de transfert de données vers des pays tiers ou des organisations internationales[1341], ainsi que dans le cadre d'une décision individuelle automatisée, y compris le profilage. En ce qui concerne cette dernière, le RGPD stipule que toute personne « *a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* »

(«consentement fondé sur le silence»), ne constitue pas, en soi, un consentement indubitable. Cela conférerait aux individus un plus grand contrôle sur leurs propres données lorsque le traitement est fondé sur leur consentement. Quant à l'incidence sur le responsable du traitement, celle-ci serait faible dès lors que cette mesure ne fait que clarifier et expliciter les implications de l'actuelle directive concernant les conditions d'un consentement valable de la part de la personne concernée. Dans la mesure où la notion de consentement «explicite» clarifierait – en remplaçant la notion de consentement «indubitable» – les modalités et la qualité du consentement et où elle ne vise pas à accroître le nombre de cas et de situations où le consentement (explicite) devrait être utilisé comme base du traitement, l'incidence de cette mesure sur les responsables du traitement ne devrait pas être majeure. » (Note de bas de p. n° 41).

[1337] RGPD, Cons. 32.

[1338] RGPD, Cons. 50.

[1339] RGPD, Cons. 50 et Art. 9 §1.

[1340] RGPD, Cons. 50 et Art. 9 §2 ; et, Loi Informatique et libertés, Art. 6.

[1341] RGPD, Cons. 111 et Art. 49 §1, point a) qui précisent qu'il y a lieu de prévoir la possibilité de transferts vers des pays ou organisations ne disposant pas d'un niveau adéquat de droit relatif à la protection des données lorsque la personne a donné son consentement explicite. Voir également, G29, Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, Adopté le 25 novembre 2005, 2093-01/05/FR WP 114, p. 13, où le G29 a indiqué que le recours au consentement pour les transferts de données périodiques ou permanents n'est pas approprié.

sauf lorsque celle-ci est, entre autres, « *fondée sur le consentement explicite de la personne concernée* »[1342].

Le consentement « explicite » semble donc se situer à un niveau supérieur de celui du consentement « valable », qui s'apparente plus à un niveau standard. Le terme « explicite », qui ne fait l'objet d'aucune définition ou précision particulière de la part du Règlement, se rapporte, selon le G29, à la manière dont le consentement est exprimé par la personne, impliquant ainsi que celle-ci formule une déclaration de consentement « exprès »[1343]. En ce sens, « *le consentement explicite couvre toutes les situations où il est proposé à une personne d'accepter ou de rejeter une utilisation particulière ou la divulgation des informations la concernant et qu'elle répond activement à la question, que ce soit oralement ou par écrit* »[1344]. En droit civil, le consentement « exprès » suppose le consentement de la personne « recueilli par écrit préalablement à la réalisation de l'opération en question, après qu'elle a été dûment informée de sa nature et de sa finalité. Le consentement mentionne la finalité de l'opération et est révocable sans forme et à tout moment »[1345].

Dès lors, de façon générale, un consentement explicite ou exprès désigne la manifestation de volonté de la personne donnée activement et expressément, après qu'elle ait dûment pris connaissance de la nature et des finalités du traitement envisagé. En tout état de cause, le responsable du traitement doit pouvoir démontrer qu'il a recueilli le consentement « explicite » des personnes concernées, préalablement à la collecte et au traitement de leurs données, sous peine de sanctions, tels que ce fut le cas, en France, pour certains sites de rencontres[1346].

[1342] RGPD, Art. 22 §1 et §2, point c) ; et, Cons. 71 qui précise que « *La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision, qui peut comprendre une mesure, impliquant l'évaluation de certains aspects personnels la concernant, qui est prise sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques la concernant ou qui, de façon similaire, l'affecte de manière significative, tels que le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine. Ce type de traitement inclut le «profilage» qui consiste en toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative. Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise [...] si la personne concernée a donné son consentement explicite. [...]* »

[1343] Formule employée par la Loi Informatique et libertés dans sa dernière version, préférée au terme « explicite » employé par le RGPD ; voir, par exemple, Art. 75 de la loi précitée.

[1344] Groupe de travail « Article 29 », Avis 15/2011 sur la définition du consentement, *loc. cit.*, p. 28 ; et, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 20-21.

[1345] Par ex., Art. 16-10, 16-11, 16-14, 73, ou 96-1 du Code civil.

[1346] CNIL, Délibération de la formation restreinte n°2016-405 du 15 décembre 2016 prononçant une sanction pécuniaire à l'encontre de la société X, et Délibération de la formation restreinte n°2016-406 du 15 décembre 2016 prononçant une sanction pécuniaire à l'encontre de la société X, où elle a considéré que la fusion de différentes informations « *au sein d'une unique case à cocher ne permettait pas de conférer au consentement des utilisateurs un caractère exprès* », que le consentement exprès « *doit être libre, informé et spécifique* » et

En règle générale, le Règlement dispose clairement que « *pour être licite, le traitement de données à caractère personnel devrait être fondé sur le consentement de la personne concernée ou reposer sur tout autre fondement légitime prévu par la loi, [...]* »[1347]. Le consentement joue un rôle essentiel en matière de traitement, en particulier du point de vue des droits et libertés fondamentales, conférant un véritable pouvoir de contrôle aux individus. Il doit donc être encadré par des conditions strictes, en raison même du fait qu'en accordant son consentement à un traitement de ses données, une personne pourrait renoncer à un droit fondamental. L'importance du rôle joué par le consentement est, en outre, soulignée par la Charte des droits fondamentaux qui affirme que les données personnelles, dont la protection est légalement assurée à toute personne, « doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi »[1348]. De plus, le consentement, dans sa version réformée, influe les nouvelles législations, tel que ce fut le cas principalement avec la proposition de règlement vie privée et communications électroniques destiné à abroger la directive de 2002 du même nom et à « compléter et préciser le RGPD », et dans laquelle il est précisé que la définition et les conditions du consentement figurant dans le RGPD s'appliquent[1349]. Comme il a été précédemment vu, le consentement est intimement associé à la notion de libre choix relative au droit à l'information, et, selon le G29, « *l'autonomie de la personne concernée est à la fois une condition préalable et une conséquence du consentement* »[1350]. Il est cependant important de rappeler que l'obtention d'un consentement valable et/ou explicite n'exonère aucunement le

souligne que « *le consentement est exprès dès lors que la personne concernée est en mesure de manifester par une action positive, son assentiment au traitement de ses données sensibles, attestant ainsi que son consentement est donné en toute connaissance de cause. En effet, afin de consentir, la personne concernée doit être pleinement éclairée sur le caractère sensible des données qu'elle renseigne, notamment en ce que celles-ci peuvent révéler leur appartenance à une communauté ou permettre qu'elles fassent l'objet d'un profilage. [...]* », disponibles en ligne :
https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000033738199&fastReqId=1859587492&fastPos=3 &
https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000033738124&fastReqId=610498006&fastPos=2

[1347] RGPD, Cons. 40 ; et Loi Informatique et libertés, Art. 5 (Modifié par l'ordonnance du 12 décembre 2018) « *Le traitement, lorsqu'il relève du titre II, a reçu le consentement de la personne concernée, dans les conditions mentionnées au 11 de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du 27 avril 2016 précédemment mentionné* ; ».

[1348] Charte des droits fondamentaux de l'Union Européenne, Art. 8 §§ 1 et 2, et Art. 7.

[1349] Proposition de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM/2017/010 final - 2017/03 (COD), Art. 9 – Consentement « *1. La définition et les conditions du consentement figurant à l'article 4, paragraphe 11, et à l'article 7 du règlement (UE) 2016/679/UE s'appliquent.* »

[1350] G29, Avis 15/2011 sur la définition du consentement, *Id.*, p. 9.

responsable du traitement de sa responsabilité, ni ne diminue ou ne supprime ses autres obligations, notamment celles relatives aux traitements, à savoir la loyauté, la nécessité, la proportionnalité ainsi que la qualité des données, et ne légitime pas un traitement qui aurait été autrement considéré comme illicite, en vertu des dispositions du Règlement[1351]. Ainsi, précise le G29, « *même si le traitement des données à caractère personnel a reçu le consentement de la personne concernée, cela ne justifie pas la collecte de données excessives au regard d'une finalité spécifique de traitement, ce qui serait foncièrement abusif* »[1352].

Le concept de consentement, tel qu'il a été réformé par le RGPD, caractérise ainsi, à la fois, un pouvoir et une liberté fondamentale pour les individus tout en impliquant de nombreux autres principes, en vue d'accorder une protection efficace aux personnes et des moyens pour développer et construire, de manière libre et éclairée, leur identité en ligne. Néanmoins, compte tenu des évolutions en matière de data et de nouvelles technologies, mais aussi en matière de stratégie pour des objectifs de marketing et de surveillance, il est utile de se demander si ce concept, et les droits et principes associés, ne sont pas en quelque sorte dépassés, n'assurant plus, de façon pragmatique, une protection concrète.

Autrement dit, « *these trends may require us to look closely at the notice and consent framework that has been a central pillar of how privacy practices have been organized for more than four decades. In a technological context of structural over-collection, in which re-identification is becoming more powerful than de-identification, focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy. In the words of the President's Council of Advisors for Science & Technology, "The notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data"* »[1353].

B. Légalité, nécessité et proportionnalité

Les principes de légalité, de nécessité et de proportionnalité ont été largement mis en évidence dans de nombreuses dispositions et situations à travers le temps, tel qu'il a pu être observé dans cette analyse[1354], et se retrouvent amplement omniprésents dans le RGPD. Comme il a été précédemment vu, le droit au respect de la vie privée fait l'objet de larges interprétations,

[1351] RGPD, Cons. 40, 78 et 156, Art. 5 et 35 §7.
[1352] G29, Lignes directrices sur le consentement au sens du règlement 2016/679, *Id.*, p. 4.
[1353] Executive Office of the President, "Big data: Seizing opportunities, preserving values", The White House, Washington, May 2014, p. 54; disponible en ligne: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
[1354] *Cf.* p. 79 et s., 168, 174, 190, 198, 288 et s.

s'étalant et se propageant progressivement avec les avancées technologiques et sociétales, et suppose qu'il « *ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* »[1355]. Selon le droit de l'Union, toute limitation ou atteinte à la vie privée doit être prévue par la loi, qui, à son tour, doit être nécessaire au regard des objectifs poursuivis, conformément au principe de proportionnalité[1356]. Le Règlement européen prévoit ainsi la « *possibilité pour les États membres, sous certaines conditions, de limiter par la loi certaines obligations et certains droits lorsque cette limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir des intérêts spécifiques importants [...]* »[1357].

Le principe de légalité suppose que toute limitation au droit à la vie privée doit être expressément « prévue par la loi », mêlant, de la sorte, le principe de transparence. En effet, la Cour européenne des droits de l'homme a plusieurs fois rappelé que « les mots « prévue par la loi » impliquent des conditions qui vont au-delà de l'existence d'une base légale en droit interne, visant aussi la qualité de la loi, et exigent que celle-ci soit « accessible » et « prévisible » »[1358]. Reconnaissant l'importance du principe de légalité, la Cour est, néanmoins, peu disposée à admettre des réclamations formelles stipulant que la loi nationale à elle toute seule, justifie l'ingérence envisagée, puisque « *l'expression « prévue par la loi » non seulement impose le respect du droit interne, mais concerne aussi la qualité de la loi, celle-ci devant être compatible avec le principe de la prééminence du droit* »[1359]. Et la Cour a, depuis 1984, précisé que ce principe implique que le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par la Convention et, en conséquence,

---

[1355] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Art. 8 §2.

[1356] Charte des droits fondamentaux de l'UE, Art. 52 §1 « *Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.* »

[1357] RGPD, Cons. 19 qui fournit des exemples de ces intérêts spécifiques importants « *[...]tels que la sécurité publique, ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cela est pertinent, par exemple, dans le cadre de la lutte contre le blanchiment d'argent ou des activités des laboratoires de police scientifique.* »

[1358] CEDH, Affaire Amann c. Suisse, *loc. cit.,* §§ 50 et 55 ; Affaire Kopp c. Suisse, du 25 mars 1998, requête n° 23224/94, §55.

[1359] CEDH (Grande Ch.), Affaire Bykov c. Russie du 10 mars 2009, requête n° 4378/02, §76.

la loi doit définir l'étendue et les modalités d'exercice d'une telle ingérence « *avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire* »[1360].

Des intrusions dans l'exercice des droits et libertés fondamentales peuvent donc avoir lieu, si elles sont prévues par des lois respectant les principes juridiques et interprétations jurisprudentielles en la matière, et si elles poursuivent un but légitime, à l'exemple de ceux mentionnés par la Convention de sauvegarde, la Charte des droits fondamentaux ou, désormais, le RGPD. Toutefois, bien que cela soit admis par les Cours européennes (CEDH et CJUE), cela n'est, en général, pas suffisant pour éviter une condamnation ; l'intérêt légitime étant une des conditions qui doit être dûment remplie et mise en balance avec les droits et libertés des personnes.

L'ingérence prévue par la loi doit ainsi être nécessaire dans une société démocratique, proportionnée à l'intérêt spécifique poursuivi pour justifier une telle ingérence, et comprendre des garanties et protections pour les personnes concernées. En d'autres termes, « *dans tous les systèmes juridiques des États membres, les interventions de la puissance publique dans la sphère d'activité privée de toute personne, qu'elle soit physique ou morale, doivent avoir un fondement légal et être justifiées par les raisons prévues par la loi et que ces systèmes prévoient, en conséquence, bien qu'avec des modalités différentes, une protection face à des interventions qui seraient arbitraires ou disproportionnées. L'exigence d'une telle protection doit donc être reconnue comme un principe général du droit communautaire* »[1361].

En vertu de ces principes clés en la matière, une intrusion ou une atteinte aux droits et libertés des personnes, notamment à leurs droits au respect de leurs vies privées, est autorisée dans la mesure où elle est proportionnée et « *reflète un juste équilibre entre les intérêts publics et privés en concurrence* »[1362]. Le principe de proportionnalité réclame alors une étude d'impact, et la recherche d'un juste équilibre entre l'atteinte au droit à la vie privée et les bénéfices pouvant être accomplis ou engendrés moyennant une telle ingérence. En ce sens, le RGPD stipule que l'analyse d'impact à la charge des responsables du traitement[1363] doit contenir au moins « *une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des*

[1360] CEDH, (Cour Plénière), Affaire Malone c. Royaume-Uni du 2 août 1984, requête n° 8691/79, §§ 67 et 68.
[1361] CJCE, Affaire Hoechst c. Commission du 21 septembre 1989, affaires jointes 46/87 et 227/88, §19.
[1362] CEDH (Grande Ch.), Affaire S. et Marper c. Royaume-Uni du 4 décembre 2008, Requêtes nos 30562/04 et 30566/04, §118.
[1363] *Cf.* p. 243.

finalités »[1364]. Ce critère de balance adéquate des intérêts en cause a été à maintes reprises souligné et élargi par la jurisprudence européenne, précisément au regard de la spécificité et de la pertinence de la mesure en cause. Selon les juges, « *une ingérence est considérée comme « nécessaire dans une société démocratique » pour atteindre un but légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants »* »[1365]. Dès lors, une mesure présentant un caractère général et indifférencié ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et outrepasserait toute marge d'appréciation nationale acceptable en la matière, la rendant, *de facto* et *de jure*, disproportionnée, ne pouvant être qualifiée de nécessaire dans une société démocratique.

En outre, la mesure prévoyant l'ingérence doit également comporter des garanties adéquates et effectives contre les atteintes prévues, offrant en conséquence une protection adéquate et réelle aux personnes concernées. Les juges européens insistent sur la nécessité de vérifier l'existence réelle et concrète de telles garanties, et n'hésitent pas à affirmer que « *faute de règles spécifiques et détaillées, le recours à* [la mesure en cause] *n'était pas entouré de garanties adéquates contre les divers abus possibles. Dès lors, sa mise en œuvre était susceptible d'arbitraire et incompatible avec la condition de légalité* »[1366], jugeant l'ingérence opérée illégale et injustifiée. Le nouveau RGPD, déclarant respecter les principes et les exigences européennes en la matière, indique que « des limitations à certains principes spécifiques ainsi qu'au droit à l'information, au droit d'accès aux données à caractère personnel, au droit de rectification ou d'effacement de ces données, au droit à la portabilité des données, au droit d'opposition, aux décisions fondées sur le profilage, ainsi qu'à la communication d'une violation de données à caractère personnel à une personne concernée et à certaines obligations connexes des responsables du traitement, peuvent être imposées par le droit de l'Union ou le droit d'un État membre, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux, et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique » pour garantir des intérêts publics importants[1367]. De plus, il précise la nécessité de respecter les

[1364] RGPD, Art. 35 §7, point b).
[1365] CEDH (Grande Ch.), Affaire S. et Marper c. Royaume-Uni du 4 décembre 2008, Requêtes n[os] 30562/04 et 30566/04, §101.
[1366] CEDH, Affaire Bykov c. Russie, *Id.*, §81.
[1367] RGPD, Cons. 73, tels que « *[…] pour garantir la sécurité publique, y compris la protection de la vie humaine, particulièrement en réponse à des catastrophes d'origine naturelle ou humaine, la prévention des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ou de manquements à la déontologie des professions règlementées, et pour garantir d'autres objectifs d'intérêt public importants de*

exigences énoncées par la Charte et la Convention européenne des droits de l'homme, et de mettre en place des mesures prévoyant des conditions spécifiques et des garanties adéquates qui « *peuvent comporter des procédures spécifiques permettant aux personnes concernées d'exercer ces droits si cela est approprié eu égard aux finalités du traitement spécifique concerné, ainsi que des mesures techniques et organisationnelles visant à réduire à un minimum le traitement des données à caractère personnel conformément aux principes de proportionnalité et de nécessité* »[1368].

Sous l'égide de ces principes et de leurs interprétations larges, ont alors émergés, à travers les dispositions du RGPD, des principes visant à assurer un niveau de protection supérieur des données et donc, *in fine*, des personnes. Ainsi, le Règlement exige que la collecte des données personnelles s'opère pour « des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités », sous certaines réserves, imposant, désormais, un principe de « limitation des finalités »[1369]. Le Règlement affirme, par ailleurs, que les données doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire*

---

l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, la tenue de registres publics conservés pour des motifs d'intérêt public général, le traitement ultérieur de données à caractère personnel archivées pour fournir des informations spécifiques relatives au comportement politique dans le cadre des régimes des anciens États totalitaires ou la protection de la personne concernée ou des droits et libertés d'autrui, y compris la protection sociale, la santé publique et les finalités humanitaires. Il y a lieu que ces limitations respectent les exigences énoncées par la Charte et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales », et Art. 23 §1 « *[...]pour garantir :*
a) la sécurité nationale ;
b) la défense nationale ;
c) la sécurité publique ;
d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ;
f) la protection de l'indépendance de la justice et des procédures judiciaires ;
g) la prévention et la détection de manquements à la déontologie des professions règlementées, ainsi que les enquêtes et les poursuites en la matière ;
h) une mission de contrôle, d'inspection ou de règlementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g) ;
i) la protection de la personne concernée ou des droits et libertés d'autrui ;
j) l'exécution des demandes de droit civil. »

[1368] RGPD, Cons. 156.

[1369] RGPD, Art. 5 §1, point b) qui précise que « *[...]le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales* ».

au regard des finalités pour lesquelles elles sont traitées » édictant un principe de « minimisation des données »[1370].

De même, en ce qui concerne la licéité du traitement, le RGPD prévoit certaines conditions où il est « nécessaire » d'effectuer un traitement : soit pour respecter « une obligation légale », ou pour « l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement », ou encore pour la réalisation des « intérêts légitimes poursuivis », « *à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel* » précise néanmoins le législateur[1371]. Celui-ci relève que le fondement de certains de ces traitements est défini par le droit de l'Union ou le droit d'un État membre, et souligne que chacun de ces droits répond à « *un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi* »[1372]. Et concernant les traitements portant sur des catégories particulières de données généralement interdits, le Règlement met en place des dérogations à ce principe, dont le traitement « *nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* »[1373].

En outre, une nouvelle obligation est mise à la charge du responsable du traitement : le devoir de mettre en place, « *tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même* », des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, destinées à mettre en œuvre les principes relatifs à la protection des données, comme celui de la minimisation des données, de façon effective, ainsi que le devoir d'assortir le traitement de « garanties nécessaires afin de répondre aux exigences du présent Règlement et de protéger les droits de la personne concernée »[1374]. Émerge alors le principe de protection des données dès la conception et celui de protection des données par défaut, grande nouveauté du RGPD, plus communément connu comme « *Privacy by design* » et « *Privacy by default* ». La « protection des données par défaut » est le principe selon lequel le responsable du traitement met en œuvre des mesures appropriées garantissant que, par défaut, « seules les données strictement nécessaires au regard de chaque finalité spécifique » sont

[1370] RGPD, Art. 5 §1, point c).
[1371] RGPD, Art. 6 §1, points c), e) et f).
[1372] RGPD, Art. 6 §3.
[1373] RGPD, Art. 9 §2, point g).
[1374] RGPD, Art. 25 §1.

traitées, et ce sans l'intervention de la personne concernée[1375]. Et la « protection des données dès la conception » désigne le principe qui vise à intégrer la protection des données ainsi que le respect de la vie privée dans la conception même des opérations de traitement et des systèmes d'information, en vue de respecter les principes de protection des données.

En conséquence, les responsables du traitement sont tenus de prendre en compte la protection des droits des personnes, « tant avant que pendant leurs activités de traitement », en mettant en œuvre des mesures techniques et organisationnelles appropriées afin de satisfaire aux principes et obligations de protection des données[1376]. Cela s'applique « à la quantité de données collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité », mais surtout, précise le législateur européen, « *ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée* »[1377].

Cela dit, une mise en œuvre effective du principe, désormais légal, de protection des données dès la conception et par défaut caractérise une « étape clé nécessaire quoiqu'insuffisante » vers une technologie responsable et une gouvernance des données au service de l'humanité, nous apprend l'ancien CEPD, et devrait être inscrite dans le cadre du concept plus large de « *Ethics by design* »[1378].

Ces principes sont, pour la plupart, repris par la directive européenne 2016/680 relative à la protection des personnes à l'égard du traitement des données par les autorités compétentes à des fins de prévention de de détection d'infractions pénales[1379] et par la directive 2016/681 relative à l'utilisation des données des dossiers passagers (PNR)[1380]. Les deux déclarent respecter, en particulier, les principes de nécessité et de proportionnalité, la première, reprenant les termes exacts du RGPD, annonce ainsi que « *[…] toute mesure devrait être appropriée, nécessaire et proportionnée en vue de garantir le respect de la présente directive, compte tenu*

[1375] RGPD, Art. 25 §2, et CEPD, « Protection des données par défaut » : https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_fr

[1376] RGPD, Art. 25 §2, et CEPD, « Protection des données dès la conception » : https://edps.europa.eu/data-protection/our-work/subjects/privacy-design_fr

[1377] RGPD, Art. 25 §2.

[1378] G. BUTTARELLI, Speech on "Privacy by design - Privacy engineering" given at the 11th International Computers, Privacy and Data Protection Conference (CPDP), EDPS side event, 25 January 2018, p. 3; disponible en ligne: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/privacy-design-privacy-engineering_en

[1379] Directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[1380] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

des circonstances de l'espèce, respecter le droit de chacun à être entendu avant que ne soit prise toute mesure individuelle susceptible d'affecter défavorablement la personne concernée et éviter les coûts superflus ainsi que les désagréments excessifs pour la personne concernée. [...] »[1381] ; et la seconde dispose, pour sa part, qu' « *en tenant pleinement compte des principes mis en évidence par la récente jurisprudence pertinente de la Cour de justice de l'Union européenne/CJUE, l'application de la présente directive devrait garantir le plein respect des droits fondamentaux et du droit au respect de la vie privée ainsi que du principe de proportionnalité. Elle devrait aussi véritablement remplir les objectifs de nécessité et de proportionnalité afin de répondre aux intérêts généraux reconnus par l'Union et à la nécessité de protéger les droits et libertés d'autrui dans la lutte contre les infractions terroristes et les formes graves de criminalité. [...]* »[1382].

Cependant, chacune prévoit dans ses dispositions certains des principes découlant des principes de légalité, de nécessité et de proportionnalité, mais pas tous : ainsi, la directive police-justice conçoit, notamment, la protection des données dès la conception et par défaut[1383], un faux semblant du principe de minimisation des données[1384], ainsi que le principe de limitation de finalité[1385] ; et, en ce qui concerne la licéité, elle indique simplement que la disposition nationale réglementant le traitement relevant de son champ d'application « *précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement* »[1386].

Quant à la directive PNR, outre les principes de nécessité et de proportionnalité, elle ne prévoit que, d'une part, des règles en matière de durée de conservation des données recueillies, analysées et traitées, disposant que les données PNR « *ne devraient être conservées que pour la durée nécessaire et proportionnée aux objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière* », une durée fixée à 5 ans, tout en précisant que « *pour éviter toute utilisation*

[1381] Directive 2016/680 police-justice, Cons. 82 ; RGPD, Cons. 129 « *[...]. Toute mesure devrait notamment être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, compte tenu des circonstances de l'espèce, respecter le droit de chacun à être entendu avant que soit prise toute mesure individuelle susceptible de lui porter atteinte et éviter les coûts superflus ainsi que les désagréments excessifs pour les personnes concernées. [...]* ».

[1382] Directive 2016/681 PNR, Cons. 22.

[1383] Directive 2016/680 police-justice, Art. 20.

[1384] Directive 2016/680 police-justice, Art. 4 §1, point c) « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;* », le RGPD employant la formulation suivante, plus précise, Art. 5 §1, point c) « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;* »

[1385] Directive 2016/680 police-justice, Art. 4 §1, point b) « *collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ;* ».

[1386] Directive 2016/680 police-justice, Art. 8 §2.

disproportionnée, il convient que, après le délai initial de conservation, les données PNR soient dépersonnalisées par le masquage d'éléments des données. »[1387]. Et, d'autre part, elle met en place la protection des données à caractère personnel en prévoyant que pour tout traitement de données effectué dans le cadre de son champ d'application, chaque État membre veille à ce que chaque passager dispose « *du même droit à la protection de ses données, des mêmes droits d'accès, de rectification, d'effacement et de limitation, et droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union et le droit national [...]*»[1388].

S'agissant des limitations de finalité, la directive précise certes que les données PNR recueillies ne « *peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière* » [1389], mais définit les infractions terroristes comme désignant les « *infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI* »[1390], et énumère une liste d'infractions « relativement vaste et étendue » comportant 26 infractions différentes[1391]. En outre, la directive PNR fixe la durée de conservation des données pour une période de 5 ans sans toutefois opérer « une quelconque distinction entre les catégories de données » en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou « selon les personnes concernées », et sans qu'il ne soit précisé que « la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire », ne respectant pas, dès lors, les exigences de la Cour de justice[1392]. À ce titre, celle-ci a déclaré que l'accord sur le transfert des données des dossiers passagers, prévu entre l'Union et le Canada, « ne peut pas être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union »[1393].

[1387] Directive 2016/681 PNR, Cons. 25 et Art. 12 ; et l'Art. 3 point 10) définit l'expression « dépersonnaliser par le masquage d'éléments des données » comme le fait de « *rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée.* »

[1388] Directive 2016/681 PNR, Art. 13 §1.

[1389] Directive 2016/681 PNR, Art. 1er §2.

[1390] Directive 2016/681 PNR, Art. 3 point 8) et Décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (2002/475/JAI) – abrogé (date de fin de validité : 19/04/2017) ; et Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil.

[1391] Directive 2016/681 PNR, Art. 3 point 9) « *«formes graves de criminalité», les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre ;* », et FRA European Union Agency For Fundamental Rights, Fundamental Rights Report 2017, Chapter 6 – Information society, Privacy and Data protection, p. 159 : https://fra.europa.eu/en/publication/2017/fundamental-rights-report-2017

[1392] CJUE, Affaire Digital Rights Ireland, *loc. cit.,* §§ 63 et 64.

[1393] CJUE, Avis de la Cour (Grande Ch.), Accord PNR UE-Canada, Avis 1/15 du 26 juillet 2017, Communiqué de Presse n° 84/17, p. 1.

En effet, la Cour observe dans son avis que, prises ensembles, les données PNR peuvent révéler, entre autres, plusieurs informations privées, intimes et personnelles sur les personnes, « voire fournir des informations sensibles sur ces passagers », et que ces données transférées sont « destinées à être analysées de manière systématique » avant l'arrivée des passagers par des moyens automatisés qui sont susceptibles de « fournir des informations supplémentaires sur la vie privée des passagers »[1394]. Elle note enfin que la durée de conservation des données pouvant aller jusqu'à 5 ans, « cet accord permet de disposer d'informations sur la vie privée des passagers sur une durée particulièrement longue », et conclut que le « transfert des données PNR de l'Union vers le Canada ainsi que les règles de l'accord envisagé sur la conservation des données, leur utilisation et leur éventuel transfert ultérieur comportent une ingérence dans le droit fondamental au respect de la vie privée, ainsi qu'une ingérence dans le droit fondamental à la protection des données à caractère personnel »[1395].
Par ailleurs, la Cour souligne que même si les ingérences en cause peuvent être justifiées par la poursuite d'un objectif d'intérêt général, « *plusieurs dispositions de l'accord ne sont pas limitées au strict nécessaire et ne prévoient pas des règles claires et précises* »[1396]. Il est donc fort probable que la Cour adopte une conclusion similaire si la directive PNR nouvellement entrée en vigueur (2018) fait l'objet de contestation.

Tout va finalement dépendre de la manière dont les États membres vont procéder à sa transposition. Dans le cas de la France, la loi renforçant la sécurité intérieure et la lutte contre le terrorisme[1397] a modifié, entre autres, des dispositions du Code de la sécurité intérieure pour pérenniser le dispositif API-PNR[1398] et transposer la directive PNR ; un décret a été, en plus,

---

[1394] CJUE, Avis 1/15 - Accord PNR UE-Canada, *Id.,* où la Cour précise que « *les données PNR peuvent, entre autres, révéler un itinéraire de voyage complet, des habitudes de voyage, des relations existant entre deux ou plusieurs personnes ainsi que des informations sur la situation financière des passagers aériens, leurs habitudes alimentaires ou leur état de santé, voire fournir des informations sensibles sur ces passagers* ».
[1395] CJUE, Avis 1/15 - Accord PNR UE-Canada, *Id.,* p. 1.
[1396] CJUE, Avis 1/15 - Accord PNR UE-Canada, *Ibid.,* p. 2.
[1397] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.
[1398] Les données PNR, définies à l'Art. 3 point 5) de la directive PNR comme « *«dossier(s) passager(s)» ou «PNR», un dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs (utilisés pour contrôler les passagers lors de l'embarquement) ou des systèmes équivalents offrant les mêmes fonctionnalités;* », se distinguent des informations préalables sur les passagers (Advance Passenger Information – API) qui désignent « *toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée)* » : directive 2016/681 PNR, Annexe I – Données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens –

adopté afin de finaliser sa transposition et redéfinir les conditions de mise en œuvre du dispositif API-PNR[1399]. Des dispositions du Code de la sécurité intérieure définissent ainsi les finalités du système API-PNR français[1400], autorisant plusieurs ministres à mettre en œuvre des traitements de données « *pour les besoins de la prévention et de la constatation de certaines infractions ainsi que de la recherche de leurs auteurs* » ; les infractions concernées étant « les actes de terrorisme, les atteintes aux intérêts fondamentaux de la nation ainsi que les infractions mentionnées à l'annexe II de la directive PNR »[1401].

Ces nouvelles dispositions procèdent donc à un renvoi à l'annexe de la directive PNR transposée, qui énumère vingt-six infractions ou catégories d'infractions, parmi lesquelles figurent « la participation à une organisation criminelle, la traite des êtres humains, la corruption, la fraude, le trafic de stupéfiants ou d'armes ou d'organes, les infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées, l'aide à l'entrée et au séjour irréguliers, la cybercriminalité, les meurtres, coups et blessures graves, le trafic de substances hormonales, le viol, l'enlèvement y compris la séquestration et la prise d'otages, la contrefaçon, le sabotage ou encore l'espionnage industriel »[1402]. Les finalités ainsi définies demeurent plus larges que celles découlant de la directive PNR, « *puisque le dispositif API-PNR France conserve une finalité de prévention des atteintes aux intérêts fondamentaux de la nation, non couverte par la directive précitée* »[1403].

Par ailleurs, prenant acte des indications et facultés fournies par la directive PNR[1404], le système désormais mis en place dispose aussi d'un champ d'application plus large que celui imposé par la directive PNR, étant donné qu'il ne concerne pas uniquement les transporteurs aériens, mais également les « agences de voyage et opérateurs de voyage ou de séjour affrétant tout ou partie

---

point 18, et Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (dite directive API), Art. 3 §2.

[1399] Décret n° 2018-714 du 3 août 2018 relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire), JORF n°0181 du 8 août 2018 (texte n° 2).

[1400] Code de la sécurité intérieure, Livre II, Titre III, Chapitre II : Traitements automatisés de données recueillies à l'occasion de déplacements internationaux – Art. L. 232-1 à L. 232-8.

[1401] Code de la sécurité intérieure, Art. L. 232-7 (Modifié par la loi du 30 octobre 2017) §I, 1er al. qui cite « *le ministre de l'intérieur, le ministre de la défense, le ministre chargé des transports et le ministre chargé des douanes* » comme ceux autorisés à mettre en œuvre un traitement automatisé de données à caractère personnel.

[1402] Directive 2016/681 PNR, Annexe II – Liste des infractions visées à l'article 3, point 9).

[1403] CNIL, Délibération n° 2018-259 du 14 juin 2018 portant avis sur un projet de décret relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire) (demande d'avis n° 18006270), JORF n°0181 du 8 août 2018, texte n° 124.

[1404] Directive PNR, Cons. 33 « *La présente directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne, sous réserve que ce droit national respecte le droit de l'Union* ».

d'un aéronef »[1405]. À ce titre, les ministres susmentionnés peuvent demander à ces agences et opérateurs de voyage ou de séjour « *de transmettre les données relatives aux passagers enregistrées dans leurs systèmes de réservation* », donc des données PNR[1406].

Il en ressort ainsi que les principes de légalité, de nécessité et de proportionnalité mis en œuvre et largement interprétés par la jurisprudence et certaines dispositions légales ont la capacité de subir de nombreuses dérogations et limitations, remettant conséquemment en cause les interprétations et les aspirations légales et jurisprudentielles en matière de protection des individus, de leurs vies privées, et de leurs données personnelles, et donc de leurs identités. Les anciens députés l'avaient en quelque sorte perçu en annonçant, déjà à l'époque de la rédaction du projet de loi Informatique et libertés, qu' « *il apparaît donc que, dans son état actuel, le projet est incapable de prévenir les abus. Même s'il contient des dispositions intéressantes — fichiers de tous les traitements informatisés, critères de collectes, droit d'accès, sanctions pénales — celles-ci ne permettent pas de garantir les libertés. […] on ne s'occupe jamais trop de la liberté. La liberté est toujours un sujet neuf. La liberté est toujours fragile*. »[1407].

[1405] Code de la sécurité intérieure, Art. L. 232-7 §§ II, III, V et VI.
[1406] Code de la sécurité intérieure, Art. L. 232-7 § II, 3ème al., et CNIL, Délibération du 14 juin 2018 portant avis sur un projet de décret relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure, *Id.*
[1407] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*, p. 5787.

Transition

Compte tenu des développements (théorico-juridiques) précédents, notamment la définition large et non exhaustive du concept d'identité, de celui de vie privée ou de celui de données à caractère personnel, ainsi que des nouvelles dispositions légales visant la protection de l'individu, ses données, ses représentations et perceptions, sa liberté de se construire et de se développer, *in fine*, son identité, physique et/ou numérique, il semble raisonnable d'examiner, dans un second temps, les diverses applications et utilisations technologiques pragmatiquement opérées, pouvant éventuellement porter atteinte à l'ensemble des droits et libertés susmentionnés. Un corpus juridique mettant en œuvre une protection assez large et de multiples conditions et obligations en matière de protection des données et des personnes est ainsi prévu, « *mais qui affirmerait sérieusement que le droit tiendra bon devant des circonstances qui rendraient possibles le dispositif que propose Black Mirror*[1408] ? »[1409].

En dépit des règles et mesures de protection adoptées, leur applicabilité et leur respect dépendent, *in concreto*, d'un domaine qui est essentiellement régi par le code informatique et les normes et dispositifs techniques, ainsi que par les intentions et aspirations de leurs créateurs et utilisateurs ; domaine qui, de surcroît, ne connaît ni frontière, ni espace délimité, ayant développé son propre espace, le cyberespace. Il est important de noter que « *algorithms are not immune from the fundamental problem of discrimination, in which negative and baseless assumptions congeal into prejudice. They are programmed by human beings, whose values are embedded into their software. And they must often use data laced with all-too-human prejudice* »[1410].

Les applications et usages des nouvelles technologies étant principalement d'ordre commercial ou gouvernemental, elles tendent, *de facto*, à porter une atteinte multidirectionnelle aux droits et libertés des individus ; ces multiples applications numériques s'avérant publiques ou privées, voire publiques et privées, comme les développements ci-dessous le montrent. En effet, « *it's*

[1408] En référence à la série télévisée **Black Mirror** qui « *est une anthologie télévisée britannique, créée par Charlie Brooker. […]. Les épisodes sont liés par le thème commun de la mise en œuvre d'une technologie dystopique. Le titre « Black Mirror » fait référence aux écrans omniprésents qui nous renvoient notre reflet. Sous un angle noir et souvent satirique, la série envisage un futur proche, voire immédiat. Elle interroge les conséquences inattendues que pourraient avoir les nouvelles technologies, et comment ces dernières influent sur la nature humaine de ses utilisateurs et inversement.* » : Wikipédia, article du 1er avril 2021 : https://fr.wikipedia.org/wiki/Black_Mirror_(série_télévisée)

[1409] F. DEFFERRARD, Chasser l'oubli comme du gibier, Dalloz IP/IT 2017, p. 672.

[1410] F. PASQUALE, *The Black Box Society*, *op. cit.*, p. 38.

not just that private corporations are using government records, like arrests, to make decisions. Police and intelligence agencies are using their databases, and private records, to revolutionize their own role in society. The dark axiom of the NSA era says that you don't have to worry if you have nothing to hide. But if your political activities or interests deviate even slightly out of the mainstream, you do »[1411].

Plus particulièrement, qu'en est-il de la réalité des traitements de données effectués, des mesures de surveillance mises en œuvre ou prévues, qu'elles soient d'initiative publique ou privée, des politiques publiques instaurées, voire des cultures subtilement développées pouvant, tout à la fois, affecter les individus, leurs vies et leurs identités, qu'elles soient physiques ou numériques, les deux étant fortement interdépendantes et inséparables ? Il apparaît, dès lors, nécessaire de s'interroger sur la réalité des enjeux affectant les identités des individus à la suite des impacts et effets générés par la révolution numérique, et ce de manière pragmatique et concrète ; une influence qui finalement s'avère être assez équivoque au regard des analyses juridiques, scientifiques, techniques, sociologiques et philosophiques entreprises jusqu'à présent.

Comme l'ont souligné les députés français, en 1977, « *l'informatique, c'est-à-dire la technique de traitement des informations par ordinateurs, constitue en effet un facteur très important de progrès. Elle peut, dans les domaines économiques et sociaux, permettre de réaliser des progrès considérables pour améliorer les conditions de travail, réduire la bureaucratie et les formalités de toute sorte. Elle peut être aussi un remarquable instrument de liberté et de démocratie. Mais, si l'on n'y prend garde, l'informatique peut être aussi un facteur de bureaucratie et de surexploitation des employés, ainsi qu'un danger pour la démocratie et les libertés* »[1412].

[1411] F. PASQUALE, *The Black Box Society*, *Id.*, p. 42.
[1412] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *Id*, p. 5786.

PARTIE II – LA RÉALITÉ DES ENJEUX DE L'IDENTITÉ NUMÉRIQUE : UNE INFLUENCE PRAGMATIQUE ET ÉQUIVOQUE

« *Il faut creuser jusqu'aux racines dont l'existence et la persistance rendent possible et même vraisemblable la répétition du monstrueux.* »[1413]

Le recours de plus en plus récurrent aux outils et dispositifs technologiques, suscitant l'édification du nouveau corpus juridique analysé visant la protection des individus et de leurs données, et attestant de l'existence effective et certaine des identités numériques, provoque, parallèlement, plusieurs effets et enjeux pragmatiques et concrets, quelque soient leur nature ; le risque majeur étant celui qui réside plutôt dans les intrusions, les ingérences subtiles, non manifestes, dans la vie privée et le quotidien des personnes, d'autant qu'une des particularités de la révolution numérique est que l'espace public numérique est façonné par l'espace privé numérique, *in fine*, par les individus et leurs connectivités.

Dans ce contexte, il est intéressant d'examiner la réalité des enjeux et des défis entourant ce nouvel environnement des identités numériques, de « *ce qui fait l'objet […] d'un affrontement, d'une discussion* »[1414] ; voire de « *ce que l'on peut gagner ou perdre dans n'importe quelle entreprise* »[1415], telle qu'entreprendre des traitements de données à caractère personnel. Il est donc question des défis entourant l'innombrable variété de traitement de données, défis occasionnés notamment par la révolution numérique survenue, et qui se révèlent comme étant pragmatiques, par opposition à théoriques, « *qui concerne*[nt] *les faits réels, l'action et le comportement que* [l'] *observation et* [l'] *étude* [de ces traitements] *enseignent* »[1416]. Se repère alors l'emprise du monde numérique dans sa globalité fondée sur une « *activité ordonnée à un but, correctement menée et productive de résultats* »[1417], « *qui s'attache à l'action, aux aspects*

[1413] G. ANDERS, *Nous, fils d'Eichmann*, Coll. Petites Bibliothèques rivages, Ed. Rivages Poche, 2003, p. 50.
[1414] Dictionnaire de l'Académie Française, 9ème Ed., « Enjeu » : https://www.dictionnaire-academie.fr/article/A9E1669
[1415] CNRTL, « Enjeu » : https://www.cnrtl.fr/definition/enjeu
[1416] CNRTL, « Pragmatique » : https://www.cnrtl.fr/definition/pragmatique
[1417] CNRTL, « Pragmatique » : *Id.*

concrets d'une affaire, plutôt qu'à la théorie ; qui envisage avant toute chose l'utilité, l'efficacité »[1418] ; *in concreto*, l'utilité et la productivité rattachées dorénavant aux opérations de traitement et d'analyse des données personnelles à disposition en masse.

Ces opérations et activités, liées aux nouvelles technologies de l'information et de la communication et au processus continu et progressif de numérisation du quotidien des humains et de leur existence, apparaissent, en outre, comme étant équivoques, ambigües, ayant « un double sens », « dont la nature est difficile à pénétrer, qui peut s'expliquer ou s'interpréter de diverses façons »[1419]. Dans ce contexte, il ressort ainsi, et à la lumière de l'étude entreprise dans la première partie de cette analyse, que « *l'enjeu essentiel, en cette période de mutation technologique majeure, est la préservation de l'équilibre complexe et fragile entre la construction de soi et le pouvoir formatif de la technologie, par lequel cette dernière façonne nos existences. […]. Or, pour que le processus de la construction de l'identité puisse prendre place de manière à permettre l'autonomie de la personne, il est nécessaire de préserver un « espace de jeu », […], espace dans lequel l'initiative de négociation des frontières entre le soi et la société est laissée à l'individu, et dans lequel il peut se retrouver dans l'intimité d'un chez-soi* »[1420].

Cette double influence provoquée par l'avènement et l'utilisation fréquente des nouvelles technologies, des pratiques et techniques informatiques et computationnelles et du Big data génère, *de facto*, de nombreux enjeux pouvant heurter à terme les individus, leurs constructions et perceptions et leur autonomie personnelle. Ce qui rappelle, à cet égard, le concept (durkheimien) de « fait social » précité[1421] qui, dans ce cadre, fait allusion aux traitements des données et, plus particulièrement, aux traitements des identités, et élargit conséquemment la portée de l'enjeu essentiel affectant l'identité numérique qui touche « *[…] non seulement la protection des données personnelles et de la sphère privée, mais à un niveau beaucoup plus fondamental, la sauvegarde de l'espace de jeu dans lequel l'identité peut se construire* »[1422].

[1418] Dictionnaire de l'Académie Française, 9ème Ed., « Pragmatique » : https://www.dictionnaire-academie.fr/article/A9P3834

[1419] Dictionnaire de l'Académie Française, 9ème Ed., « Équivoque » : https://www.dictionnaire-academie.fr/article/A9E2434 & CNRTL, « Équivoque » : https://www.cnrtl.fr/definition/équivoque

[1420] A. KHATCHATOUROV et P.-A. CHARDEL, « Fiche 1. La construction de l'identité dans la société contemporaine : enjeux théoriques », *In* Chaire Valeurs et Politiques des Informations Personnelles, *Cahier N°1 Identités numériques*, coordonné par C. Levallois-Barth, Institut Mines-Télécom, mars 2016, p. 14 ; disponible en ligne : https://blogrecherche.wp.imt.fr/files/2016/03/Cahier-Identites-numeriques_web.pdf

[1421] É. DURKHEIM, *Les règles de la méthode sociologique*, *op. cit.*, p. 14 ; *Cf.* p. 38-38.

[1422] A. KHATCHATOUROV et P.-A. CHARDEL, « Fiche 1. La construction de l'identité dans la société contemporaine : enjeux théoriques », *Id.,* p. 15.

De façon simultanée et analogue, ceci peut laisser les individus, sujets des identités numériques, dans le doute quant aux traitements, aux analyses, aux collectes, aux finalités et aux intérêts des opérations réellement entreprises, créant de fait une « *situation d'incertitude, d'ambiguïté, qui laisse hésitant* »[1423], tout en accordant plus de responsabilités et plus d'obligations à tout opérateur de traitement de données, donc plus de pouvoir. En effet, « *lestés d'obligations règlementaires, contractuelles et éthiques, les opérateurs de traitement et les sous-traitants deviennent à leur tour agents de leur richesse et co-régulateurs des normes protectrices* »[1424].

Le postulat principal qui transparaît à travers cette partie repose ainsi sur la conquête du cyberespace qui s'entreprend, essentiellement et fondamentalement, par la conquête et le contrôle de l'information ; conquête à laquelle s'ajoute, de surcroît, une multitude de menaces avenues, notamment, avec la mondialisation et la globalisation. Cela entraîne la mise en œuvre de nombreuses réponses, stratégies, solutions et cultures, légales comme sociales, également porteuses de risques et d'ambiguïtés.

En ce sens, « *l'érection d'un mur* [matériel, juridique ou virtuel, entendu métaphoriquement] *offre l'immense avantage, pour les gouvernants du moment, de donner l'impression, ou l'illusion, de « faire quelque chose ». La démonstration a un effet rassurant, à la fois sur la capacité d'agir des gouvernants et sur la reconnaissance des « dangers ». La construction d'un mur se fait donc toujours avec l'accord plus ou moins tacite de l'opinion publique du pays concerné. […]. Ainsi, les murs « fonctionnent souvent sur un mode spectaculaire, projetant un pouvoir et une efficacité qu'ils ne sauraient exercer concrètement et qui sont contredits dans les faits »* »[1425].

Dès lors, il semble utile de s'interroger sur la nature et la portée de ces enjeux et défis, mais aussi sur la manière dont ils risquent d'affecter l'identité des personnes, légalement et socialement, que ce soit dans sa dimension ou dans l'espace numérique et/ou physique.

Quels sont, *in concreto*, les enjeux touchant l'identité numérique des personnes ? Comment se manifestent, empiriquement, l'influence opérée par l'environnement numérique, la culture numérique et le recours aux technologies de l'information et de la communication impliquant, à la fois, de nombreux acteurs privés comme publics ?

[1423] CNRTL, « Équivoque » : *Id.*

[1424] A. BASDEVANT, J.-P. MIGNARD, *L'empire des données*, *op. cit*., p. 147.

[1425] F. NEISSE, A. NOVOSSELOFF, « L'expansion des murs : le reflet d'un monde fragmenté ? ,» *In* Politique étrangère, Vol. Hiver n°4, 2010 (p.731-742), p. 737, et les auteurs rajoutent « *La construction du mur israélien a, par exemple, été décidée à la suite de l'action d'un mouvement citoyen (Fence for Life) créé, en juin 2001, pour promouvoir le principe même d'une barrière, relativement déconnectée de la problématique des frontières, dans le contexte d'une vague d'attentats suicides (qui, au total, ont fait près de 1 000 victimes et traumatisé durablement la population israélienne). Ce « mur de séparation » ne fait guère débat au sein de la société israélienne, et ce, en dépit de son coût financier très lourd de 2,5 millions d'euros le kilomètre.* »

L’étude de cette partie permet d’observer que les enjeux de l’identité numérique sont d’ordre économico-sécuritaire (Titre I), d’un côté, et sociojuridique, de l’autre (Titre II), illustrant ainsi l’étendue de la réalité des enjeux et des défis auxquels sont confrontées toute identité numérique et donc, par extension, toute personne à l’ère du numérique.

TITRE I – UNE RÉALITÉ ÉCONOMICO-SÉCURITAIRE

« *To be fond of learning is to be near to knowledge. To practice with vigor is to be near to magnanimity. To possess the feeling of shame is to be near to energy.*
He who knows these three things knows how to cultivate his own character. Knowing how to cultivate his own character, he knows how to govern other men. Knowing how to govern other men, he knows how to govern the kingdom with all its states and families. »[1426]

Les différents enjeux pouvant impacter les identités numériques, à travers les traitements de leurs données personnelles, impliquent, pour la plupart, les analyses et/ou les jugements entrepris sur leurs personnes suivant une approche technologique, computationnelle et numérique, de calcul, visant, principalement, une surveillance continue et poursuivant, notamment, des objectifs d'économie et/ou de sécurité, entendus largement ; pourtant, « *rabattre le jugement sur le calcul conduit à se couper progressivement de la complexité du réel* »[1427].

Emprunté du latin *œconomicus*, « *bien ordonné, méthodique* », le terme économique désigne la « science de l'économie, l'ensemble des phénomènes se rapportant à l'économie »[1428]. Celle-ci, du latin *œconomia*, qui suppose une « disposition, un arrangement […] », se réfère, dans la sphère privée, à l' « art de gérer », l' « art d'administrer un bien, une entreprise par une gestion prudente et sage afin d'obtenir le meilleur rendement en utilisant les moindres ressources »[1429], et, dans la sphère publique, à l'« ensemble des activités humaines et des ressources concourant à la production et à la répartition des richesses »[1430]. Précisément, l'économie désigne l' « harmonie existant entre les différentes parties d'un corps organisé, tendant à en assurer le bon fonctionnement », le « système général dans lequel vit une collectivité, une nation »[1431]. À travers les nombreuses discussions, combinaisons et affrontements relatifs aux identités numériques et à leurs utilisations, se révèle la réalité de la « science économique » déployée à l'ère de la numérisation de la société qui est, certes, « *[…] peu de chose, mais ce peu de chose n'est pas rien. Ce peu de chose est d'une énorme importance pour chacun d'entre nous, et pourrait nous éviter bien des erreurs économiques, politiques et sociales : bien des*

[1426] Confucius, *The Doctrine of the mean: How to achieve equilibrium*, written ca 500 B.C.E., Ed. CreateSpace Independent Publishing Platform, 2014, p. 16.
[1427] A. SUPIOT, *La gouvernance par les nombres*, *op. cit*., p. 250.
[1428] Dictionnaire de l'Académie Française, 9ème Ed., « Économique » : https://www.dictionnaire-academie.fr/article/A9E0289
[1429] CNRTL, « Économie » : https://www.cnrtl.fr/definition/économie
[1430] Dictionnaire de l'Académie Française, 9ème Ed., « Économie » : https://www.dictionnaire-academie.fr/article/A9E0288 & CNRTL, « Économie » : *Id.*
[1431] Dictionnaire de l'Académie Française, 9ème Ed., « Économie » : *Id.*

souffrances…il pourrait, ce peu, s'il était perçu et compris, valoriser la science universitaire, aujourd'hui divisée, contradictoire, impuissante, faute de vue d'ensemble sur les réalités essentielles »[1432].

En outre, les enjeux et les risques touchant les données personnelles et, en prolongement, les individus se concrétisent en une réalité sécuritaire, qui prône, en particulier, « *[…] la sécurité publique et les moyens pour la garantir* »[1433], comprenant toute question liée à l'intérêt public et à la défense en rapport avec la sécurité, terme employé « *avec une connotation légèrement péjorative* [pour souligner] *le fait que la défense de la sécurité publique est susceptible d'engendrer des abus de pouvoir* »[1434].

S'observe alors la concrétisation des divers enjeux auxquels est confronté aujourd'hui tout traitement de données personnelles, qui, pour se faire, requiert une quantité importante de données, de toute forme et nature, appelant ainsi à plus de surveillance et de collecte numériques de la part d'acteurs publics comme privés. La réalité des enjeux économico-sécuritaire de l'identité numérique montre « *[…] très clairement l'ambivalence de la surveillance opérée qui tient à la fois de la lutte contre la criminalité organisée et de la lutte économique. Elle montre aussi un changement radical dans l'approche de la surveillance liée à la capacité de calcul disponible. On passe d'une surveillance ciblée en fonction de suspicions (à l'ancienne) à une surveillance globale sans motif. Cette logique est celle du Big Data. On amasse et on voit ce qui peut servir ultérieurement* »[1435].

Ce contexte entraîne ainsi la nécessité de s'interroger sur l'étendue et l'interprétation desdits enjeux économiques et sécuritaires, sans compter que, dès 2016, l'Autorité de la concurrence avait, de surcroît, souligné « les enjeux économiques et concurrentiels liés à l'utilisation de vastes ensembles de données ou Big data »[1436].

Comment les enjeux entourant la question des identités numériques forment aujourd'hui une réalité économico-sécuritaire ? Quelles sont, par ailleurs, les implications et les conséquences des réalités économique et sécuritaire mises en œuvre à l'ère numérique sur le traitement des données à caractère personnel ?

[1432] J. et J. FOURASTIÉ, *La réalité économique*, Ed. Hachette, Coll. Pluriel, 1986, p. 10.
[1433] Dictionnaire de l'Académie Française, 9ème Ed., « Sécuritaire » : https://www.dictionnaire-academie.fr/article/A9S1021
[1434] CNRTL, « Sécuritaire » : https://www.cnrtl.fr/definition/sécuritaire
[1435] CESE – E. PERES, *Les données numériques : un enjeu d'éducation et de citoyenneté, op. cit.,* p. 42.
[1436] Autorité de la concurrence, « Droit de la concurrence et données », étude coréalisée avec l'Autorité de concurrence allemande le Bundeskartellamt, du 10 mai 2016, p. 61-63, disponible en ligne : https://www.autoritedelaconcurrence.fr/sites/default/files/2019-05/rapport-concurrence-donnees-vf-mai2016.pdf ; et, Autorité de la concurrence, Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, *loc. cit*., p. 2.

Cette étude montre que le traitement des données personnelles se manifeste, désormais, comme étant le fruit d'une combinaison d'influence entre des espaces et des concepts originellement distincts (Chap. I), tout en constituant une lutte d'influence dans le but de détenir et de gérer toujours plus d'informations pouvant dégager toujours plus de valeurs (Chap. II) ; l'ensemble attestant, *ipso facto*, la réalité économico-sécuritaire des enjeux de l'identité numérique au XXI^{e} Siècle.

Chapitre I. Le traitement des données personnelles : Une combinaison d'influences

« *As long as secrecy can be used to undermine market competition and law enforcement,* [the market and the state] *will be emboldened to experiment with ever creepier, more intrusive, and even exploitative practices.* »[1437]

Un traitement, qui désigne de manière générale « l'objet d'un processus, l'accueil, la réception, la manière d'agir avec quelqu'un ou quelque chose »[1438], indique l' « *action d'agir sur une substance ou un produit en vue de le modifier et de l'adapter à un usage déterminé* »[1439] ; la substance ou le produit étant, dans ce contexte, les données. Le concept de « traitement de données à caractère personnel » se réfère, plus usuellement, au « traitement de l'information », « *[…] une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement)* »[1440]. Il suppose alors, de manière équivalente et parallèle, une combinaison, une fusion, d'informations facilitée et véhiculée, simultanément, par l'utilisation des nouvelles technologies, l'émergence du cyberespace et du Big data, le développement des techniques de surveillance ou de gestion dans des secteurs, initialement, distincts mais désormais confus, asseyant conséquemment la combinaison d'influences manifestée et qui s'opère, de façon générale, dans le secret. Pourtant, dès 1961, il fut proclamé, par le président des États-Unis de l'époque, que « *the very word "secrecy" is repugnant in a free and open society; and we are as a people inherently and historically opposed to secret societies, to secret oaths and secret proceedings* »[1441].

Cette combinaison, d'après le bas latin *combinatio*, « assemblage de deux choses », caractérisant l' « action, la manière de combiner » et le « résultat de cette action »[1442], désigne l' « *assemblage, union de deux ou de plusieurs éléments concrets ou abstraits, suivant certains rapports voulus ou fortuits, produisant un effet d'ensemble ou orientés vers un but précis* »[1443].

[1437] F. PASQUALE, *The black box society, op. cit.*, p. 11.
[1438] Dictionnaire de l'Académie Française, 8ème Ed., «Traitement » : https://www.dictionnaire-academie.fr/article/A8T0978 ; et CNRTL, « Traitement » : https://www.cnrtl.fr/definition/traitement
[1439] CNRTL, « Traitement » : *Id.*
[1440] CNIL, Définition « Traitement de données personnelles » : https://www.cnil.fr/fr/definition/traitement-de-donnees-personnelles
[1441] F. PASQUALE, *The black box society, Id.*, p. 12 (Note de bas de p. n° 37).
[1442] Dictionnaire de l'Académie Française, 9ème Ed., « Combinaison » : https://www.dictionnaire-academie.fr/article/A9C3055 ; et CNRTL, « Combinaison » : https://www.cnrtl.fr/lexicographie/combinaison
[1443] CNRTL, « Combinaison » : *Id.*

C'est donc une « *organisation précise de moyens en vue d'assurer le succès d'une entreprise* »[1444], celle du traitement des données personnelles traduisant le mélange d'influences et de logiques, informatique, économique et politique, effectué en vue d'assurer un équilibre dans un espace saturé et sans frontières, le cyberespace, éventuellement porteur de confusion, voire de tension ou d'abus ; cela dit, « *il y'a équilibre des libertés quand l'État permet l'exercice de toutes les libertés sans qu'aucune d'entre elles n'empiète sur les autres* »[1445].

Comment s'opère alors, en pratique, le traitement de données à caractère personnel ? l'entreprise de ces divers traitements assure-elle un équilibre entre les différents droits, libertés et obligations en la matière ? Plus particulièrement, comment les enjeux touchant les secteurs de l'économie et de la sécurité affectent-t-ils les opérations de traitement de données ?

Il apparaît que le traitement des données personnelles, tel qu'il s'effectue concrètement, résulte d'une combinaison d'influences découlant, principalement, de la confusion qui existe dorénavant entre l'espace public et l'espace privé (Section 1), générant conséquemment la tension qui se décèle entre deux notions fondamentales : la liberté et la sécurité (Section 2).

Section 1 – La confusion entre espace public et espace privé

Avec la révolution numérique et les multiples possibilités et quantités de traitement de données qu'elle fournit, émerge une confusion entre l'espace public et l'espace privé : confusion qui se caractérise notamment par le biais d'une cybersurveillance de masse devenue généralisée et ubiquitaire recourant à de nombreuses pratiques privées et publiques permettant de récolter des données (§1), ainsi que par une suprématie informationnelle déjà omniprésente et qui ne fait que s'étendre en vue de maîtriser et de détenir plus d'informations (§2).

§1. Une cybersurveillance de masse généralisée et ubiquitaire

La cybersurveillance de masse mise en œuvre s'observe à travers, d'une part, les pratiques de surveillance adoptées particulièrement marquées par leur opacité (A), et, d'autre part, les pratiques computationnelles, calculatoires, effectuées ayant la particularité d'être intrusives (B) ; pratiques révélant, *in concreto,* le caractère généralisé et ubiquitaire de la cybersurveillance mise en place.

[1444] CNRTL, « Combinaison, substantif » : https://www.cnrtl.fr/lexicographie/combinaison
[1445] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*., p. 5789.

A. Des pratiques de surveillance opaques

Dès le XX^e Siècle, des révélations pointues sur des pratiques de cybersurveillance massives ont commencé à voir le jour, lançant parallèlement et à un niveau mondial plusieurs débats, critiques, menaces, frustrations et peurs[1446]. Dans la deuxième moitié des années 90, des divulgations médiatiques et une étude générale de la STOA[1447] suivies de nombreux rapports européens sur le programme de surveillance et d'interception 'Echelon' ont été révélées ; puis en 2013, surgissent les révélations d'Edward Snowden et de Wikileaks sur l'ampleur de la cybersurveillance désormais généralisée et ubiquitaire, et s'avérant être autant opaque et contestée que les pratiques opérées sous le programme Echelon.

Même en étant légales, nécessaires ou légitimes[1448], les pratiques de surveillance numérique de masse opérées au XXI^e Siècle suscitent plusieurs débats et enjeux quant aux limites de ces pratiques, leurs modalités, les risques de dérapages ou d'abus, ou même d'atteintes à de nombreux droits et libertés fondamentaux. En outre, moyennant les techniques de cybersurveillance, il est facilement possible d'exercer un contrôle sur les individus ou encore sur des groupes, des organisations, des sociétés civiles, des entreprises au nom d'intérêts légitimes et nécessaires, comme la lutte contre le terrorisme, contre le crime, contre le cyber-terrorisme, le maintien de l'ordre public, de la sécurité nationale ou encore le développement d'un marché économique. Mais ces pratiques représentent également des procédés opaques et controversés puisque *« rien ne garantit que les résultats poursuivis et motivant ces pratiques de surveillance, soient atteints effectivement, ni que leur mise en œuvre ne soit détournée de l'objectif initial* », pour une surveillance d'opposants politiques par exemple, ou à des fins personnelles ou économiques, ou à des fins de monopolisation du marché économique et de distorsion de concurrence[1449], ainsi qu'il a pu être observé à la suite des diverses révélations de lanceurs d'alertes.

Les pratiques de surveillance, d'interception, de collecte, d'agrégation ou de traitement de données s'inscrivent dans une continuité historique linéaire, non ébranlable : quelles que soient les technologies développées et déployées au cours de l'histoire, allant du télégraphe en passant par les réseaux téléphoniques et les communications satellitaires et jusqu'à l'avènement d'internet, les efforts pour surveiller et/ou intercepter les communications, les flux, les

[1446] *Cf.* p. 480 et s.
[1447] EPRS - Scientific Foresight Unit (STOA), "An Appraisal of technologies of political control" Scientific and Technological Options Assessment, Luxembourg, 6 janvier 1998, PE 166 499, 97 p.
[1448] *Cf.* p. 297.
[1449] P. GUILLOT et D. VENTRE, Projet UTIC - Livrable 1 « Capacités d'interception et surveillance », Paris 8 – CNRS, Version du 03/04/2017, p. 5.

échanges, les données, les signaux représentent une constante des activités étatiques en particulier. En dépit des diverses révélations survenues au cours de l'histoire, ces pratiques n'ont jamais été interrompues ou abandonnées mais ont plutôt continué à évoluer et à s'adapter aux nouvelles technologies et aux nouvelles conditions et nouveaux enjeux, comprenant désormais, avec notamment la révolution numérique, les activités du secteur privé.

Déjà en 1973-1974, à la suite des révélations portant sur le projet SAFARI[1450], les parlementaires et les citoyens français ont vivement réagi, contraignant le gouvernement à mettre en place une Commission nationale d'informatique et des libertés (CNIL) et engendrant la création de la loi de 1978 Informatique et libertés pour assurer, nommément, la protection de la vie privée des citoyens et éviter les dérives et les abus des pouvoirs étatiques. Selon A. Peyrefitte, député de cette époque, « *la détention de l'informatique a toujours été un pouvoir parmi les autres. Aldous Huxley disait « toute science doit être traitée comme un ennemi possible ». Ce pouvoir est d'autant plus menaçant qu'il se nourrit d'indications à caractère individuel. Tant que ces renseignements étaient atomisés, parcellisés, les risques d'abus de pouvoir l'étaient aussi. Mais le développement de l'informatique entraîne une concentration et une croissance des informations personnalisées, nominatives, à caractère individuel, donc, une augmentation considérable des risques pour les libertés individuelles et collectives. Beaucoup d'entre nous ne supportent pas l'idée qu'on puisse, grâce à des fiches informatisées, tout savoir, à tout jamais, sur eux* »[1451]. Or, depuis cette époque, des divulgations sur des pratiques de surveillance et d'utilisation massive de données par les États et leurs services de renseignements ont régulièrement émaillé l'actualité.

La notion de surveillance signifie « l'action ou le fait de surveiller une personne dont on a la responsabilité ou à laquelle on s'intéresse, l'action de surveiller un territoire ou de surveiller un lieu et ses environs pour se prémunir contre une agression, de s'assurer de la sécurité » ; et en technologie, elle désigne le « contrôle permanent du déroulement d'un processus, du bon état de dispositifs, de systèmes »[1452]. Les technologies de surveillance peuvent être définies comme des dispositifs ou des systèmes qui peuvent « monitorer »[1453], tracer et évaluer les mouvements des individus, leurs propriétés et autres biens ou ressources ; la plupart employées pour suivre les activités de dissidents, de militants des droits de l'homme, de journalistes, de leaders ou

[1450] *Cf.* p. 72 et s., 182 et s.
[1451] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit.,* p. 5787.
[1452] CNRTL, 'Surveillance' : http://www.cnrtl.fr/definition/surveillance
[1453] Anglicisme, du mot 'Monitor' « *A device used for observing, checking, or keeping a continuous record of something* », English Oxford Living Dictionaries : https://en.oxforddictionaries.com/definition/monitor, qui signifie, en informatique, le « *fait de maintenir un œil, de surveiller quelqu'un ou quelque chose avec un appareil de suivi, de contrôle automatique* » : https://www.linternaute.fr/dictionnaire/fr/definition/monitorer/

associations étudiantes, de minorités, de dirigeants syndicaux et d'opposants politiques[1454]. Les différentes révélations observées au cours de l'histoire le démontrent de manière assez pragmatique, régulière et frappante.

En France, grâce aux travaux de M. Vaillé, on apprit l'existence des « cabinets noirs » nés dans la deuxième moitié du XVII[e] siècle, qui correspondaient à des « officines secrètes » placées sous le contrôle du pouvoir public, en l'occurrence le roi[1455], un auteur affirmant à ce titre que « *la violation systématique, à certaines époques, du secret des correspondances, a paralysé un mode d'expression de la pensée qui, [...], eût pu revêtir une importance capitale. Qui dira l'influence du Cabinet Noir sur la formation de l'esprit public en France au XVII[e] et au XVIII[e] siècle ?* »[1456]. Aboli pendant la Révolution française, le système du cabinet noir a été rétabli par le Directoire, maintenu sous l'Empire et la Restauration, et perdurera jusqu'au second Empire[1457].

Jusqu'aux années 60, la plupart des activités de surveillance étaient rudimentaires, *low-tech* et coûteuses, impliquant de nombreux agents pour des filatures, des rapports analogiques traités par d'autres agents sans perspectives réelles d'interconnexion ou de croisement rapide et/ou efficace. Néanmoins, passée cette époque, « *new technologies which were originally conceived for the Defense and Intelligence sectors, have after the cold war, rapidly spread into the law enforcement and private sectors* »[1458]. Dès les années 1980, de nouvelles formes de technologies de surveillance émergeaient, la plupart orientées vers l'automatisation des interceptions de communications. En 1994, le Département de la défense des États-Unis a signé un *Memorandum of Agreement* pour des « Opérations autres que la guerre et l'application de la loi » en vue de faciliter le développement conjoint et le partage des technologies entre différents services[1459]. Pendant la même période, un nouveau marché s'est manifesté : celui des dispositifs et équipements technologiques de surveillance qui seront créés, et régulièrement mis à jour, par

---

[1454] EPRS - Scientific Foresight Unit (STOA), "An Appraisal of technologies of political control", *Id.*, p. 15 ; et, P. GUILLOT et D. VENTRE, Projet UTIC - Livrable 1 « Capacités d'interception et surveillance », I*d.,* p. 5.

[1455] E. VAILLE, *Le Cabinet Noir*, Paris, PUF, 1950, un vol. in-8° de 412 p. ; et, P. GUILLOT et D. VENTRE, Projet UTIC - Livrable 1 « Capacités d'interception et surveillance », *Ibid.,* p. 7.

[1456] J. STENGERS, « Vaillé (Eugène). Le Cabinet Noir. », *In* Revue belge de philologie et d'histoire, t. 30, fasc. 1-2, 1952 (p. 363- 368), p. 364, et l'auteur poursuit « *Pour mesurer l'étendue possible de cette influence, il suffit de songer à ce qu'était le rayonnement intellectuel des grands épistoliers, d'un Voltaire par exemple : que n'eût été leur action si elle eût pu se développer librement sur le terrain de la politique?* » ; https://www.persee.fr/doc/rbph_0035-0818_1952_num_30_1_2135_t1_0363_0000_2

[1457] *Cf.* S. LAURENT, *Politiques de l'ombre - État, renseignement et surveillance en France*, Paris, Ed. Fayard, 2009, 704 p.

[1458] EPRS - Scientific Foresight Unit (STOA), "An Appraisal of technologies of political control", *Ibid.*, p. 16.

[1459] Memorandum of Understanding between Department of Defense and Department of Justice on "Operations other than War and Law enforcement", 20 avril 1994, signed by Janet Reno - Attorney General & John Deutch - Secretary of Defense; http://www.namebase.net:82/foia/mou01.html

des entreprises privées, et vendus aux gouvernements locaux ou étrangers qui y recouraient dans le cadre de l'application de la loi, les contrôles aux frontières ou encore dans le cadre de l'administration du travail et de la protection sociale.

Il ressort de cette période que le simple besoin d'une efficacité bureaucratique accrue a constitué un impératif puissant pour améliorer l'identification et la surveillance des individus. Plusieurs systèmes et dispositifs de surveillance de masse, portant pour la plupart atteinte aux vies privées des individus, ont été testés sur des groupes minoritaires faibles, tels que des immigrés ou des criminels, et ensuite déployés à l'échelle socioéconomique. Ainsi mises en place, ces technologies et les réglementations les autorisant sont difficiles à éliminer et s'étendent inévitablement à une utilisation plus générale[1460]. Ces pratiques caractérisent trois grandes catégories : la surveillance, l'identification et la gestion du réseau souvent utilisées conjointement avec d'autres technologies de surveillance comme les vidéos caméras de surveillance (CCTV), la reconnaissance faciale, la biométrie ou les cartes d'identités, poussant ainsi un auteur à affirmer que « *they facilitate mass and routine surveillance of large segments of the population without the need for warrants and formal investigations. What the East German secret police could only dream of is rapidly becoming a reality in the free world* »[1461]. Depuis, le concept de surveillance numérique généralisée et d'utilisation massive des données personnelles par les États et leurs services de renseignement ressort assez régulièrement dans l'actualité.

Vers la fin des années 90, l'existence du réseau Echelon fut dévoilée. Celui-ci désigne « *un système d'interception des télécommunications construit et géré par les services de renseignements des États-Unis d'Amérique en collaboration avec leurs homologues d'autres puissances occidentales. Il sert à intercepter les communications téléphoniques (conversations et télécopies) et les courriers électroniques d'autres pays, y compris alliés* »[1462]. Dans le cadre de l'étude générale entreprise par l'unité STOA du Parlement européen, les rumeurs révélées initialement par la presse ont été confirmées à travers, *inter alia*, l'étude des technologies de surveillance et d'interception employées dans le cadre de ce réseau ainsi que celle portant,

---

[1460] D. BANISAR, 'Big Brother goes High-Tech", Covert Action Quarterly, No. 56, Spring 1996, p. 6-10: "*Fingerprints, ID cards, data matching and other privacy invasive schemes were originally tried on populations with little political power, such as welfare recipients, immigrants, criminals and members of the military, and then applied up the socioeconomic ladder. Once in place, the policies are difficult to remove and inevitably expand into more general use.*"

[1461] D. BANISAR, 'Big Brother goes High-Tech", *Id.*

[1462] EPRS – Service de recherche du Parlement européen, Auteurs de l'étude : Franco PIODI et Iolanda MOMBELLI, « L'affaire ECHELON - Les travaux du Parlement européen sur le système global d'interception, 1998 – 2002 », Direction générale des services de recherche parlementaire - Unité Archives historiques, Octobre 2014 – PE 538.877, Luxembourg : Office des Publications de l'Union européenne, p. 9.

spécifiquement, sur les réseaux d'interception des communications nationales et internationales[1463], révélant l'ampleur de ce système : « *The Echelon system forms part of the UKUSA[1464] system but unlike many of the electronic spy systems developed during the cold war, Echelon is designed for primarily non-military targets: governments, organisations and businesses in virtually every country. The Echelon system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex to find key words. Five nations share the results with the US as the senior partner under the UKUSA agreement of 1948, Britain, Canada, New Zealand and Australia are very much acting as subordinate information servicers* »[1465].

En outre, une autre étude plus globale sur ce système et sur les pratiques de surveillance et d'interception opérées montre que la totalité de ces technologies de surveillance étaient utilisées

[1463] EPRS - Scientific Foresight Unit (STOA), "An Appraisal of technologies of political control", *Ibid.,* p. 19: "*Modern communications systems are virtually transparent to the advanced interceptions equipment which can be used to listen in. Some systems even lend themselves to a dual role as a national interceptions network. For example, the message switching system used on digital exchanges like System X in the UK supports an Integrated Services Digital Network (ISDN) Protocol. This allows digital devices, e.g. fax to share the system with existing lines. The ISDN subset is defined in their documents as "Signaling CCITT1-series interface for ISDN access. What is not widely known is that built in to the international CCITT protocol is the ability to take phones 'off hook' and listen into conversations occurring near the phone, without the user being aware that it is happening. (SGR Newsletter, No.4, 1993) This effectively means that a national dial up telephone tapping capacity is built into these systems from the start. (System X has been exported to Russia & China) Similarly, the digital technology required to pinpoint mobile phone users for incoming calls, means that all mobile phone users in a country when activated, are mini-tracking devices, giving their owners whereabouts at any time and stored in the company's computer for up to two years. Coupled with System X technology, this is a custom-built mobile track, tail and tap system par excellence. (Sunday telegraph,2.2. 97).*
Within Europe, all email, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London then by Satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York Moors of the UK. The system was first uncovered in the 1970's by a group of researchers in the UK (Campbell, 1981). The researchers used open sources but were subsequently arrested under Britain's Official Secrets legislation. The 'ABC' trial that followed was a critical turning point in researcher's understanding both of the technology of political control and how it might be challenged by research on open sources. (See Aubrey,1981 & Hooper 1987) Other work on what is now known as Signals intelligence was undertaken by researchers such as James Bamford, which uncovered a billion-dollar worldwide interceptions network, which he nicknamed 'Puzzle Palace'. A recent work by Nicky Hager, Secret Power, (Hager,1996) provides the most comprehensive details to date of a project known as ECHELON. Hager interviewed more than 50 people concerned with intelligence to document a global surveillance system that stretches around the world to form a targeting system on all of the key lntelsat satellites used to convey most of the world's satellite phone calls, internet, email, faxes and telexes. These sites are based at Sugar grove and Yakima, in the USA, at Waihopai in New Zealand, at Geraldton in Australia, Hong Kong, and Morwenstow in the UK. […]"

[1464] The National Archives, "Newly released GCHQ files: UKUSA Agreement": "*UKUSA Agreement - the top secret, post-war arrangement for sharing intelligence between the United States and the UK. Signed by representatives of the London Signals Intelligence Board and its American counterpart in March 1946, the UKUSA Agreement is without parallel in the Western intelligence world and formed the basis for co-operation between the two countries throughout the Cold War*": https://www.nationalarchives.gov.uk/ukusa/ ; R. WHITAKER, *The end of privacy – How total surveillance is becoming a reality*, The New Press New York, 1999, p. 92-93.

[1465] EPRS - Scientific Foresight Unit (STOA), "An Appraisal of technologies of political control", *Ibid.*, p. 19.

pour un contrôle politique et public mais aussi à des fins économiques et commerciales[1466]. La capacité de ce projet en matière de collecte et de traitement des informations publiques et privées est indéniable et ressort clairement à travers le 'cadre' dans lequel ce système opérait, comprenant les États et leurs services de renseignement ainsi que leurs liens ou alliés internationaux officieux, informels. Dans le cadre de ce système, les activités de renseignements étaient notamment des activités de COMINT « Communication Intelligence » effectuées entre les États-Unis et la Grande-Bretagne ayant tous deux signés un accord secret à cet effet[1467]. Le COMINT inclut les « *Special Intelligence of World War II* » et tout autre information technique ou de renseignement (au sens de 'Intelligence') dérivée des communications étrangères publiques et privées, par exemple « *medium and low-grade cypher messages, plain language transmissions radio telephone conversations, traffic analysis, and direction-finding* »[1468]. Les COMINT sont une grande composante des SIGINT « Signals Intelligence », qui incorporent également ELINT « Electronic or Non-communications Intelligence » la collecte et l'analyse de signaux non liés aux communications, tels que ceux des émissions radars, ainsi que FISINT « Foreign Instrumentation Signals Intelligence » la collecte des émissions électromagnétiques associées aux essais et aux opérations des systèmes aériens, spatiaux, de surface ou souterrain, qui englobe par ailleurs une sous-catégorie, TELINT « Telemetry Intelligence » l'interception des signaux envoyés par les missiles ou leurs composantes lors des essais[1469]. Outre l'alliance UKUSA, plus de trente autres pays pratiquent des activités de COMINT : le plus grand système d'interception et de collecte de renseignement étant celui de la Russie FAPSI[1470] qui dirige plusieurs sites de collecte, notamment à Lourdes

[1466] Working document for the STOA Panel, European Parliament, Directorate General for Research, "Development of Surveillance Technology and Risk of Abuse of Economic Information - Appraisal of Technologies of Political Control (Vol. 1 to 5)", PE 168.184/Vol 1/5/EN, Luxembourg, décembre 1999.
[1467] The National Archives, Highlights Guide "*The 10-page, Top Secret British-U.S Communication Intelligence Agreement was signed on 5 March 1946 and committed both nations to sharing intelligence with each other, continuing a practice which had begun during the Second World War. Later referred to as the 'UKUSA Agreement' the document lays out the terms of the deal which formed the basis for signals intelligence co-operation between the two countries throughout the Cold War. The agreement was later extended to cover Canada, Australia and New Zealand and this is covered in other files in the HW80 series*", p. 2: https://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf
[1468] NSA - William F. Friedman, Report on the Potentialities of COMINT as a Source of Warning of the Eminence of Hostilities, 28 aout 1953, Ref ID A39176, p. 1: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_138/41712209075151.pdf
[1469] J. T. RICHELSON, *The U.S. Intelligence Community*, Boulder, Co.: Westview Press, 2011, p. 203-208, et, R. M. CLARK, *The Technical Collection of Intelligence*, Washington, D.C.: CQ Press, 2011, p. 157-214.
[1470] "The Federal Agency for Government Communications and Information [FAPSI - Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii], the Russian counterpart to the US National Security Agency, was established by the Presidential Decree "On the Federal Government Communications and Information Agency" on 19 February 1993. In 1994, the Russian president approved the statute of this secret service. FAPSI replaced the Administration of Information Resources (AIR) at the Presidential Office, which was formed from the KGB Eighth (Encoding) Chief Directorate and Sixteenth Directorate, the Decoding and Radio Interception Service,

(Cuba) et au Vietnam. Le BND allemand[1471] et la DGSE française[1472] collaboraient au fonctionnement de l'opération d'exploitation de sites de collecte COMSAT[1473] à Kourou, en Guyane, ciblant les communications satellitaires américaines et Sud-américaines. La DGSE a par ailleurs d'autres sites de collecte COMSAT à Domme (Dordogne, France), en Nouvelle-Calédonie et aux Émirats Arabes Unis[1474]. La Chine maintenait également un système SIGINT substantiel, dont deux stations visant la Russie et opérant en collaboration avec les États-Unis. Plusieurs autres États du Moyen-Orient ou d'Asie avaient également largement investi dans des opérations de SIGINT, en particulier Israël, l'Inde et le Pakistan[1475].

Des différentes études susmentionnées, il découle que l'alliance UKUSA gérait à elle seule 120 systèmes de satellites de collecte d'informations dont 40 ciblant nommément les « *western commercial communications satellites (ILC)* »[1476]. Une quantité massive de données est

---

and the Government Communications Directorate of the USSR KGB. FAPSI's functions extend beyond ComInt and include providing government and commercial communications systems", Federation of American Scientists: https://fas.org/irp/world/russia/fapsi/history.htm

[1471] Bundesnachrichtendienst - The foreign intelligence service of Germany, "*Intelligence collected by the Bundesnachrichtendienst (BND) contributes to foreign and security policy-making at national level and helps to protect German interests all over the world. In order to do so the BND uses intelligence resources at its disposal to collect information unobtainable by any other mean*": http://www.bnd.bund.de/EN/Home/home_node.html

[1472] Direction Générale de la Sécurité Extérieure : « *La DGSE est un service de l'État, placé sous l'autorité du pouvoir exécutif. Ses activités, définies par l'autorité politique, ont pour objectif exclusif la protection des intérêts français. Leur réalisation concourt, notamment, à la protection des citoyens français partout dans le monde. Pour cette mission spécifique, elle œuvre en partenariat étroit avec l'ensemble des services de sécurité nationaux. Son champ d'action se situe principalement hors des frontières de notre pays, où elle applique des méthodes clandestines de recherche du renseignement* » : https://www.defense.gouv.fr/dgse

[1473] Communications Satellite: A communications satellite is a type of artificial satellite that is placed in Earth's orbit for the purpose of sending and receiving communication data between a source and destination. It is used to provide data communication and relaying services for televisions, radio, telecommunication, weather and Internet services: https://www.techopedia.com/definition/6567/communications-satellite

[1474] La France a depuis mis en place le COMSAT NG (Communication par satellite de nouvelle génération) : « *Le programme communication par satellite de nouvelle génération (COMSAT NG), notifié en décembre 2015 par la Direction générale de l'armement (DGA), doit permettre le maintien de la permanence des communications sur le territoire national et avec les zones prioritaires d'intérêt, ainsi qu'avec nos bâtiments à la mer, en tout temps (paix, crises ou catastrophe majeure). Moyens primordiaux pour les télécommunications à longue distance ou pour les forces, les systèmes de communication par satellite constituent une pierre fondamentale pour la maîtrise de l'information. Cette maîtrise, clé de la supériorité des forces armées, est indispensable aux cinq fonctions stratégiques. Elle permet à tous les niveaux d'engagement (du niveau stratégique jusqu'à la plate-forme de combat) d'apprécier la situation et de conduire l'action opérationnelle* » : https://www.defense.gouv.fr/dga/equipement/information-communication-espace/comsat-ng-communication-par-satellite-de-nouvelle-generation

[1475] Working document for the STOA Panel, European Parliament, Directorate General for Research, Development of Surveillance Technology and Risk of Abuse of Economic Information, "Vol 2/5 The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition", Interception Capabilities 2000 – IC 2000 Report, PE 168.184/Vol 2/5, point 1, p. 7 et point 47, p. 8; et, EPRS – Service de recherche du Parlement européen, « L'affaire ECHELON - Les travaux du Parlement européen sur le système global d'interception, 1998 – 2002 », *Id.*, p. 10.

[1476] Working document for the STOA Panel, Development of Surveillance Technology and Risk of Abuse of Economic Information, "Vol 2/5 The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems,

collectée, traitée et analysée par le système Echelon pour des finalités assez antipodes, consistant en des pratiques d'espionnage à des fins de contrôle politique ou alors à des fins économiques et commerciales : « *Whilst there is much information gathered about potential terrorists, there is a lot of economic intelligence, notably intensive monitoring of all the countries participating in the GATT negotiations. [...]* »[1477]. De nombreuses révélations depuis le début des années 90 montrent que la NSA collecte, assez ouvertement, des informations économiques, révélations confirmées par des fonctionnaires américains qui reconnaissent la collecte particulière de renseignements économiques, « *whether intentionally or otherwise* », en raison même de la conception du système qui collecte massivement et à haut débit toutes les données de communications, les communications civiles se mêlant aux communications militaires et politiques[1478]. D'autres pays de l'UKUSA pratiquent également l'espionnage économique, tels que la Grande-Bretagne, l'Australie, le Canada ou la Nouvelle-Zélande[1479]. Quelques cas spécifiques sur des activités de COMINT d'espionnage économique ayant profité à des sociétés américaines pour l'acquisition de contrats à l'étranger furent ainsi révélées par les études du STOA : en 1993, la compagnie européenne Panavia a été spécifiquement espionnée concernant des ventes au Moyen-Orient ; en 1994, la NSA a intercepté des communications entre Thomson-CSF et le Brésil concernant SIVAM le système de surveillance prévu pour la forêt amazonienne, initiant des accusations de corruption et de pots-de-vin contre l'entreprise Thomson, et le contrat fut finalement attribué à Raytheon Corporation une entreprise américaine participant activement au système Echelon ; en 1995, la NSA a intercepté des communications entre le consortium européen Airbus, la compagnie aérienne nationale

---

and its applicability to COMINT targeting and selection, including speech recognition", IC 2000 Report, *Id.*, point 46, p. 8.

[1477] EPRS - Scientific Foresight Unit (STOA), "An Appraisal of technologies of political control", *Id.*, p. 20.

[1478] Working document for the STOA Panel, Development of Surveillance Technology and Risk of Abuse of Economic Information, "Vol 2/5 The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition", IC 2000 Report, *Ibid.*, point 95, p. 17: « *US officials acknowledge that NSA collects economic information, whether intentionally or otherwise. Former military intelligence attaché Colonel Dan Smith worked at the US Embassy, London until 1993. He regularly received Comint product from Menwith Hill. In 1998, he told the BBC that at Menwith Hill: "In terms of scooping up communications, inevitably since their take is broadband, there will be conversations or communications which are intercepted which have nothing to do with the military, and probably within those there will be some information about commercial dealings"*
"Anything would be possible technically. Technically they can scoop all this information up, sort through it and find out what it is that might be asked for …" ».

[1479] Working document for the STOA Panel, Development of Surveillance Technology and Risk of Abuse of Economic Information, "Vol 2/5 The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition", IC 2000 Report, *Ibid.*, points 98 à 100, p. 17-18; et, EPRS – Service de recherche du Parlement européen, « L'affaire ECHELON - Les travaux du Parlement européen sur le système global d'interception, 1998 – 2002 », *Ibid.*, p. 10.

saoudienne et le gouvernement saoudien, a usé de ses pouvoirs de divulgations et d'accusations en matière de corruption grâce aux informations recueillies et le contrat a été attribué aux entreprises américaines Boeing Co and McDonnell Douglas Corp. ; nombreuses pratiques d'espionnage effectuées dans le cadre des négociations internationales sur le commerce, notamment l'interception de communications relatives aux normes d'émissions des véhicules japonais, aux négociations commerciales en matière d'importation de voitures de luxe japonaises, à la participation de la France aux négociations du GATT en 1993 et à la Coopération économique pour l'Asie-Pacifique (APEC) en 1997[1480]. De ce fait, l'espionnage économique effectué dans le cadre du système Echelon ne semblait pas avoir de limites, touchant aussi des particuliers et affectant la concurrence loyale en raison des différents avantages concurrentiels octroyés aux entreprises qui participent à ce système, dénotant avec force l'étendue et l'opacité des pratiques de surveillance et d'interception.

En outre, ces pratiques ne se sont pas uniquement limitées à l'alliance UKUSA, des États membres de l'Union ayant rapidement suivi cette nouvelle tendance : ainsi, un rapport spécial de Statewatch[1481] a dévoilé que l'UE avait secrètement accepté de mettre en place un système de surveillance des communications international au moyen d'un réseau secret de comités établis en vertu du troisième « pilier » du traité de Maastricht portant sur la coopération dans les domaines de la justice et des affaires intérieures[1482]. Ce rapport publia les détails d'une stratégie commune élaborée par le Conseil de l'Union Européenne, qui avait pourtant déclaré laconiquement lors des questions posées sur le système Echelon que « le Conseil ne disposait lui-même d'aucune information à ce sujet, qu'il n'était pas impliqué dans de telles choses, et qu'il ne pouvait, partant, fournir aucune réponse »[1483], et le Bureau fédéral des investigations

[1480] Working document for the STOA Panel, Development of Surveillance Technology and Risk of Abuse of Economic Information, "Vol 2/5 The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition", IC 2000 Report, *Ibidem*, points 101 à 105, p. 18; et, EPRS – Service de recherche du Parlement européen, « L'affaire ECHELON - Les travaux du Parlement européen sur le système global d'interception, 1998 – 2002 », *Ibidem*, p. 10-11.
[1481] Statewatch – monitoring the State and civil liberties in Europe, based in the UK: http://www.statewatch.org
[1482] Statewatch bulletin, EU & FBI launch global telecommunications surveillance system: "not a significant document" - UK Home Secretary, January-February 1997, Vol. 7 n° 1: http://www.statewatch.org/EUFBISW.HTM
[1483] Question écrite E-0499/98 posée Elly Plooij-van Gorsel (ELDR) au Conseil (27.2.1998), Question écrite E-1775/98 posée par Lucio Manisco (GUE-NGL) au Conseil (8.6.1998), Question orale H-1086/98, posée au Conseil par Patricia McKenna (16.12.1998), question orale H-1172/98, posée au Conseil par Patricia McKenna (13.1.1999), question orale H-1172/98 posée au Conseil par Inger Schörling (13.1.1999), Question orale H-0526/99, posée au Conseil par Pernille Frahm (6.10.1999), Question orale H-0621/99, posée au Conseil par Lone Dybkjaer (19.11.1999), etc. ; Rapport Du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI)) du 11 juillet 2001, Rapporteur : Gerhard Schmid, FINAL A5-0264/2001 Partie 1, PE 305.391 RR\445698FR.doc, p. 80-81

des États-Unis (FBI) en vue d'introduire un système global de surveillance des télécommunications, appels téléphoniques, mails et faxes. Ce rapport révéla, par ailleurs, que la décision concrétisant effectivement ce système n'a jamais été discutée ou examinée par le Conseil des ministres de la justice et des affaires intérieures, il a simplement été convenu par 'procédure écrite' *via* un échange de télex entre 15 gouvernements de l'UE[1484]. Les « Requirements - Spécifications » prévues pour les fournisseurs de services et les opérateurs de réseaux par l'Union afin de permettre la surveillance des communications, adoptées en 1995 et non publiés jusqu'en novembre 1996[1485], sont fondées sur les « Requirements » mises en place par le FBI en 1992, révisées en 1994. La résolution adoptée en 1995 mettant en place un système d'interception légale des télécommunications[1486] au sein de l'Union en collaboration avec les États-Unis n'a fait l'objet d'aucune publicité à l'époque de son adoption. Tout a été entrepris en suivant une stratégie opaque, que ce soit pour l'adoption de la résolution ou pour son contenu, le terme de « services autorisés »[1487] étant défini de manière flou et imprécise par exemple : « *The US-FBI use of the term "transparency" has strange ring in European understanding, it is taken to mean ensuring that the subjects of the interception are "unaware of ongoing electronic surveillance"* »[1488].

Et cette résolution a été révisée vers 1998 pour inclure la surveillance d'internet et des communications satellitaires ainsi que des téléphones mobiles nouvelles générations[1489], alors

---

(disponible en ligne : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//FR) ; et, EPRS – Service de recherche du Parlement européen, « L'affaire ECHELON - Les travaux du Parlement européen sur le système global d'interception, 1998 – 2002 », *Id.,* p. 11-12.

[1484] Statewatch bulletin, EU & FBI launch global telecommunications surveillance system, *Id.*: « *On 21 December 1994 a decision was taken, under the German Presidency, not to wait for the next Council meeting in March 1995 but to adopt the "Resolution" setting out the "Requirements" by "written procedure". The "written procedure" process of decision making meant that the draft Resolution was sent out by telex from Brussels to each Member State. On 9 January a further telex attached two statements by Denmark and France for agreement, and a final telex with a statement by the Netherlands was telexed out on 18 January - the day after the official adoption of the measure on 17 January 1995. [...]* »

[1485] Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, Journal officiel n° C 329 du 04 novembre 1996 (96C 329/01), p. 01 – 06, En vigueur : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31996G1104&from=EN & https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:C:1996:329:FULL&from=FR

[1486] Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, *Id.,* Glossaire, p. 5-6 : le terme d'interception désigne « *ici l'action légale permettant aux services autorisés d'accéder aux télécommunications envoyées ou reçues par une personne ainsi qu'aux informations afférentes aux appels* » ; et la notion de télécommunications est définie comme « *tout transfert de signes , signaux , écrits , images , sons , données ou informations de toute nature transmis en totalité ou en partie par fil , radio , système électromagnétique , photo électronique ou photo optique* ».

[1487] Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, *Ibid.,* Glossaire, p. 5 : « Un service autorisé par la loi à procéder à des interceptions de télécommunications. »

[1488] Statewatch bulletin, EU & FBI launch global telecommunications surveillance system, *Ibid.*

[1489] ENFOPOL 98, Rev 1 & ENFOPOL 98 REV 2 + COR 1 - Draft Council Resolution on New Technologies, Bruxelles 4 novembre 1998, Document 10951/1/98 LIMITE ENFOPOL Rev 1 Note et Document 10951/2/98 ENFOPOL rev 2 : https://www.heise.de/tp/features/ENFOPOL-98-Rev-1-3446438.html?seite=all &

même qu'un rapport du Parlement européen recommandait dans ses conclusions de rejeter la proposition du Conseil[1490].

Un document intitulé « Requirements for Trusted Third Party Services »[1491] rédigé par ETSI 'European Telecommunications Standards Institute', souligne clairement et sans équivoque l'importance et les implications globales de ce nouveau système : « *there is a need to facilitate the growing importance and development of electronic commerce, the European Information Infrastructure (EII) and the Global Information Infrastructure (GII) by the introduction of suitable measures to safeguard the integrity and confidentiality of electronic information* »[1492], et, plus particulièrement, en matière d'interception légale, il indique que « *lawful interception of telecommunications traffic is commonly recognized as an important instrument to fight crime and to assure national security. LEAs* [Law Enforcement Agencies] *have the need to intercept incoming and outgoing telecommunications traffic, which is transported via telecommunications networks, without knowledge of e.g. the interception subjects and the foreign country or countries involved* »[1493]. De plus, compte tenu de la nécessité et du besoin pour les services autorisés de recevoir les interceptions dans un langage 'interprétable', la résolution du Conseil dispose ainsi que « *si les opérateurs de réseaux ou les fournisseurs de services procèdent au codage, à la compression ou au chiffrement des données transmises, les interceptions correspondantes doivent être fournies 'en clair' aux services autorisés par les opérateurs de réseaux ou les fournisseurs de services* »[1494], donc fournies sans aucune technique de cryptage.

Pour compléter la stratégie développée et en assurer le respect et la conformité à l'échelle mondiale, un '*Memorandum of Understanding*' reprenant les termes de la résolution du Conseil ainsi que les 'Spécifications' pour les opérateurs de réseaux et fournisseurs de service a été

---

https://publications.parliament.uk/pa/ld199899/ldselect/ldeucom/94/9453.htm ; Devenue ENFOPOL 19 – Draft Council Resolution on the lawful interception of telecommunications in relation to new technologies, Bruxelles 15 mars 1999, Document 6715/99 : https://www.fipr.org/polarch/enfopol19.html

[1490] Rapport sur le projet de résolution du Conseil relative à l'interception légale des télécommunications compte tenu des nouvelles technologies (10951/2/98 - C40052/99 - 99/0906(CNS)), du 23 avril 1999, A4-0243/99 : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1999-0243+0+DOC+XML+V0//FR

[1491] ETSI Guide, "Telecommunications Security; Trusted Third Parties (TTP); Requirements for TTP services", EG 201 057 V1.1.2 (1997-07) - DEG/SEC-003000 (9sc00ide.PDF), European Telecommunications Standards Institute juillet 1997: https://www.etsi.org/deliver/etsi_eg/201000_201099/201057/01.01.02_60/eg_201057v010102p.pdf

[1492] ETSI Guide, "Telecommunications Security; Trusted Third Parties (TTP); Requirements for TTP services", *Id.,* p. 6.

[1493] ETSI Guide, "Telecommunications Security; Trusted Third Parties (TTP); Requirements for TTP services", *Ibid.,* p. 30.

[1494] Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, *Ibid.,* Art. 3.3.

élaboré afin d'étendre ce nouveau système UE-US à des pays tiers non européens, invités par conséquent à adopter les mêmes spécifications[1495]. Le nombre de signataires de ce Mémorandum est illimité, tout pays pouvant y adhérer, sous réserve de l'accord des États membres actuels. Celui-ci invite des 'participants' puisque « *"the possibilities for intercepting telecommunications are becoming increasingly threatened" and there is a need to introduce "international interception standards" and "norms for the telecommunications industry for carrying out interception orders" in order to "fight… organised crime and for the protection of national security."* »[1496]. Plusieurs pays faisant déjà partie du système Echelon ont manifesté leur intérêt d'y adhérer, comme l'Australie, montrant en conséquence la facilité d'interconnexion et d'interopérabilité de ces pratiques de surveillance. Aucun élément de ce plan, de cette stratégie n'a fait l'objet de discussion ou n'a été soumis au Parlement européen ou à la Commission des libertés publiques et des affaires intérieures ou à la Commission juridique des droits des citoyens en dépit des questions irréfutables liées aux droits et libertés fondamentales soulevées par de tels systèmes ne prévoyant aucun régime de responsabilité. Statewatch en conclut à juste titre que « *it is the interface of the Echelon system and its potential development on phone calls combined with the standardisation of "tappable" telecommunications centres and equipment being sponsored by the EU and the USA which presents a truly global threat over which there are no legal or democratic controls* »[1497].

[1495] Statewatch bulletin, EU & FBI launch global telecommunications surveillance system, *Ibidem,* et Statewatch Report, European Union and the FBI launch global surveillance system, 10 février 1997: "*The "Memorandum of understanding with third countries" (later described as the "Memorandum of Understanding on the Legal Interception of Telecommunications") was discussed at the K4 Committee in November 1994. The significance of the "Memorandum" is that it extends the agreement on the surveillance of telecommunications to non-EU countries who are being invited to adopt it - and with it the "Requirements".*
The Memorandum of Understanding was signed by the 15 EU Member States on 23 November 1995 at the meeting of the Council of Justice and Home Affairs Ministers. The contact addresses for signatory countries and for further information, which confirms the EU-USA link, should be sent to:
"a) Director Federal Bureau of Investigation, Attention: Information Resource Division, 10 Pennsylvania Avenue, N.W., Washington D.C. 20535
b) General Secretary of the Council of the European Union, FAO The President, Rue de la Loi 175, B-1048 Brussels, Belgium.": http://statewatch.org/NEWS4A.HTM

[1496] Statewatch Report, European Union and the FBI launch global surveillance system, *Id.*: "*The strategy appears to be to first get the "Western world" (EU, US plus allies) to agree "norms" and "procedures" and then to sell these products to Third World countries - who even if they do not agree to "interception orders" will find their telecommunications monitored by ECHELON (see below) the minute it hit the airwaves.*"; et, Statewatch bulletin, EU & FBI launch global telecommunications surveillance system, *Ibidem.:* "*By October 1996 Australia, Canada and the US had informed the European Council in Brussels of their support for the "Requirements", Norway had signed the "Memorandum of Understanding", and Hong Kong and New Zealand are "considering the means by which they could support the "Requirements"." Ongoing meetings of "experts" from these six countries and the EU are being organised under the "informal title of ILETS (International Law Enforcement Telecommunications Seminar)".*"

[1497] Statewatch Report, European Union and the FBI launch global surveillance system, 10/02/1997, *Id.*

Puis, vinrent les années 2010 et le tour des divulgations de E. Snowden et de Wikileaks illustrant l'ampleur et l'étendue des pratiques de surveillance conduites par les services de renseignement américains, qualifiées de surveillance de masse, mais aussi par de nombreux autres États, l'ensemble tirant profit des évolutions et développements technologiques en matière d'information et de communication, des capacités renouvelées offertes par internet, de l'avènement du Big data et des métadonnées, et ainsi de suite. Il fut alors révélé que les autorités américaines ont la possibilité d'accéder à grande échelle, *via* des programmes de collecte de renseignements tels que PRISM[1498], aux données personnelles de citoyens de l'Union lorsqu'ils ont recours à des prestataires de services en ligne américains, et de les traiter[1499]. Les services de renseignement opèrent une collecte d'information massive et généralisée sur des infrastructures, telles que les câbles sous-marins ou la fibre optique, sur des *Data centers* ainsi que sur les réseaux, en exploitant des failles de protocoles ou en installant des « *backdoors* » (une porte dérobée – une entrée) dans les matériels informatiques et les logiciels largement utilisés, par exemple. Les documents révélés par Snowden montrent clairement à quel point les autorités américaines et les services de renseignement se fient aux entreprises américaines pour surveiller internet : ayant remarqué que le secteur privé mettait déjà en place un système de surveillance généralisée à travers ses services et produits, ils en ont simplement profité en se servant là-dessus.

[1498] PRISM/US-984XN, Planning Tool for Research Integration, Synchronization and Management: « *The program facilitates extensive, in-depth surveillance on live communications and stored information. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US. It also opens the possibility of communications made entirely within the US being collected without warrants. […]. Some of the world's largest internet brands are claimed to be part of the information-sharing program since its introduction in 2007. Microsoft – which is currently running an advertising campaign with the slogan "Your privacy is our priority" – was the first, with collection beginning in December 2007.*
It was followed by Yahoo in 2008; Google, Facebook and PalTalk in 2009; YouTube in 2010; Skype and AOL in 2011; and finally Apple, which joined the program in 2012. The program is continuing to expand, with other providers due to come online.»: Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps into user data of Apple, Google and others", The Guardian, Thursday 6 June 2013:
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data &
https://www.pulitzer.org/files/2014/public-service/guardianus/02guardianus2014.pdf

[1499] Résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union (2013/2682(RSP)), P7_TA(2013)0322, p. 2, point C. ; Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)), Commission des libertés civiles, de la justice et des affaires intérieures, Rapporteur: Claude Moraes, Document de séance - A7-0139/2014, du 21 février 2014, p. 8-9 ; Communication de la Commission au Parlement Européen et au Conseil, Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique, Bruxelles, le 27 novembre 2013 COM/2013/0846 final ; CESE - E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op.cit.*, p. 41-42 ; B. SCHNEIER, *Data and Goliath – The Hidden battles to collect your data and control your world*, Ed. W.W. Norton & Company Independent Publishers, 2015, p. 92 à 95.

À travers des programmes comme PRISM, la NSA a la capacité de légalement contraindre des entreprises telles que Microsoft, Google, Apple, Facebook, Skype ou Yahoo à fournir des données personnelles et/ou des données brutes sur plusieurs milliers de 'personnes d'intérêts', certaines coopérant volontairement et devenant des partenaires d'autres forcées par la loi généralement de manière secrète, et, par le biais d'autres programmes, l'agence de renseignement américaine obtient un accès direct au réseau de base – la dorsale internet – afin de procéder à une surveillance de masse sur tout le monde, visant *in fine* l'infrastructure d'une entreprise non-coopérative ou lente à coopérer, l'architecture d'internet et le trafic de données de manière généralisée[1500].

Ces pratiques se ne limitaient pas uniquement aux services de renseignement américains, mais ont eu lieu partout dans le monde. En effet, les documents divulgués montrent que plusieurs États membres de l'Union européenne ont « coopéré avec Prism et d'autres programmes de même nature ou se sont vu accorder un accès aux bases de données créées » et qu'en outre, ils « disposent de programmes de surveillance similaires ou envisagent d'en créer »[1501]. Par ailleurs, l'agence britannique de renseignement électronique le GCHQ[1502], par le biais de programmes de surveillance comme Tempora consistant à détourner directement les communications électroniques passant par les câbles transatlantiques, paye des entreprises de communications telles que BT et Vodafone pour lui garantir un accès direct aux communications électroniques partout dans le monde[1503]. Et le gouvernement français entreprend des pratiques de surveillance et d'écoute ainsi que de collecte de renseignements en épiant, entre autres, France Télécoms et Orange[1504]. Les révélations ont également montré que les entreprises associées au programme Prism font toutes partie de l'accord sur la 'sphère de

---

[1500] B. SCHNEIER, *Data and Goliath*, *Id.*, p. 92, et L. PÉTINIAUD, « Cartographie de l'Affaire Snowden », *In* Hérodote N° 152-153, *Cyberespace : Enjeux géopolitiques*, *op. cit.*, p. 35 à 42.

[1501] Résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union, *Id.,* p. 2, points D et E.

[1502] Government Communications Headquarters – Pioneering a new kind of security for an ever more complex world: "*GCHQ is a world-leading intelligence, cyber and security agency with a mission to keep the UK safe":* https://www.gchq.gov.uk

[1503] Résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union, *Id.,* p. 2, point F, et le Parlement souligne en outre : « *considérant que d'autres États membres intercepteraient des communications électroniques transnationales sans mandat formel mais sur décision de juridictions spéciales, qu'ils partageraient leurs données avec d'autres pays (Suède) et qu'ils pourraient élargir leurs capacités de surveillance (Pays-Bas, Allemagne); que des voix se sont élevées, dans d'autres États membres, pour s'inquiéter des pouvoirs d'interception laissés aux services secrets (Pologne);* » ; et, B. SCHNEIER, *Data and Goliath*, *Id.*, p. 93, et l'auteur nous apprend que « *Vodafone gives Albania, Egypt, Hungary, Ireland, and Quatar – possibly 29 countries in total – direct access to internet traffic flowing inside their countries. […]*»

[1504] B. SCHNEIER, *Data and Goliath*, *Ibid.*, p. 93.

sécurité' dit 'Safe Harbor', qui a été déclaré invalide par la CJUE, une fois qu'elle a eu l'occasion de l'examiner[1505]. En effet, « *toutes les entreprises participant au programme PRISM, qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux États-Unis, semblent être certifiées dans le cadre de la sphère de sécurité. La sphère de sécurité est donc devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'UE* »[1506]. En outre, plusieurs législations prévoyant l'obligation généralisée de conservation des données aux fournisseurs ainsi que leur accès aux autorités nationales compétentes sans limitations, aux seules fins de lutte contre la criminalité grave, ont été déclarées invalides par la Cour, à l'image de la directive de 2006 sur la conservation de données[1507]. En 2017, de nouveaux documents exfiltrés de la CIA ont été divulgués relançant les débats sur les pratiques de surveillance effectuées[1508]. À ce stade, il ne s'agit plus vraiment de montrer les capacités d'interception et de collecte massives mais plutôt de dévoiler les méthodes et les techniques d'interception, de collecte, de cybersurveillance à travers

[1505] CJUE, Affaire Schrems du 7 octobre 2015, points 80 à 86 où la Cour souligne notamment « *Ainsi, la décision 2000/520 consacre la primauté des «exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis» sur les principes de la sphère de sécurité, primauté en vertu de laquelle les organisations américaines auto certifiées recevant des données à caractère personnel depuis l'Union sont tenues d'écarter, sans limitation, ces principes lorsque ces derniers entrent en conflit avec ces exigences et s'avèrent donc incompatibles avec celles-ci* » ; et *Cf.* p. 271.

[1506] Communication de la Commission au Parlement Européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, Bruxelles, le 27 novembre 2013, COM(2013) 847 final, p. 19.

[1507] CJUE, Affaire Digital Rights Ireland du 8 avril 2014, *loc. cit.,* où la Cour a déclaré que « *En imposant la conservation des données énumérées à l'article 5, paragraphe 1, de la directive 2006/24 et en permettant l'accès des autorités nationales compétentes à celles-ci, cette directive déroge, ainsi que l'a relevé M. l'avocat général notamment aux points 39 et 40 de ses conclusions, au régime de protection du droit au respect de la vie privée, instauré par les directives 95/46 et 2002/58, à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques, ces dernières directives ayant prévu la confidentialité des communications et des données relatives au trafic ainsi que l'obligation d'effacer ou de rendre anonymes ces données lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, hormis si elles sont nécessaires à la facturation et uniquement tant que cette nécessité perdure* » (point 32), et a dit pour droit « *La directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, est invalide.* », dispositif de l'arrêt.

[1508] Le Monde, « De nouveaux documents publiés par WikiLeaks montrent que la CIA a pu pirater des MacBook », Publié le 23 mars 2017 : https://www.lemonde.fr/pixels/article/2017/03/23/de-nouveaux-documents-publies-par-wikileaks-montrent-que-la-cia-a-pu-pirater-des-macbook_5099828_4408996.html ; The Guardian, « WikiLeaks publishes 'biggest ever leak of secret CIA documents' », E. MacAskill, S. Thielman and P. Oltermann, Publié le 7 Mars 2017 : https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance

l'exploitation des dernières technologies développées et l'Internet des Objets : les pratiques de surveillance et d'interception se font là plus précises, plus intrusives[1509].

Depuis les évènements du 11 septembre 2001, il est quelque part universellement admis que la lutte contre le terrorisme est devenue l'une des grandes priorités de la plupart des gouvernements du monde. Cela dit, les révélations faites depuis les années 2010 sur l'envergure des pratiques de surveillance opérées et celles mises en place ou prévues, ont *de facto* suscité de nombreux enjeux et plusieurs inquiétudes, alimentant différentes polémiques autour de : la portée et la légitimité des systèmes de surveillance révélés aux États-Unis et dans les États membres de l'Union ; la violation des normes et droits fondamentaux de l'Union européenne ainsi que des normes juridiques en matière de protection des données ; le niveau de confiance entre les partenaires transatlantiques ou entre les internautes et les services et produits numériques du secteur privé ; les menaces sur les libertés individuelles, la démocratie et l'état de droit ; le degré de coopération et d'implication de certains États membres de l'Union dans des programmes de surveillance américains ou des programmes équivalents au niveau national ; le manque de contrôle et de surveillance effective par les autorités politiques américaines ou européennes de leurs services de renseignement ; les rapports de force ou de coopération, entre acteurs étatiques et privés (entreprises, associations, industriels, citoyens), civils et militaires ; la possibilité que ces activités de surveillance de masse soient utilisées pour des raisons autres que la sécurité nationale et la lutte contre le terrorisme au sens strict, par exemple à des fins d'espionnage économique et industriel ou de profilage pour des motifs politiques ; l'atteinte à la liberté de la presse et aux communications des membres des professions soumises au secret professionnel, dont les avocats et les médecins ; les rôles et degrés d'implication respectifs des agences de renseignement et des entreprises informatiques et de télécommunications privées ; les frontières de plus en plus floues entre les activités répressives et les activités de renseignement, avec pour effet que chaque citoyen est traité comme un suspect et fait l'objet d'une surveillance ; les multiples menaces relatives à la vie privée à l'heure du numérique[1510].

[1509] Wikileaks, « Vault 7: CIA Hacking Tools Revealed », Publié le 7 mars 2017 : https://wikileaks.org/ciav7p1/ ; et, P. GUILLOT et D. VENTRE, Projet UTIC - Livrable 1 « Capacités d'interception et surveillance », *Ibidem,* p. 5-6.

[1510] Résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union, *Ibid.,* p. 3 à 6, points 1 à 17; Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures du 21 février 2014, *Id.,* p. 8-9, points E et F.

L'ambivalence des surveillances opérées ressort clairement de ces divulgations et semble tenir à la fois de la lutte contre le terrorisme et la criminalité organisée ainsi que de la lutte économique et commerciale ; dénotant par là même un changement radical dans l'approche de la surveillance liée de plus en plus à la capacité de calcul disponible. Le passage d'une surveillance ciblée, en fonction de suspicions à l'ancienne, à une surveillance globale, ubiquitaire sans motif particulier est devenue une réalité digne des meilleurs films de science-fiction, notamment eu égard aux révélations sur les pratiques computationnelles intrusives employées dans le cadre de ces systèmes de surveillance.

B. Des pratiques computationnelles intrusives

Les diverses révélations sur les nombreux systèmes de surveillance mis en œuvre montrent le changement radical de paradigme en matière de pratiques et modalités technologiques de surveillance et d'interception. Celles-ci se sont affinées, caractérisées désormais par des aspects comme « l'échelle, le niveau de profondeur des intrusions, la multiplicité des méthodes, les partenariats secrets, les attaques illicites, la compromission des matériels », là où les anciennes l'étaient par « le modèle d'interception légale, l'interception ciblée, la cause antérieure, la proportionnalité, l'exception européenne de sécurité nationale, l'infraction à la CEDH »[1511]. En dépit des différentes publications divulguant les pratiques de surveillances opaques développées, ces dernières se sont non seulement généralisées, devenues en quelque sorte admises, prises aujourd'hui pour habitude, mais les modalités et les techniques utilisées se sont en outre perfectionnées et adaptées devenant de plus en plus intrusives, ayant recours au computationnel.

De l'anglais « computing », le concept de computation se réfère au « calcul, à l'évaluation » désignant, « *very broadly, the field encompassing computer science, computer engineering, communications, information science and information technology* »[1512]. Certains l'identifient comme étant une discipline en indiquant que « *the discipline of computing is the systematic*

[1511] D. CAMPBELL, State Interference with privacy on the internet – Interception Capabilities 2014, commissioned by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in Brussels, Octobre 2013 : Presentation in Session II: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BLIBE-OJ-20130905-2%2B01%2BDOC%2BPDF%2BV0%2F%2FEN ; http://www.duncancampbell.org/PDF/CoECultureCommittee1Oct2013.pdf & http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf

[1512] CNRTL, « computation » : http://www.cnrtl.fr/definition/computation, et J. M. WING, « Computational thinking and thinking about computing » , Philosophical Transactions of the Royal Society, Series A - Mathematical, Physical, and Engineering Sciences (2008) 366 (p. 3717–3725), p. 3717 (note de pied de p.)

study of algorithmic processes that describe and transform information : their theory, analysis, design, efficiency, implementation, and application. The fundamental question underlying all of computing is, "What can be (efficiently) automated? »[1513]. Les capacités informatiques en matière de surveillance et d'interception ne cessent de se peaufiner et de s'adapter aux évolutions continues de l'environnement numérique : le cyberespace ne fait que s'étendre avec la multiplication des matériels, des équipements, notamment les objets connectés, ou encore des applications et services. Parallèlement, les pratiques ou programmes développés par les services de renseignement du monde entier sont le reflet de ces évolutions et adaptations. De nos jours, des entreprises présentent des catalogues offrant des technologies de surveillance et d'interception, donnant la sensation que tout est désormais possible en matière de surveillance[1514].

Les révélations sur les pratiques suivies par les services de renseignement ont montré l'ampleur des collectes de données effectuées à travers des programmes de surveillance tels que Prism ou Tempora, et ont aussi dévoilé leurs utilisations de programmes de recherche par recoupements, comme XKeyscore[1515], pour cibler les informations recherchées provenant d'entreprises privées, d'ONG, d'institutions internationales, de ministères de pays étrangers ou de personnalités politiques[1516]. De plus, les alliances secrètes dévoilées se sont elles aussi adaptées et développées à l'ère du tout numérique, « associant alliances pérennes et partenariats ponctuels dont les ramifications hiérarchisées s'étendent à l'ensemble du monde »[1517] :

[1513] P. J. DENNING, D.E. COMER, D. GRIES, M. C. MULDER, A. TUCKER, A. J. TURNER & P. R. YOUNG, "Computing as a discipline", Communications of the ACM, 32 (1): 9-23, 1989, p. 12; et, P. J. DENNING & C. H. MARTELL, "Great Principles of Computing", Cambridge, MA: MIT press, 2015.

[1514] L'entreprise Nexa Technologies – membre de l'Alliance Intellexa : https://www.nexatech.fr/products ; L'entreprise Ercom – A Thales Company : https://www.ercom.fr/entreprises/ ; L'entreprise Systancia : https://www.systancia.com/en/our-solutions/

[1515] « *XKeyscore, […], is the NSA's "widest reaching" system developing intelligence from computer networks – what the agency calls Digital Network Intelligence (DNI). One presentation claims the program covers "nearly everything a typical user does on the internet", including the content of emails, websites visited and searches, as well as their metadata. Analysts can also use XKeyscore and other NSA systems to obtain ongoing "real-time" interception of an individual's internet activity.* »: G. GREENWALD, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", The Guardian, publié le 31 juillet 2013: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data ; IC Off The Record, "NSA Tool Collects 'Nearly Everything a User Does on the Internet'", 31/7/2013: https://nsa.gov1.info/dni/xkeyscore.html ; The Unofficial XKeyscore User Guide: https://www.documentcloud.org/documents/2116191-unofficial-xks-user-guide.html#document/p1; et, E. SNOWDEN, XKeyscore presentation: https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf

[1516] L. PÉTINIAUD, « Cartographie de l'Affaire Snowden », *op. cit.*, p. 35, et, D. CAMPBELL, State Interference with privacy on the internet – Interception Capabilities 2014, *Id.,* Slide n° 8.

[1517] L. PÉTINIAUD, « Cartographie de l'Affaire Snowden », *Id.*, p. 40 ; Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures du 21 février 2014, *loc. cit.,* p. 15, point AQ ; et, D. CAMPBELL, State Interference with privacy on the internet – Interception Capabilities 2014, *Id.,* Slides n° 2, 9, 17 et 19.

l'alliance UKUSA est devenue les « five eyes » alliant les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. S'ajoutaient à ces « five eyes » les alliés secondaires, nommés dans les documents révélés les « Third Party Liaison » qui coopéraient avec les autorités étatiques de l'alliance dite des « cinq yeux » de façon variable selon la nature de leur alliance, tel que ce fut le cas pour la Lybie de Kadhafi. Beaucoup se sont étonnés du manque de répression ou de l'absence de mesure coercitive vis-à-vis des États-Unis en particulier, l'État représentant le pôle central de cette coopération de nature mono-centrique amassant et échangeant fréquemment et aisément les données du monde.

En effet, les révélations ont montré que les États membres de l'Union sont pour la plupart des agents très actifs en matière de pratiques de surveillance et d'interception, « *autant comme partenaires de la NSA que comme Little Brothers nationaux* »[1518]. Outre l'alliance privilégiée des « Five eyes », les documents publiés font mention d'autres réseaux de coopération échelonnés et structurés : les « nine eyes/9-eyes », qui regroupent le Danemark, la France, les Pays-Bas et la Norvège, ainsi que les « fourteen eyes/14-eyes » ajoutant l'Allemagne, l'Italie, la Belgique, l'Espagne et la Suède[1519]. Dans ce contexte, il semble alors difficile pour les autorités européennes de s'insurger contre les pratiques avancées de leur 'allié' outre Atlantique ; leurs propres différentes pratiques, partiellement illégales et peu connues, rendant « *toute tentative d'indignation ridicule et toute prise de mesure profondément hypocrite* »[1520].

Par ailleurs, les États-Unis ont également établi des partenariats avec d'autres pays du monde assez distants comme l'Inde, dont certains ayant des régimes brutalement répressifs comme l'Arabie Saoudite. De même, ils ont une relation exceptionnelle avec l'État d'Israël, partageant avec leurs services des « raw SIGINT », des renseignements d'origine électromagnétique bruts[1521]. L'ensemble de ces alliances fournit alors aux agences de renseignement américaines un accès à presque tout : « *The result is a European bazaar, where an EU member state like Denmark may give the NSA access to a tapping center on the (unenforceable) condition that NSA doesn't search it for Danes, and Germany may give the NSA access to another on the condition that it doesn't search for Germans. Yet the two tapping sites may be two points on the same cable, so the NSA simply captures the communications of the German citizens as they transit Denmark, and the Danish citizens as they transit Germany, all the while considering it*

[1518] L. PÉTINIAUD, « Cartographie de l'Affaire Snowden », *Ibid.*, p. 42.
[1519] B. SCHNEIER, *Data and Goliath*, *op. cit.*, p. 90; L. PÉTINIAUD, « Cartographie de l'Affaire Snowden », *Ibidem*, « Carte 3. – La NSA et l'Union Européenne : Des relations coupables ? », p. 41.
[1520] L. PÉTINIAUD, « Cartographie de l'Affaire Snowden », *Ibidem*, p. 42.
[1521] D. CAMPBELL, State Interference with privacy on the internet – Interception Capabilities 2014, *Ibid.,* Slides n° 28 et 29; B. SCHNEIER, *Data and Goliath*, *Id.*, p. 91.

entirely in accordance with their agreements. Ultimately, each EU national government's spy services are independently hawking domestic accesses to the NSA, GCHQ, FRA[1522]*, and the like without having any awareness of how their individual contribution is enabling the greater patchwork of mass surveillance against ordinary citizens as a whole* »[1523].

En outre, les autorités américaines encouragent leurs alliés à procéder à des « opérations d'accès » qui consistent en des efforts pour obtenir l'accès aux communications en vrac de tous les principaux fournisseurs de services de télécommunication situés sur leurs territoires. Pour ce faire, la NSA fournit des consultations, des technologies, ou même du matériel physique en soi, à ses partenaires pour « ingérer » ces quantités massives de données de manière à permettre leurs traitements ; et il ne faut pas longtemps pour accéder à la totalité : ainsi, en Grande-Bretagne, British telecommunications (BT), Vodafone Cable, l'entreprise américaine Verizon, Global Crossing, Level 3, Viatel et Interoute ont toutes coopéré et accordé au GCHQ un accès illimité secret à l'intégralité de leurs réseaux de câbles sous-marins, câbles qui transportent une grande partie des appels téléphoniques et du trafic internet mondiaux, transmettant *inter alia* les détails des appels téléphoniques, des communications électroniques et des entrées Facebook de leurs clients[1524].

[1522] FRA - Försvarets radioanstalt, the National Defence Radio Establishment, is the Swedish national authority for Signals Intelligence: "*FRA supplies intelligence to the Government of Sweden, to the Swedish Armed Forces and to other concerned authorities. FRA also provides cyber security services for selected government authorities and state-owned companies*.": https://www.fra.se/system/engelska/english.4.6a76c4041614726b25ae4.html

[1523] E. Snowden Testimony to the European Parliament – The Civil Liberties, Justice and Home affairs (LIBE) Committee, May 2014, Answer to a question by Rapporteur Claude Moraes (MEP, S&D Group), p. 4; et l'auteur explique le processus: "*One of the foremost activities of the NSA's FAD, or Foreign Affairs Division, is to pressure or incentivize EU member states to change their laws to enable mass surveillance. Lawyers from the NSA, as well as the UK's GCHQ, work very hard to search for loopholes in laws and constitutional protections that they can use to justify indiscriminate, dragnet surveillance operations that were at best unwittingly authorized by lawmakers. […]. The ultimate result of the NSA's guidance is that the right of ordinary citizens to be free from unwarranted interference is degraded, and systems of intrusive mass surveillance are being constructed in secret within otherwise liberal states, often without the full awareness of the public. […]. By the time this general process* [including the 'access operations'] *has occurred, it is very difficult for the citizens of a country to protect the privacy of their communications, and it is very easy for the intelligence services of that country to make those communications available to the NSA -- even without having explicitly shared them. The nature of the NSA's "NOFORN," or NO FOREIGN NATIONALS classification, when combined with the fact that the memorandum agreements between NSA and its foreign partners have a standard disclaimer stating they provide no enforceable rights, provides both the NSA with a means of monitoring its partner's citizens without informing the partner, and the partner with a means of plausible deniability*.", p. 3-4: http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf

[1524] J. BALL, L. HARDING et J. GARSIDE, "BT and Vodafone among telecoms companies passing details to GCHQ", The Guardian, publié le 2 août 2013: "*The document identified for the first time which telecoms companies are working with GCHQ's "special source" team. It gives top secret codenames for each firm, with BT ("Remedy"), Verizon Business ("Dacron"), and Vodafone Cable ("Gerontic"). The other firms include Global Crossing ("Pinnage"), Level 3 ("Little"), Viatel ("Vitreous") and Interoute ("Streetcar"). The companies refused to comment on any specifics relating to Tempora, but several noted they were obliged to comply with UK and EU law*.": https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq, et, E.

Globalement, la cybersurveillance recouvre plusieurs catégories d'action et implique des techniques adaptées et des technologies spécifiques, les pratiques de surveillance et d'interception ne s'arrêtant pas à la capture du message, du signal, des données. Il faut naturellement rattacher des systèmes de stockage, d'agrégation, de traitement et d'analyse des données collectées en masse. Autrement dit, « *the word "collect" has a very special definition, according to the* [US] *Department of Defense. It doesn't mean collect; it means that a person looks at, or analyses, the data* »[1525].

Quatre grandes catégories de pratiques computationnelles mobilisées pour la surveillance peuvent être identifiées : la surveillance d'internet, la surveillance des téléphones mobiles, l'interception des lignes fixes et les technologies d'intrusion. La surveillance d'internet représente le fait de saisir les données alors qu'elles traversent le réseau vers leurs destinations prévues, qui peut être déployée à travers tout point des systèmes physiques ou électroniques composant le réseau d'internet (fournisseurs, opérateurs, câbles, routeurs, serveurs, etc.). Ces types de technologies comptent, par exemple, des logiciels qui ciblent les informations publiées sur des sources 'accessibles au public' qui, dans le passé, englobaient les nouveaux sites web, mais qui comprennent dorénavant, de façon assez controversée, les réseaux sociaux.

Les technologies de surveillance des téléphones mobiles saisissent, pour leurs parts, les informations transmises au sein des réseaux mobiles ; l'une des formes les plus courantes étant l'utilisation des IMSI Catcher – des dispositifs techniques de proximité « *permettant de capter à distance les données de connexion comme les correspondances échangées ; il s'agit en pratique de fausses antennes relais, installées à proximité de la personne dont on souhaite intercepter les échanges électroniques, afin de capter l'ensemble des données transmises entre le périphérique électronique et la véritable antenne relais* »[1526]. Ce dispositif permet ainsi non seulement de s'immiscer dans le réseau et les échanges, mais aussi de contourner certaines mesures de chiffrement, interceptant les données produites ou reçues (sur le terminal électronique) avant ou après tout chiffrement.

L'interception des lignes fixes implique le recueil d'informations traversant les réseaux téléphoniques commutés (RTC)[1527], le RTC formant le socle des réseaux de communications

---

Snowden Testimony to the European Parliament, May 2014, *Id.,* Answer to a question by Rapporteur Claude Moraes (MEP, S&D Group), p. 3-4.

[1525] B. SCHNEIER, *Data and Goliath*, *Ibid.*, p. 152.

[1526] CNIL, « L'accès des autorités publiques aux données chiffrées », du 30 août 2017 : https://www.cnil.fr/fr/lacces-des-autorites-publiques-aux-donnees-chiffrees

[1527] Le Réseau Téléphonique Commuté (RTC) est « *la technologie historique du service téléphonique fixe (avec le téléphone directement branché à la prise en « T »). En France, ce réseau a été déployé autour des années 80 par Orange (anciennement « France Télécom »). L'obligation imposée à Orange d'ouvrir son réseau à la concurrence a permis à d'autres opérateurs d'émerger et de fournir des services de téléphonie fixe.* » :

internationaux ; et des appareils et solutions technologiques permettant de surveiller et d'exploiter simultanément des réseaux de ce genre, à l'échelle de tout un pays, sont de nos jours vendus par des entreprises privées. Quant aux technologies d'intrusion, elles servent à déployer clandestinement des logiciels malveillants, « malwares », sur des téléphones mobiles ou des ordinateurs. Le malware, ou Cheval de Troie, permet aux opérateurs de prendre le contrôle complet de l'appareil de la cible en s'incrustant dans l'ensemble des fonctions du système, caractérisant ainsi la catégorie d'action de surveillance la plus intrusive qui soit.

Alors que les appareils deviennent plus connectés, liés aux réseaux de communications, et se font partie intégrante de nos vies quotidiennes, les individus deviennent de plus en plus dépendants de ces dispositifs pour tenir leurs détails et informations intimes ou professionnelles. Les pratiques d'intrusion accordent aux opérateurs un accès illimité à ces appareils et à tout ce qu'ils contiennent, recueillant et transmettant les données à l'opérateur du Cheval de Troie, pendant que l'utilisateur est dans l'ignorance totale, l'appareil infecté fonctionnant normalement et sans entraves. Durant tout ce temps, ces technologies d'intrusion peuvent surveiller tout ce qui apparaît sur l'écran de l'individu, pister les entrées de clavier et tout autre entrée, surveiller le contenu des communications envoyées par l'appareil, y compris l'historique des communications comme les anciens mails ou les clavardages (conversation de chat). Par ailleurs, ces technologies peuvent récolter bien plus que les informations se trouvant seulement sur le dispositif : les données collectées par l'opérateur de l'outil d'intrusion pouvant ainsi inclure des enregistrements en temps réel des flux audio et vidéo en direct de la caméra ou du microphone de l'appareil. En conséquence, l'appareil de l'utilisateur se transforme en un espion en soi, capturant toutes les informations autour de la personne, y compris ses conversations avec des tiers, et surveillant automatiquement toutes ses activités en ligne et hors ligne[1528].

La Commission européenne, dans sa proposition de règlement relative aux biens à double usage, définit les technologies de cybersurveillance comme étant « *des biens spécifiquement conçus pour permette l'intrusion secrète dans des systèmes d'information et de*

Télécoms-infoconso, Arcep, « Arrêt du RTC et transition vers les réseaux téléphoniques de nouvelle génération », du 2 novembre 2018 : https://www.telecom-infoconso.fr/arret-du-rtc-et-transition-vers-les-reseaux-telephoniques-de-nouvelle-generation/

[1528] Par ex., B. SCHNEIER, *Data and Goliath*, *Ibidem.*, pp. 55-60 et 82-84 ; P. GUILLOT et D. VENTRE, Projet UTIC - Livrable 1 « Capacités d'interception et surveillance », *op. cit.,* pp. 22-24 : et, Privacy International, Topic « Communications surveillance » : https://privacyinternational.org/explainer/1309/communications-surveillance

télécommunication afin de surveiller, d'extraire, de collecter et d'analyser des données et/ou de paralyser ou d'endommager le système visé »[1529].

En revanche, le Parlement européen a apporté des amendements à cette proposition annonçant, à titre liminaire, que « *certaines technologies de cybersurveillance se sont avérées constituer une nouvelle catégorie de biens à double usage utilisés pour compromettre directement les droits de l'homme , notamment le droit à la protection de la vie privée et des données, la liberté d'expression, la liberté de réunion et la liberté d'association, par la surveillance ou l'exfiltration de données [...], et/ou par la neutralisation ou la dégradation du système visé* »[1530], et considère pour sa part que les « *biens de cybersurveillance, y compris le matériel informatique, les logiciels et les technologies*, [sont] *conçus spécifiquement pour permettre l'intrusion secrète dans des systèmes d'information et de télécommunication et/ou la surveillance, l'exfiltration, la collecte et l'analyse des données et/ou la paralysie ou l'endommagement du système visé sans l'autorisation expresse, informée et univoque du propriétaire des données, et susceptibles d'être utilisés en lien avec des violations des droits de l'homme, notamment du droit à la vie privée, [...], ou susceptibles d'être utilisés pour commettre des violations graves du droit de l'homme ou du droit humanitaire international, ou pouvant constituer une menace pour la sécurité internationale ou pour la sécurité fondamentale de l'Union et de ses États membres* »[1531].

Ces biens englobent les équipements d'interception des télécommunications, les logiciels d'intrusion, les centres de surveillance, les systèmes d'interception licite et de conservation de données, l'investigation numérique, et, rajoute le Parlement européen, les appareils utilisés pour

---

[1529] Proposition de Règlement du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte), COM(2016) 616 final-2016/0295(COD), Bruxelles le 28 septembre 2016, Art. 2, point 21) : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52016PC0616 ; Adoptée et entrée en vigueur : Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte), Art. 2, point 20) « *«biens de cybersurveillance», les biens à double usage conçus spécifiquement pour permettre la surveillance discrète de personnes physiques par la surveillance, l'extraction, la collecte ou l'analyse de données provenant de systèmes d'information et de télécommunications;* » : https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32021R0821.

[1530] Amendements du Parlement européen, adoptés le 17 janvier 2018, à la proposition de règlement du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte) (COM(2016)0616 – C8-0393/2016 – 2016/0295(COD)), A8-0390/2017 (Procédure législative ordinaire – refonte), Amendement 2 : Proposition de règlement Cons. 5 : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0006+0+DOC+XML+V0//FR#def_1_1

[1531] Amendements du Parlement européen, adoptés le 17 janvier 2018, à la proposition de règlement instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage, *Id.,* Amendement 26 : Proposition de règlement Art. 2 – al. 1 – point 1 – sous-point b.

le déchiffrement, la récupération des disques durs, le contournement des mots de passe et l'analyse des données biométriques, ainsi que les systèmes de surveillance sur réseau IP[1532]. Il est intéressant de noter que certaines technologies de cybersurveillance, auparavant exclues de la définition de ces biens de cybersurveillance, tels que les dispositifs et services de localisation ou de géolocalisation, l'analyse des métadonnées, les sondes-capteurs – « Probes »[1533], ou les systèmes d'inspection approfondie de paquets – Deep Packet Inspection (DPI)[1534], ont finalement été intégrées dans le Règlement entré en vigueur[1535].

In fine, les pratiques de surveillance peuvent varier allant de l'analyse du trafic, née dans les années 80 grâce aux travaux de Welchman qui a développé la pratique de production de renseignements par l'analyse du trafic[1536], à l'exploitation des métadonnées. Et les documents publiés par Snowden ont révélé que le gouvernement britannique, souvent avec la collaboration des entreprises de télécommunication, a fixé des sondes aux câbles sous-marins pour intercepter leurs trafics. Une fois ceux-ci interceptés, les autorités anglaises utilisent des « sélecteurs » et des « critères de recherche » pour filtrer le contenu et les métadonnées recueillis. Grâce à ces technologies de « Probe » et d'analyse de trafic, et en raison de la position géographique

---

[1532] Proposition de Règlement instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte), *Id.*, Art. 2, point 21), sous-points a) à e) ; et, Amendements du Parlement européen, adoptés le 17 janvier 2018, à la proposition de règlement instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage, *Ibid.,* Amendement 4 : Proposition de règlement Cons. 6 *bis* (nouveau).

[1533] "*Probe = A physical device inserted at a key juncture in a network for the purposes of monitoring or collecting data traveling through the network. Network technologies also include surveillance tools that place probes on an operator's network to deliver information directly to law enforcement or intelligence agencies. This set of technologies serve no other purpose than to intercept and deliver information. This is referred to as the External Interception Framework*": Privacy International, Topic "Communications Surveillance: Distinctions and Definitions": https://privacyinternational.org/course-section/2088/communications-surveillance-distinctions-and-definitions

[1534] "*Deep packet inspection is a type of data processing that looks in detail at the contents of the data being sent, and re-routes it accordingly. It can be used for perfectly innocuous reasons, like making sure that a feed of data is supplying content in the right format, or is free of viruses. Or it can be used for more nefarious motives, like eavesdropping and censorship. Between those two extremes is a grey area of datamining and privacy violation, and it's these aspects that are raising hackles in some parts of the web.":* D. GEERE, "How deep packet inspection works", Wired, Publié le 27 avril 2012: https://www.wired.co.uk/article/how-deep-packet-inspection-works

[1535] Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte), Cons. 8 ou Partie VIII par ex.

[1536] G. WELCHMAN, The Hut Six story – Breaking the Enigma codes, McGraw-Hill, 1982, 326 p.; et, A. J. MARTIN, "Bletchley Park remembers 'forgotten genius' Gordon Welchman", The Register UK, publié le 27 septembre 2015: "*The analysis programme, named "Sixta", was a fusion of traffic analysis and cryptography. In a personal paper titled A Personal Record, written shortly before his death in 1984, Welchman stated:* ***No-one else was doing anything about this potential goldmine; so, I drew up a comprehensive plan which called for close coordination of radio interception, analysis of the intercepted traffic, the breaking of Enigma keys, and extracting intelligence from the decodes***.": https://www.theregister.co.uk/2015/09/27/gordan_welchman_bletchley_park_remembers/

stratégique de la Grande-Bretagne, ces critères de sélection et de recherche peuvent être aussi larges que : tout le trafic à destination et en provenance de la France, toutes les requêtes de recherche sur Google, tous les achats faits sur Amazon, toutes les données de localisation, ou un large éventail d'adresses IP[1537]. En outre, les documents ont également révélé l'installation de matériels de surveillance spécifiques au sein même des locaux des entreprises de télécommunication, mais aussi leurs capacités et puissances de traitement dans le cadre de ces salles protégées et secrètes, à l'image du *Narus Semantic Traffic Analyser*, un outil puissant pour l'inspection approfondie de paquets - DPI[1538]. Et du côté de l'Europe, l'Institut européen des normes de télécommunication (ETSI) vise à « *contraindre les fournisseurs d'informatique en nuage – Cloud computing – à concevoir des «capacités d'interception légales» dans la technologie nuagique pour permettre aux pouvoirs publics d'accéder directement aux contenus stockés par ces prestataires, y compris aux courriels, messages et messages vocaux* »[1539]. Les différentes atteintes aux droits et libertés fondamentales, notamment au droit à la vie privée, pouvant en découler paraissent, dans ce contexte, évidentes.

Les pratiques de cybersurveillance en masse consistent finalement à intercepter aussi bien le contenu que les métadonnées. L'interception, la conservation et l'analyse des métadonnées sont tout aussi intrusives que les autres interférences du même genre dans les communications. Les métadonnées sont l'équivalent numérique d'un détective privé qui suit un individu en tout temps, enregistrant la totalité des déplacements et des conversations effectués. Or, dans le

---

[1537] Privacy International, "UK mass interception law violates human rights - but the fight against mass surveillance continues", publié le 13 septembre 2018 : "*Intercepted information is stored in databases, which government analysts can query, data-mine or use to call up information to examine further. This process provides the UK intelligence agencies with a vast trove of content and metadata (referred to as "communications data" in the judgment) that is capable of revealing the most intimate details of anyone who uses online communications*.": https://privacyinternational.org/feature/2267/uk-mass-interception-law-violates-human-rights-fight-against-mass-surveillance

[1538] Electronic Frontier Foundation (EFF), NSA Spying – How it works, publié en 2017: "*It works like this: when you send an email or otherwise use the internet, the data travels from your computer, through telecommunication companies' wires and fiber optics networks, to your intended recipient. To intercept these communications, the government installed devices known as "fiber-optic splitters" in many of the main telecommunication junction points in the United States (like the AT&T facility in San Francisco). These splitters make exact copies of the data passing through them: then, one stream is directed to the government, while the other stream is directed to the intended recipients*.": https://www.eff.org/nsa-spying/how-it-works ou http://www.acamedia.info/politics/surveillance/references/eff/How_the_NSAs_Domestic_Spying_Program_Works.pdf

[1539] ETSI, Technical Report : Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD), ETSI TR 101 567 V1.1.1 (2016-01), Reference: DTR/LI-00084, 2016: https://www.etsi.org/deliver/etsi_tr/101500_101599/101567/01.01.01_60/tr_101567v010101p.pdf ; et, Assemblée générale des Nations-Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, du 17 avril 2013, Conseil des droits de l'homme 23ème session, A/HRC/23/40, p. 11, point 35 ; disponible en ligne : https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/04/PDF/G1313304.pdf?OpenElement & https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

monde numérique, les métadonnées enregistrent bien plus : les activités en ligne, par exemple, qui peuvent révéler les articles achetés, les nouveaux sites web visités, les forums rejoints, les livres lus et les films regardés. Ensemble, elles permettent d'avoir une vision globale et intrusive dans la vie privée d'une personne, révélant son identité, ses relations, ses intérêts, ses activités, ses intentions et ses emplacements[1540]. Les pratiques computationnelles à des fins de surveillance, développées au cours du XXIe Siècle, se font ainsi plus précises, plus individualisées, plus dynamiques et plus intrusives variant entre des exploitations de caméra ou de micros intégrés dans un téléphone ou dans un téléviseur connecté et intelligent, des contrôles à distance des téléphones mobiles, des tablettes ou encore des véhicules connectés, pour n'en citer que quelques exemples ; le tout opéré dans le plus grand secret et avec la plus grande discrétion. Et l'ensemble s'opère quasiment dans l'ombre, sans examen ni consultation ou information du public.

Dans ces conditions, indiquaient les parlementaires en 1977, « *on peut se demander si le secteur public ne va pas être appelé à financer et à établir des fichiers directement utilisables par le privé sur le plan économique* »[1541].

§2. L'étendue de la suprématie informationnelle omniprésente

Les personnes derrière la masse de données ainsi récoltées et exploitées apparaissent dès lors comme le produit de cette suprématie informationnelle omniprésente qui fait, désormais, l'objet d'une collaboration pour une meilleure exploitation sous l'égide des secrets « d'État ou des affaires » (A), induisant par là même une alliance déconcertante et assez sensationnelle entre deux secteurs initialement distincts (B).

A. Un manque de transparence pour des motifs de « secret d'État » et de « secret des affaires »

Le concept de vie privée est aujourd'hui perçu de manière apophatique : les individus veulent maintenir leurs biens privés privés ; les entreprises connaissent l'importance de la *privacy* afin de ne pas faire l'objet de divulgations compromettantes exposant leur linge sale ou leurs petits secrets au monde, et vont même jusqu'à faire le nécessaire pour gagner plus en terme de confidentialité, de secret d'intimité, installant des alarmes, des serrures, des *firewalls* et des politiques de sécurité de l'entreprise ; et les gouvernements sont très à l'aise avec les concepts

[1540] Privacy International, "UK mass interception law violates human rights - but the fight against mass surveillance continues", du 13 septembre 2018, *Id.*

[1541] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit.*, p. 5786.

de « privé » et de « confidentialité » leur permettant de ne pas dévoiler leurs secrets militaires, qui, finalement, pourraient se retrouver entre des mauvaises mains.

Depuis les années 60 et le développement du secteur privé, les entreprises ont réussi à remettre en question avec succès le contrôle ou la surveillance de leurs activités par l'État et les institutions gouvernementales. L'agence de protection environnementale américaine a voulu, à un certain moment, publier des données sur la composition de certains pesticides, l'entreprise Monsanto a riposté et a réussi à obtenir de la Cour suprême une décision qui a empêché la divulgation d'informations au motif que les formules étaient un « secret industriel et commercial »[1542].

En général, les investigations et/ou divulgations touchaient les activités étatiques de surveillance ou de contrôle, toujours perçues comme celles opérées dans le secret pour des motifs de sécurité ou de défense par exemple, pouvant générer le plus d'impact en termes d'atteintes et d'ingérences aux droits des personnes. En effet, « *one of the truisms of national security is that secrecy is necessary in matters of intelligence, foreign policy and defense* »[1543]. Il est vrai que pendant une époque, la communication au public par l'État de certaines informations sur leurs capacités militaires par exemple, aurait accordé un avantage aux ennemis et aux adversaires qui auraient pu facilement retourner ces informations à leur avantage ; or, cette notion de secret militaire ou de secret-défense, bien que véridique et concrète depuis des millénaires, s'est récemment dramatiquement transformée[1544].

À la suite des événements du 11 septembre 2001, les États ont encouragé plus fortement le secret gouvernemental, arguant que le seul moyen de combattre efficacement le terrorisme était que l'État agisse aussi clandestinement que ses sombres adversaires ; le résultat qui en a découlé est que, désormais, presque tout peut être tenu secret.

[1542] U.S. Supreme Court, Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984), No. 83-196: "*However, under the statutory scheme in effect between October 22, 1972, and September 30, 1978, a submitter was given an opportunity to protect its trade secrets from disclosure by designating them as trade secrets at the time of submission. The explicit governmental guarantee to registration applicants of confidentiality and exclusive use with respect to trade secrets during this period formed the basis of a reasonable investment-backed expectation. If EPA, consistent with current provisions of FIFRA, were now to disclose such trade secret data or consider those data in evaluating the application of a subsequent applicant in a manner not authorized by the version of FIFRA in effect between 1972 and 1978, its actions would frustrate appellee's reasonable investment-backed expectation. […]*": https://supreme.justia.com/cases/federal/us/467/986/

[1543] B. SCHNEIER, *Data and Goliath*, *op. cit.*, p. 117.

[1544] B. SCHNEIER, *Data and Goliath*, *Id.*, p. 117, l'auteur explique ainsi, en prenant comme exemple les Etats-Unis, « *in World War I, we were concerned about the secrecy of specific facts, like the location of military units and the precise plans of a battle. In World War II, we extended that secrecy to both large scale operations and entire areas of knowledge. Not only was our program to build an atomic bomb secret; the entire science of nuclear weaponry was secret. After 9/11, we generalized further, and now almost anything can be a secret.* »

Par ailleurs, depuis les années 70, les pratiques du secteur privé comportent autant d'atteintes et d'ingérences, non révélées sous couvert du « secret commercial et industriel », et n'attirant pas, par conséquent, l'attention de l'opinion publique. Les entreprises se sont toujours efforcées de maintenir un avantage supplémentaire sur leurs concurrents, en classant leurs travaux novateurs comme « exclusifs » ou « confidentiels ». Depuis que les échanges informatisés ont permis de gagner ou de perdre des fortunes en l'espace de quelques secondes, l'avantage et la suprématie de l'information sont devenues cruciales dans l'ensemble des secteurs de l'économie : « *Some economists began to question the wisdom of regulating, or even monitoring, the fast-moving corporate world. Some failed to disclose that they were being paid for "consulting" by the same secretive corporations their writings supported. Business schools taught MBAs the basics of game theory, which stressed the importance of gaining an information advantage over rivals* »[1545]. De plus, depuis que le recours à des techniques furtives et secrètes a commencé à générer encore plus de profits aux entreprises, le classement en « exclusif », « confidentiel », ou encore en « secret des affaires » est devenu très attrayant au sein du secteur privé. Ce fut une des stratégies de Google ayant précieusement conservé sa « sauce secrète » : son algorithme complexe d'évaluation de sites[1546].

En France, une loi relative à la protection du secret des affaires votée en 2018[1547] a remplacé la notion de « secret industriel et commercial » par « secret des affaires », élargissant en quelque sorte sa portée. Aux termes de cette loi, « *est protégée au titre du secret des affaires toute information répondant aux critères suivants : 1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ; 2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ; 3° Elle fait l'objet de la part de son détenteur légitime de mesures de*

[1545] F. PASQUALE, *The Black Box society, op. cit.*, p. 12-13.

[1546] F. FILLOUX, « Google News: The secret sauce », The Guardian, publié le 25 février 2013: "*Ten years after its launch, Google News' raw numbers are staggering: 50,000 sources scanned, 72 editions in 30 languages. Google's crippled communication machine, plagued by bureaucracy and paranoia, has never been able to come up with tangible facts about its benefits for the news media it feeds on. Its official blog merely mentions "6 billion visits per month" sent to news sites and Google News claims to connect "1 billion unique users a week to news content" (to put things in perspective, the NYT.com or the Huffington Post are cruising at about 40 million UVs per month). Assuming the clicks are sent to a relatively fresh news page bearing higher value advertising, the 6 billion visits can translate into about $400m (£264m) per year in ad revenue. (This is based on a $5 to $6 revenue per 1,000 pages, i.e. a few dollars in CPM per single ad, depending on format, type of selling, etc.) That's a very rough estimate. […]*': https://www.theguardian.com/technology/2013/feb/25/1

[1547] Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, Art. 1 – Crée Code de commerce - Art. L 151-1 (V)

protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret »[1548].

Définis ainsi, ces critères sont assez larges et vagues, laissant pas mal de marges de manœuvre, et pouvant potentiellement accorder une protection au motif du « secret des affaires » à n'importe quelle information détenue par les entreprises privées. L'intégralité du modèle économique des géants du web peut ainsi ne jamais être dévoilé au titre de la transparence pour des motifs de « secret des affaires », leur permettant *ipso facto* de garder une emprise dominante sur l'économie numérique, absorbant automatiquement toute nouvelle concurrence. Un nouveau concept émergent, exploité initialement et prodigieusement par Google, illustre bien ce manque de transparence pour des raisons de « secret des affaires » : c'est le « Data exhaust »[1549].

Actuellement, Google détient sans doute le correcteur orthographique, « *spell-checker* », le plus complet et le plus performant au monde ; le système se perfectionnant constamment, ajoutant continuellement de nouveaux mots. L'entreprise a d'apparence obtenu gratuitement son correcteur d'orthographe, réutilisant les fautes d'orthographes saisies dans son moteur de recherche parmi les trois milliards de requêtes traitées chaque jour : une boucle de rétroaction intelligente donne des instructions au système sur quel mot les utilisateurs entendaient réellement taper. Ainsi, dans certains cas, ce sont les utilisateurs eux-mêmes qui 'signifient' explicitement à Google la réponse à la question posée en haut de la page de résultat – « Did you mean » épidémiologie ou épidémie ou n'importe quelle autre entrée – en cliquant directement dessus pour commencer une nouvelle recherche avec le terme correct, contribuant, à leurs insu, au perfectionnement du système. D'autres fois, c'est la page web visitée par les utilisateurs qui signale implicitement la bonne orthographe, la page web étant probablement plus étroitement

[1548] Art. L 151-1 Code de commerce – Créé par la loi du 30 juillet 2018.

[1549] "*Unstructured information or data that is a by-product of the online activities of Internet users: Collecting and analyzing data exhaust can provide valuable insight into the purchasing habits of consumers*.", nommé également "Digital exhaust", Dictionary.com: https://www.dictionary.com/browse/data-exhaust; K. NOYES, "5 things you need to know about Data exhaust", Computerworld – IDG News Service, publié le 13 mai 2016: "*The "data exhaust" term has been around for more than a decade, and it arose with the new streams of data coming from smartphones, [...]. Today, more accessible data tools are bringing exhaust to the fore. If big data is "primary" data that relates to the core function of your business, data exhaust is secondary data, or everything else that's created along the way, [...]. There are no standard definitions or schemas for data exhaust, which tends to be raw and unstructured, but in many ways, it's equivalent to the byproducts associated with a company's machines and core online activities. It can include streams coming in from Web browsers, plug-ins, log files, Internet of Things (IoT) devices, and more*." : https://www.computerworld.com/article/3070475/5-things-you-need-to-know-about-data-exhaust.html ; K. HYDE, "What Is Data Exhaust? Cutting Through the Fumes", Capture Higher Ed, publié le 13 juin 2017: https://capturehighered.com/predictive-modeling/data-exhaust-cutting-fumes/

corrélée avec le mot correctement orthographié qu'avec le mot incorrect[1550]. Le système de vérification orthographique de Google montre que les données 'mauvaises', 'incorrectes' ou 'défectueuses' peuvent néanmoins être encore très utiles : « *only Google recognised that the detritus of user interactions was actually gold dust that could be gathered up and forged into a shiny ingot* »[1551].

Là où Google a compris l'utilité profonde d'un tel système, Microsoft n'a simplement perçu la valeur de la vérification orthographique que dans un seul but précis : le traitement de texte. Et Google ne s'est pas arrêtée là : l'entreprise ne s'est pas seulement servie des coquilles (des erreurs, typos) pour développer le meilleur, et le plus actualisé, vérificateur orthographique du monde afin d'améliorer la recherche, mais elle a adopté ce système pour de nombreux autres services, tels que la fonction « autocomplete », d'auto-complétion de la recherche, Gmail, Google Docs ou encore son système de traduction[1552].

Émergea alors le concept décrivant les traces numériques que les personnes laissent dans leur sillage : le « data exhaust » qui fait référence à des données et traces générées comme sous-produits, ou produits dérivés des actions et mouvements des personnes dans le monde[1553]. Transposé dans le monde numérique, ce concept décrit les interactions en ligne des utilisateurs : où ils cliquent, combien de temps ils regardent une page, où le curseur de la souris rôde, ce qu'ils frappent sur leurs claviers, leurs actions et préférences en matière de fichiers logs et bien plus. De nombreuses entreprises conçoivent leurs systèmes de façon à pouvoir récolter, en toute discrétion, les *data exhaust* et les recycler pour en tirer des bénéfices[1554]. Google en est toutefois

---

[1550] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *op. cit.*, p. 112: "*This is more important than it may seem: as Google spell check continually improved, people stopped bothering to type their searches correctly, since Google could process them well regardless*".

[1551] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Id.*, p. 112-113.

[1552] Par ex., Google Search Help, Web Search – How autocomplete works: https://support.google.com/websearch/answer/106230?hl=en-FR

[1553] "*Data exhaust refers to the data generated as trails or information byproducts resulting from all digital or online activities. These consist of storable choices, actions and preferences such as log files, cookies, temporary files and even information that is generated for every process or transaction done digitally. This data can be very revealing about an individual, so it is very valuable to researchers and especially to marketers and business entities*", Technopedia, "Data Exhaust": https://www.techopedia.com/definition/30319/data-exhaust

[1554] The Economist, « Clicking for gold – How the internet companies profit from data on the Web », *In* Special Report: Data, Data everywhere, publié le 27 février 2010: "*Amazon.com does not want you to know what it knows about you. It not only tracks the books you purchase, but also keeps a record of the ones you browse but do not buy to help it recommend other books to you. Information from its e-book, the Kindle, is probably even richer: how long a user spends reading each page, whether he takes notes and so on. But Amazon refuses to disclose what data it collects or how it uses them.*

It is not alone. Across the internet economy, companies are compiling masses of data on people, their activities, their likes and dislikes, their relationships with others and even where they are at any particular moment—and keeping mum. For example, Facebook, a social-networking site, tracks the activities of its 400m users, half of whom spend an average of almost an hour on the site every day, but does not talk about what it finds. Google reveals a little but holds back a lot. Even eBay, the online auctioneer, keeps quiet. ":

le leader incontesté : elle applique récursivement le principe de « l'apprentissage à partir des données » à bon nombre de ses services ; « *every action a user performs is considered a signal to be analyzed and fed back into the system* »[1555]. Ces informations sont très précieuses et d'un grand intérêt, ayant une « valeur commerciale effective ou potentielle », et sont tenues entièrement secrètes, que ce soit leurs récoltes, contenus, agrégations, traitements ou analyses, au profit des géants du web sous l'égide du secret des affaires.

Ce système est dorénavant employé par de nombreuses entreprises du web tels que Facebook qui, à ses balbutiements, a examiné et exploité son riche réservoir de données sous-produits, les *data exhaust*. Or, celui-ci ne se limite plus au secteur du web et se propage bien au-delà, affectant n'importe quelle entreprise ayant les moyens de recueillir les commentaires et réactions des utilisateurs (*user feedback*). Le *data exhaust* caractérise le mécanisme qui régit de nombreux services, comme la reconnaissance vocale, les filtres anti-spam, la traduction de langue et bien d'autres. Quand un utilisateur indique à un programme de reconnaissance vocale qu'il a mal compris ses propos, il 'entraîne' en réalité le système à s'améliorer[1556]. L'ensemble de ces informations découlant de l'exploitation du *data exhaust* a une grande valeur commerciale et est maintenu secret, non dévoilé au grand public qui utilise pourtant quotidiennement ces différents services, accordant par là même aux entreprises un énorme avantage concurrentiel ainsi qu'une puissante barrière à l'entrée d'entreprises concurrentes[1557]. En effet, dans ce contexte, il semble que « *the less known about our algorithms—by spammers, hackers, cheats, manipulators, competitors, or the public at large—the better, went the new reasoning. Transparency was replaced by ironclad secrecy, both real and legal* »[1558].

Dans les années 90, internet et son fondateur promettaient un nouveau monde de ressources libre, gratuit, ouvert, un espace universel, une ère de transparence accessible à tout le monde, dans lesquels l'ouverture à l'information et au savoir circulant sur la Toile ainsi créée conduirait

---

https://www.economist.com/special-report/2010/02/27/clicking-for-gold &
https://www.economist.com/sections/special-reports?page=67

[1555] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Ibid.*, p. 113: "*For example, Google is acutely aware of how many times people searched for a term as well as related ones, and of how often they clicked on a link but then returned to the search page unimpressed with what they found, only to search again. It knows whether they clicked on the eighth link on the first page or the first link on the eighth page – or if they abandoned the search all together. The company may not have been the first to have this insight, but it implemented it with extraordinary effectiveness*".

[1556] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Ibidem*, p. 114.

[1557] "How to Turn 'Data Exhaust' into a Competitive Edge", Knowledge@Wharton, The Wharton School, University of Pennsylvania, publié le 1er mars 2018: https://knowledge.wharton.upenn.edu/article/turn-iot-data-exhaust-next-competitive-advantage/ ; D. NEEF, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization and Digitally Driven Innovation*, FT Press Analytics, Ed. Pearson FT Press, 2014, 320 p.; V. MAYER-SCHÖNBERGER & K. CUKIER, *Big Data*, *Ibidem.*, p. 114-115; B. SCHNEIER, *Data and Goliath*, *Id.*, p. 45-47; F. PASQUALE, *The Black Box society*, *Id.,* p. 94-95.

[1558] F. PASQUALE, *The Black Box society*, *Ibid.,* p. 193.

à une liberté profonde et exceptionnelle. Le constat prononcé trente ans après sa création fut : « *de l'utopie à un capitalisme de surveillance* »[1559].

Les capacités acquises et les pouvoirs obtenus grâce au refus de transparence pour des raisons de 'secret' englobent confusément le secteur public. Mises à part les révélations sur les pratiques de surveillance susmentionnées, pratiques maintenues intégralement secrètes jusqu'à leurs révélations et considérées par certains comme illégales, les autorités publiques recourent au « secret d'État » et au « secret défense » de façon quasi-discrétionnaire et aléatoire. Presque tout ce qui touche aux pratiques effectuées par les services de renseignement et les services militaires est gardé secret pour des motifs de sécurité ou de défense et, depuis peu, les forces de police locales accroissent également leur niveau de discrétion. La directive 2016/680 dite directive sécurité et prévention, ou directive police-justice, vise à instituer une harmonisation et une coopération entre les régimes juridiques nationaux relatifs aux traitements à finalité répressive, en facilitant les échanges de données personnelles entre les autorités compétentes voire avec des entités privées[1560]. Ces harmonisation et coopération relatives à l'échange des données entre États membres existaient auparavant, la nouveauté étant que celles-ci s'appliquent, depuis l'entrée en vigueur de la directive, aux traitements de fichiers nationaux, notamment les fichiers de police et de justice comme le fichier de traitement d'antécédents judiciaires (TAJ)[1561] ou le fichier national des empreintes génétiques (FNAEG)[1562] en France.

[1559] F. JOIGNOT, « Les 30 ans du Web : de l'utopie à un capitalisme de surveillance », Le Monde – Enquête, Publié le 14 février 2019 : « Son inventeur, l'informaticien britannique Tim Berners-Lee, ne s'y résout pas : sa créature lui a échappé, l'utopie d'Internet a déraillé. » : https://www.lemonde.fr/pixels/article/2019/02/14/les-30-ans-du-web-de-l-utopie-a-un-capitalisme-de-surveillance_5423578_4408996.html#xtor=AL-32280270

[1560] Directive 2016/680, Cons. 11 « *[…]. Les autorités compétentes en question peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive. […]. » ;* et Cons. 25 « *Tous les États membres sont affiliés à l'Organisation internationale de police criminelle (Interpol). Pour exécuter sa mission, Interpol reçoit, conserve et diffuse des données à caractère personnel pour aider les autorités compétentes à prévenir et à combattre la criminalité internationale. Il est dès lors approprié de renforcer la coopération entre l'Union et Interpol en favorisant un échange efficace de données à caractère personnel […]. »*

[1561] « *Le traitement d'antécédents judiciaires (TAJ) est un fichier commun à la police et à la gendarmerie nationale, en remplacement des fichiers STIC de la police nationale et JUDEX, de la gendarmerie nationale, qui ont été définitivement supprimés. le traitement d'antécédents judiciaires (TAJ), en application des articles 230-6 à 230-11 du Code de procédure pénale, est utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d'infractions) et d'enquêtes administratives (comme les enquêtes préalables à certains emplois publics ou sensibles).* » : CNIL, « TAJ : Traitement d'Antécédents Judiciaires », publié le 15 novembre 2018 : https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires & https://www.service-public.fr/particuliers/vosdroits/F32727

[1562] « *Le FNAEG sert à faciliter l'identification et la recherche des auteurs d'infractions à l'aide de leur profil génétique, et de personnes disparues à l'aide du profil génétique de leurs descendants ou de leurs ascendants. Le FNAEG centralise les empreintes génétiques de : personnes non identifiées (empreintes issues de prélèvements sur les lieux d'une infraction) et de personnes identifiées (personnes condamnées ou mises en cause pour une des infractions listées à l'article 706-55 du code de procédure pénale).*

En outre, à la suite des attentats de Londres en 2017, la Commission européenne a manifesté le souhait d'élaborer un nouveau projet de loi facilitant l'accès des autorités répressives aux données personnelles détenues par les entreprises du web[1563] et a proposé un renforcement du système d'information Schengen (SIS), proposition adoptée par le Conseil de l'Union[1564]. C'est ce que B. Schneier nomme les systèmes GAK « Government access to keys », les accès du gouvernement aux clés, comportant tous des portes dérobées « backdoors » et partageant deux éléments essentiels : «*first, a mechanism, external to the primary system, by which a third party can obtain covert access to the plaintext of encrypted data ; and second, the existence of a highly sensitive secret recovery key (or collection of keys) that must be secured for an extended period of time. On the policy side, GAK systems need to give police timely access to plaintext, without notifying the user* »[1565]. Par ailleurs, les autorités publiques n'hésitent pas à se cacher derrière les accords de confidentialité signés par ou avec les entreprises, refusant ainsi de divulguer les détails des algorithmes de police prédictive et préventive développés à l'échelle

---

Les empreintes sont complétées des informations suivantes : Les nom, prénoms, date et lieu de naissance, filiation et sexe ; le service ayant procédé à la signalisation ; la date et le lieu d'établissement de la fiche signalétique ; la nature de l'affaire et la référence de la procédure.», CNIL, « FNAEG : Fichier national des empreintes génétiques », publié le 15 novembre 2018 : https://www.cnil.fr/fr/fnaeg-fichier-national-des-empreintes-genetiques ; et, Pôle judicaire de la gendarmerie nationale (PJGN), Le Fichier National Automatisé des Empreintes Génétiques (FNAEG), « *Potentialités du fichier : Ces dernières années, le FNAEG a connu plusieurs développements, notamment en matière de lutte contre la criminalité transfrontalière à travers l'accélération des échanges de données génétiques entre États européens et sur ses modalités d'utilisation avec la mise en œuvre de la recherche en parentalité.* » : https://www.gendarmerie.interieur.gouv.fr/pjgn/IRCGN/Division-Criminalistique-Biologie-et-Genetique-DCBG/Le-Fichier-National-Automatise-des-Empreintes-Genetiques-FNAEG

[1563] A. ORSINI, « Terrorisme : Bruxelles veut faciliter l'accès de la police aux données personnelles sur Facebook et Google en Europe », numerama, publié le 8 juin 2017 : https://www.numerama.com/politique/264933-terrorisme-bruxelles-veut-faciliter-lacces-de-la-police-aux-donnees-personnelles-sur-facebook-et-google-en-europe.html; C. STUPP – Traduction de M. CANDAU, « Bruxelles veut faciliter l'accès de la police aux données chiffrées », Euractiv, publié le 19 octobre 2017 : https://www.euractiv.fr/section/economie/news/brussels-promises-more-police-access-to-encrypted-data-but-no-backdoors/ ; J. FIORETTI, « EU seeks to expedite police requests for data from tech firms », Reuters, publié le 8 juin 2018 : https://www.reuters.com/article/us-eu-data-security-idUSKBN18Z0H0?feedType=RSS&feedName=technologyNews

[1564] Commission européenne - Communiqué de presse, « Union de la sécurité : adoption du système d'information Schengen renforcé », Bruxelles, le 19 novembre 2018 : « Le SIS renforcé comprendra, entre autres, les améliorations suivantes : *[...] une interopérabilité améliorée : le SIS renforcé permettra une utilisation plus efficace des empreintes digitales, des empreintes palmaires et des images faciales pour identifier les suspects. Les améliorations visent également à assurer la pleine interopérabilité du SIS avec les autres systèmes de l'UE en matière de migration, de gestion des frontières et de sécurité ; L'amélioration de l'accès pour les agences de l'UE : Europol aura désormais accès à toutes les catégories de signalements dans le SIS, tandis que les équipes opérationnelles de l'Agence européenne de garde-frontières et de garde-côtes pourront accéder au SIS afin d'accomplir leurs tâches dans les centres d'accueil et d'enregistrement et aux frontières extérieures. »* : http://europa.eu/rapid/press-release_IP-18-6450_fr.htm ; Commission européenne - Communiqué de presse, « Union de la sécurité: la Commission comble les lacunes en matière d'information afin de mieux protéger les citoyens de l'Union », Strasbourg, le 12 décembre 2017 : « *Ces mesures permettront l'échange d'informations et le partage de données entre les différents systèmes et assureront aux garde-frontières et aux agents de police un accès aux informations pertinentes exactement au moment et à l'endroit où ils en ont besoin pour s'acquitter de leur mission [...]» :* http://europa.eu/rapid/press-release_IP-17-5202_fr.htm

[1565] B. SCHNEIER, *Secrets & Lies*, *op. cit.*, p. 241-242.

commerciale. De plus, la transformation du secret d'État et de son emploi réside dans la manière dont il est exercé s'avérant être à un niveau extrême, en recourant aux classifications et à la hiérarchisation des informations pour maintenir une suprématie informationnelle : « *knowledge is currency, and the intelligence community is hoarding it* »[1566].

Il semble bien que les manifestations de plus en plus récurrentes alimentant le « secret d'État » tiennent au fait que les gouvernements condamnent, pour la plupart, sévèrement les personnes révélant des informations classées secret d'État, décourageant ainsi toute révélation sur leurs pratiques secrètes légalement protégées : ce fut le cas de Snowden, Manning[1567], Drake ou Ellsberg[1568]. *In fine*, dans la mesure où la surveillance étatique exige le secret et la discrétion, les citoyens n'ont plus la capacité de débattre ou de voter sur ce que le gouvernement entreprend en leur nom, ni de signifier à leurs élus leur opinion sur la démarche à suivre ou la position à prendre. Dans le secret, toute personne n'a plus le moyen de pouvoir librement s'exprimer sur une question ou sur un sujet puisqu'elle est tenue intentionnellement dans l'ignorance ; et la stratégie du « secret » touche indifféremment le secteur public comme le secteur privé : « *these secrets are usually military in nature : strategy and tactics, weapon capabilities, designs and procurements, troop strengths and movements, research and development. Military secrets often broaden into state secrets: negotiating positions on treaties and the like. And they often overlap into corporate secrets: military contracts, bargaining positions, import and export dealings, and so forth* »[1569].

Il y a un célèbre adage qui dit « le savoir, c'est le pouvoir »[1570] et pouvoir observer, surveiller les autres tout en évitant d'être soi-même surveillé caractérise l'une des plus importantes formes de pouvoir. Comme le précise Foucault, « *il faut plutôt admettre que le pouvoir produit du savoir (et pas simplement en le favorisant parce qu'il le sert ou en l'appliquant parce qu'il est*

[1566] B. SCHNEIER, *Data and Goliath*, *Ibid.*, p. 119.

[1567] "*U.S. Army intelligence analyst Bradley Manning delivered hundreds of thousands of classified documents that he found troubling to WikiLeaks, and in 2013 was sentenced to 35 years in prison for espionage and theft*", Biography.com Editors, Chelsea Manning Biography, Initialement publié le 2 avril 2014, Mis à jour le 12 avril 2019: https://www.biography.com/activist/chelsea-manning

[1568] Dr. Daniel Ellsberg "was a U.S. military analyst who, while employed by the RAND Corporation in 1971, released the Pentagon Papers, a top-secret Pentagon study of U.S. government decision-making in relation to the Vietnam War, to The New York Times.", CBS News, Famous Whistleblowers: https://www.cbsnews.com/pictures/famous-whistleblowers/ ; "Born in Chicago in 1931, military strategist Daniel Ellsberg helped strengthen public opposition to the Vietnam War in 1971 by leaking secret documents known as the Pentagon Papers to the New York Times. The documents contained evidence that the U.S. government had misled the public regarding U.S. involvement in the war.", Biography.com Editors, Daniel Ellsberg Biography, Initialement publié le 2 avril 2014, Mis à jour le 12 avril 2019 : https://www.biography.com/activist/daniel-ellsberg ; http://www.ellsberg.net/bio/

[1569] B. SCHNEIER, *Secrets & Lies, Id.*, p. 61.

[1570] « *Scientia potestas est - Knowledge is power* » attribué à Sir Francis Bacon, Philosophe et théoricien de la science expérimentale (1561-1626) ; et *Cf.* p. 630.

utile) ; que pouvoir et savoir s'impliquent directement l'un l'autre ; qu'il n'y a pas de relations de pouvoir sans constitution corrélative d'un champ de savoir, ni de savoir qui ne suppose et ne constitue en même temps des relations de pouvoir »[1571]. Or, les entreprises recherchent des détails intimes sur la vie de leurs employés et clients potentiels, mais fournissent aux organismes régulateurs le moins d'informations possibles sur leurs propres statistiques et procédures ; les géants du web collectent de plus en plus de données sur leurs utilisateurs, mais luttent contre des réglementations qui permettraient à ces mêmes utilisateurs d'exercer un certain contrôle sur les dossiers et profils numériques qui en résultent.

Et à mesure que la technologie progresse et évolue, les pressions du marché augmentent la mise du jeu que constituent les données : les caméras de surveillance deviennent moins chères chaque année et plus facilement disponibles sur le marché, les capteurs sont intégrés dans plus d'endroits, les nouveaux matériels et logiciels promettent de faire de nous des êtres quantifiés, « quantified self »[1572], que cela nous plaise ou nous déplaise[1573]. Les informations qui en résultent, une quantité massive de données collectées de manière ubiquiste, sont systématiquement introduites et ajoutées dans les bases de données et assemblées en profils d'une ampleur et d'une précision sans précédents. La légalisation du secret d'État et du secret des affaires participe à ce manque de transparence de plus en plus observé, et vis-à-vis duquel plusieurs auteurs et juristes perdent foi et remettent en question le principe même de transparence et son efficacité ou son effectivité, et, de ce fait, participe, également et simultanément, au déclin du respect de la vie privée des personnes.

Les autorités et organismes publics, les grandes banques, les organismes d'évaluation de crédit, les moteurs de recherche, les fournisseurs d'accès et bien d'autres recueillent des données personnelles pour les convertir en suspects, listes de surveillance, calculs de risques, scores, notes - notations, ou classements, présentant des conséquences majeures, mais les algorithmes

---

[1571] M. FOUCAULT, *Surveiller et Punir*, Coll. Tel, Ed. Gallimard, 1975 (Impression de 2013), p. 36 ; l'auteur précise ainsi que « *ces rapports de « pouvoir-savoir » ne sont donc pas à analyser à partir d'un sujet de connaissance qui serait libre ou non par rapport au système du pouvoir ; mais il faut considérer au contraire que le sujet qui connaît, les objets à connaître et les modalités de connaissance sont autant d'effets de ces implications fondamentales du pouvoir-savoir et de leurs transformations historiques [...].* ».

[1572] *Cf.* p. 156.

[1573] A. ZASLAVSKY, « September 2013 Theme: Internet of Things and Ubiquitous Sensing », Tech News – Computing now, IEEE Computer Society: "*A pillar of the Future Internet, the Internet of Things (IoT) will comprise many billions of Internet-connected objects (ICOs) or "things" that can sense, communicate, compute, and potentially actuate, as well as have intelligence, multimodal interfaces, physical/virtual identities, and attributes. The IoT incorporates concepts from pervasive, ubiquitous, and ambient computing, which have been evolving since the late '90s and have now reached some level of maturity. It fuses the digital and physical worlds by bringing different concepts and technical components together. Along with the World Wide Web and mobility, IoT potentially represents the most disruptive technological revolution to date. With billions of ICOs and a diverse abundance of sensors, the IoT will be an enabler of ubiquitous sensing*": https://www.computer.org/publications/tech-news/computing-now/internet-of-things-and-ubiquitous-sensing

propriétaires ou commerciaux par lesquels ils procèdent sont à l'abri de tout examen pour des motifs de secret des affaires. De plus, la protection du secret commercial crée effectivement un droit de propriété sur un algorithme, sans exiger sa divulgation, et renforce l'importance de tenir les algorithmes secrets, puisqu'une fois publiés, ils perdent *de facto* la protection accordée par la loi. Parallèlement, les règles en matière de secret d'État constituent un arsenal juridique encore plus redoutable lorsque la sécurité nationale est en jeu : « *This move from legitimation-via-transparency to protection-via-secrecy was the soil out of which the black box society sprang, and with it, many of the social dangers of the information age* »[1574].
Comme le précise le Professeur, « *Black boxes embody a paradox of the so-called information age: Data is becoming staggering in its breadth and depth, yet often the information most important to us is out of our reach, available only to insiders* ».[1575]

B. L'alliance déconcertante et sensationnelle entre État et marché

À l'heure actuelle, avec le nouveau défi que représente le cyberespace et sa conquête, la direction que prend la surveillance apparaît être d'essence unilatérale : les gouvernements et les entreprises se sont effectivement unis pour se concentrer, exclusivement et massivement, sur les citoyens. Contrairement à d'autres domaines ou milieux, nommément le domaine militaire, la terre, la mer, l'air ou l'espace, le cyberespace « *[…] n'est pas un milieu naturel – tout ce qui s'y passe est le produit de l'action humaine – et il est transverse à tous les autres domaines* »[1576]. La quantité massive de données collectées par les entreprises privées en font des partenaires précieux privilégiés pour le partage d'informations, et il existe en réalité pas mal de marge de manœuvre pour l'échange et le traitement dans les deux sens : public-privé. Ainsi, les autorités publiques veulent les données qu'elles ne peuvent d'elles-mêmes recueillir légalement ou constitutionnellement, les courtiers en données, *data brokers*, les détiennent et veulent les vendre, et d'autres types d'entreprises peuvent aisément entreprendre d'autres sortes de transactions concernant les données personnelles. Dans ce contexte, « *the government's interest in intelligence gathering has led it into a pragmatic, powerful, and largely secret partnership with interests whose concern is not the public good, but private profit or personal advance* »[1577].

[1574] F. PASQUALE, *The Black Box society*, *op. cit.,* p. 193.
[1575] F. PASQUALE, *The Black Box society*, *Id.,* p. 191.
[1576] F. DOUZET, « La géopolitique pour comprendre le cyberespace », *In* Hérodote N° 152-153, *Cyberespace : Enjeux géopolitiques*, La Découverte, 2° trimestre 2014, p. 13.
[1577] F. PASQUALE, *The Black Box Society*, *Ibid.,* p. 43.

De nos jours, il semble évident qu'avec le Big data, la valeur, au sens large, des données évolue drastiquement. À l'ère du numérique, les données ont manifesté leur rôle d'appui aux opérations et sont souvent devenues le produit même faisant l'objet de transactions, de négoces et de commerces. Dans le monde du Big data, la donne change encore et évolue : la valeur des données se déplace de leur utilisation principale instantanée à leur utilisation future potentielle. Ce décalage entraîne de nombreuses conséquences ayant une incidence sur la manière dont les entreprises évaluent les données qu'elles détiennent, et sur les individus ou entités à qui elles accordent l'accès auxdites données, ou permettant, voire forçant les entreprises à modifier leur business modèle d'affaires ; *in fine*, ce changement modifie la façon dont les organisations perçoivent les données et leurs utilisations.

L'information a toujours été essentielle dans les transactions de marché, les données permettant la découverte et la détermination des prix pour une production plus optimale par exemple, le contenu des livres, articles, musiques ou films a souvent fait l'objet de transactions financières, tout comme les informations financières et le cours des actions. Le décalage s'observe néanmoins à travers le fait que s'ajoutent à ces informations, depuis les quelques dernières décennies, les données à caractère personnel. En conséquence, des courtiers en données spécialisés, tels que Acxiom[1578], Experian[1579] ou Equifax[1580], facturent généreusement pour des

[1578] Acxiom provides the data, technology, and services you need to power exceptional customer experiences everywhere: https://www.acxiom.com, Our capabilities: Our leading capabilities in identity, data stewardship, and integrations help you understand your customers and engage them everywhere: https://www.acxiom.com/what-we-do/

[1579] Experian marketing services: Connect the dots of consumer identity - Link together disparate systems of audience insights and engagement. Whether you're a brand, agency, or publisher, Experian wants to help you put people at the heart of your business. Our consumer data, cross-channel media partnerships, and marketing campaign measurement capabilities make Experian the connective marketing tissue for thousands of brands around the globe. If you're ready to know more about your customers than ever before, reach them across channels and discover just how effective your marketing is, let's get to work together: https://www.experian.com/marketing-services/marketing-services.html ; About Experian - We unlock the power of data to create opportunities for people, business and society: Our world is built on data. It's all around us, growing in power and influence every day. We work to turn that data into something meaningful. We gather, analyse, combine and process it to help people and organisations achieve their goals – whether that means planning for a secure future or getting to know your customers better: https://www.experian.co.uk/about-us/index.html ; Experian Marketing Suite : Integrate customer Identity, Intelligence, and Interactions with the Experian Marketing Suite's award award-winning technology and best-in-class services. Resolve identities across channels, link complex data to build rich customer personas and create personalised, 1-2-1 engagements with a single, simple and comprehensive platform. Harness the world's most flexible and comprehensive cloud-based marketing platform used by more than 10,000 of the world's leading brands and access the largest global account teams, strategists, statisticians and data scientists. Link data, advertising and marketing technologies to reach the right audiences, maximise the value of every customer relationship and inspire long-term brand advocacy: https://www.experian.co.uk/marketing-services/marketing-suite/index.html

[1580] Equifax is a global data, analytics, and technology company. We believe knowledge drives progress. We blend unique data, analytics, and technology with a passion for serving customers globally, to create insights that power decisions to move people forward. Headquartered in Atlanta, Equifax operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region : https://www.equifax.com/about-equifax/company-profile/ ; Equifax offers Products and solutions for Government areas and needs, such as leverage analytics or verify information:

dossiers détaillés dans lesquels figurent des informations personnelles sur des centaines de millions de consommateurs, utilisateurs. Avec Facebook, Twitter, LinkedIn, et d'autres plateformes de réseaux sociaux, les connections personnelles, opinions, préférences et les schémas de vie au quotidien ont rejoint le bassin d'informations personnelles déjà disponible. En effet, à l'ère du Big data, toutes les données sont intrinsèquement considérées comme utiles et précieuses, même les données les plus crues, voire des parcelles d'informations d'apparence banale ou anodine.

L'ensemble de ces informations fait aujourd'hui, dans le monde des données produites en masse, l'objet de convoitises mais surtout l'objet de nombreux échanges entre les entreprises et les gouvernements, caractérisant leur alliance fortuite et surprenante. Les évènements marquants le début du XXI[e] Siècle ont modifié le climat et le contexte, ouvrant la voie à une circulation plus aisée de l'information du secteur privé vers le secteur public pour diverses raisons (défense, sécurité, opérations sensibles, etc.). Des universités américaines ont ainsi accordé l'accès aux dossiers sur leurs étudiants étrangers aux autorités publiques, souvent sans assignation ou ordonnance judiciaire[1581]. La compagnie aérienne JetBlue, en violation de sa propre politique de confidentialité, a partagé les informations personnelles d'un million de ses passagers avec l'entreprise Torch Concepts, une entreprise militaire ayant conclu un contrat avec le Ministère de la Défense américain pour établir des profils de passagers pouvant menacer la sécurité. Cette entreprise combinait les données de la compagnie JetBlue avec les numéros de sécurité sociale, les informations sur l'emploi et d'autres détails obtenus de l'entreprise Acxiom précitée[1582]. Le tout s'est fait au nom de la sécurité ou de la défense dans l'univers du

---

https://www.equifax.com/government/ ; What you need to know: Equifax® 3-Bureau credit scores are each based on the Equifax Credit Score model, but calculated using the information in your Equifax, Experian® and TransUnion® credit files: https://www.equifax.com/personal/

[1581] Par ex. : D. Eggen & C. W. Thompson, "INS to monitor foreign students", The Washington Post, publié le 11 mai 2002: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiW8PKCvuvhAhUHUBoKHf-ADgEQFjAAegQIARAB&url=https%3A%2F%2Fwww.washingtonpost.com%2Farchive%2Fpolitics%2F2002%2F05%2F11%2Fins-to-monitor-foreign-students%2Fe29d277e-bbc3-4ba9-9db7-59c995e585ce%2F&usg=AOvVaw1MI3HpXYOwydtOlQxzFHJV

[1582] D. PHILLIPS, "JetBlue apologizes for use of Passenger Records", The Washington Post, publié le 20 septembre 2003: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjKpaSHv-vhAhVCRBoKHfT1BtsQFjAAegQIAxAB&url=https%3A%2F%2Fwww.washingtonpost.com%2Farchive%2Fbusiness%2F2003%2F09%2F20%2Fjetblue-apologizes-for-use-of-passenger-records%2F207e5529-db29-40f3-9e27-6195faed2bff%2F&usg=AOvVaw1Pbh23KrqFfeqpxaEgoeHl; P. SHENON, "JetBlue Chief Says He Wasn't Told About Release of Data", The New York Times, publié 25 septembre 2003: https://www.nytimes.com/2003/09/25/business/jetblue-chief-says-he-wasn-t-told-about-release-of-data.html ; D. SOLOVE, *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004, p. 171, où l'auteur indique que : "*In a similar incident, Northwest Airlines secretly turned over to NASA its*

cyberespace et des données en masse où tout le monde peine à tout contrôler mais tout le monde aspire férocement à pouvoir le faire. En effet, les enjeux et risques liés au cyberespace sont tels qu' « *il en va de la puissance économique et financière des nations, au point que les intérêts du secteur privé rejoignent ceux de la nation et que la cybersécurité des entreprises puisse relever de l'intérêt national. Il va sans dire que le marché de la cybersécurité est aussi sensible que florissant, ce qui encourage également les gouvernements à s'impliquer* »[1583].

Il arrive aussi que les entreprises soutiennent l'appareil de renseignement simplement pour obtenir un avantage concurrentiel : ce fut le cas de la compagnie Boeing qui a bénéficié d'un accès en temps réel aux informations des centres de fusion du bureau d'échange de renseignement grâce à sa participation au Centre d'analyse conjoint de Washington. Selon un conseiller principal de Boeing, R. Hovel, « *Boeing wants to set an example of how private owners of critical infrastructure can get involved in such centers to generate and receive criminal and anti-terrorism intelligence* », et explique que « *the private sector, which owns about 80 percent of critical infrastructure, needs to have real-time access to information from the fusion centers. At the same time, the fusion centers need access to "mature intelligence capabilities" in private companies* »[1584]. Des géants du marché comme Amazon ou Starbucks ont, par la suite, également manifesté leur intérêt dans ce modèle de partenariat[1585], d'autant que cette alliance leur permet de jouir de nombreux privilèges et immunités sans comporter des conséquences directes et sans avoir une part de responsabilité.

À la suite des révélations minutieuses et détaillées sur le programme PRISM, son fonctionnement et ses participants[1586], ni Google ni la NSA n'ont confirmé ou infirmé leur coopération et l'échange massif d'informations contribuant au développement de ces opérations de renseignement, alors même que des efforts ont eu lieu pour vérifier la véridicité des révélations publiées, en vain. Ce fut le cas de l'initiative judicaire lancée en 2012 par le centre EPIC, « Electronic Privacy Information Center », contre la NSA pour obtenir plus d'informations sur le partenariat existant entre cette dernière et l'entreprise Google, un an avant les révélations spectaculaires marquant l'année 2013 : l'initiative a été annulée et cassée par le

customer data—including addresses, phone numbers, and credit card information—for use in a government data mining project."

[1583] F. DOUZET, « La géopolitique pour comprendre le cyberespace », *op. cit.*, p. 13.

[1584] A. LIPOWICZ, "Boeing to staff FBI Fusion Center", Washington Technology, publié le 1er juin 2007: https://washingtontechnology.com/articles/2007/06/01/boeing-to-staff-fbi-fusion-center.aspx

[1585] J. STRAW, "Smashing Intelligence Stovepipes", Security Management – A publications of ASIS International, publié le 1er mars 2008: https://sm.asisonline.org/Pages/Smashing-Intelligence-Stovepipes.aspx

[1586] *Cf.* p. 319 et s. ; Voir aussi, G. GREENWALD, *No place to hide: Edward Snowden, The NSA & The Surveillance State*, Penguin Books, Penguin Random House UK, 2014, p. 74-75 et 108-111.

juge fédéral arguant que « *even if EPIC is correct that NSA possesses records revealing information only about Google, those records, if maintained by the agency, are evidence of some type of interaction between the two entities, and thus still constitute an NSA "activity" undertaken as part of its Information Assurance mission, a primary "function" of the NSA. Moreover, if private entities knew that any of their attempts to reach out to NSA could be made public through a FOIA request, they might hesitate or decline to contact the agency, thereby hindering its Information Assurance mission* », et annonçant par la suite que « *NSA's determination that certain security vulnerabilities in Google technologies pose (or do not pose) a risk to the government's information systems constitutes an "activity" of the agency, as does a relationship between the agency and Google* »[1587]. Il semble par conséquent évident que les autorités publiques ne mènent pas seules les opérations de surveillance, de censure et de contrôle mais sont plutôt soutenues par un vaste partenariat public-privé de surveillance, un éventail d'entreprises à but lucratif.

Une enquête menée en 2010 aux États-Unis a montré, dans ce sens, que 1,931 entreprises différentes travaillent sur le renseignement, la lutte contre le terrorisme ou la sécurité intérieure[1588]. En 2013, des documents divulgués ont ainsi montré que la NSA ou son partenaire anglais a ciblé le fonctionnaire chargé d'enquêter sur les violations présumées de Google du droit de la concurrence de l'Union[1589]. Ces mêmes documents ont aussi révélé l'appétit insatiable des agences de renseignement pour les informations et le renseignement : « *the French companies Total, the oil and gas giant, and Thales, an electronics, logistics and transportation outfit, appear as targets, as do a French ambassador, an "Estonian Skype security team" and the German Embassy in Rwanda* »[1590]. Et ce ne sont que quelques exemples

---

[1587] United States Court of Appeal – For the District of Columbia Circuit, EPIC v. NSA, USCA Case No. 11-5233, May 11, 2012, (EPIC v. NSA 798 F. Supp. 2d 26 (D.D.C. July 8, 2011)), § II., p. 7-8: https://www.wired.com/images_blogs/threatlevel/2012/05/EPIC-v.-NSA-DC-Cir.-2012.pdf ; https://epic.org/2012/03/epic-v-nsa-no-11-5233.html; https://epic.org/privacy/nsa/foia/EPIC-v-NSA-OB-FINAL.pdf

[1588] B. SCHNEIER, *Data and Goliath*, *op. cit.*, p. 95.

[1589] J. GLANZ et A. W. LEHREN, « N.S.A. Spied on Allies, Aid Groups and Businesses », The New York Times, publié le 20 décembre 2013: "*Mr. Almunia, a Spaniard, assumed direct authority over the commission's antitrust office in 2010. He has been involved in a three-year standoff with Google over how the company runs its search engine. Competitors of the online giant had complained that it was prioritizing its own search results and using content like travel reviews and ratings from other websites without permission. While pushing for a settlement with Google, Mr. Almunia has warned that the company could face large fines if it does not cooperate.*

The surveillance reports do not specify whether the interceptions of Mr. Almunia's communications were requested by the N.S.A. or British spies. Nor do the reports make clear whether he was a longstanding surveillance target or swept up as part of a fleeting operation. Contacted by The Times, Mr. Almunia said he was "strongly upset" about the spying.": https://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html ; et, F. PASQUALE, *The Black Box Society*, *Id.,* p. 50.

[1590] J. GLANZ et A. W. LEHREN, « N.S.A. Spied on Allies, Aid Groups and Businesses », *Id.*

montrant l'ampleur et l'étendue de l'alliance entre États et entreprises, entre renseignement et commerce : la privatisation peut être plus qu'une transaction entre les gouvernements et les entreprises, « *it can be a marriage—a secret marriage—with a hidden economy of favors exchanged* »[1591].

Et cette alliance est encore plus profonde compte tenu de l'existence d'une forte porte tournante entre le secteur public et le secteur privé, assurant par conséquent le succès de ce partenariat inédit. Des fonctionnaires peuvent ainsi faire profiter, tout en la protégeant, une entreprise qu'ils comptent rejoindre à l'avenir ; de même, un grand nombre de responsables de la sécurité poursuivent des emplois lucratifs dans le secteur privé peu après avoir quitté leurs fonctions publiques. Ce fut le cas de l'Amiral McConnell, directeur de la NSA de 1992 à 1996, qui a quitté son poste pour devenir vice-président de la centrale du fournisseur de l'État Booz Allen Hamilton[1592] où il continue son travail sur le renseignement national, mais aussi le cas de K. Alexander qui, après avoir démissionné de son poste de directeur de la NSA en 2013, a créé sa propre entreprise d'expert-conseil en sécurité informatique[1593]. *In fine*, cela aboutit à une alliance profitable bilatéralement : « *the manipulation of threat perception by the "homeland security-industrial complex" feeds corporate profits as well as government budgets* »[1594].

Le marché de la cybersécurité s'avère ainsi être bel et bien florissant et en plein épanouissement, de nombreuses entreprises vendant, de manière égale, des services et produits de sécurité et d'interception aux gouvernements et aux entreprises, entretenant par là même, et de manière équivalente, de bonnes relations d'affaire dans les deux secteurs. C'est le cas de la compagnie italienne Hacking Team[1595], un fabricant de cyberarme, qui vend des systèmes de piratage et d'interception aux gouvernements du monde entier destinés à être employés contre les systèmes d'exploitation des ordinateurs et des téléphones portables : « *the mobile malware installs itself remotely and collects e-mails, text messages, call history, address books, search history data,*

[1591] F. PASQUALE, *The Black Box Society*, *Ibid.,* p. 50.

[1592] Booz Allen Hamilton, About Us: "*We are a global firm of approximately 24,600 diverse, passionate, and exceptional people driven to excel, do right, and realize positive change in everything we do. We bring bold thinking and a desire to be the best in our work in consulting, analytics, digital solutions, engineering, and cyber, and with industries ranging from defense to health to energy to international development*": https://www.boozallen.com/about.html ; Meet Mike – Senior Executive Advisor "*Senior Executive Advisor Mike McConnell is the firm's former vice chairman, where his primary roles included serving on the firm's Leadership Team and leading Booz Allen's rapidly expanding cyber business*": https://www.boozallen.com/d/bio/leadership/mike-mcconnell.html

[1593] B. SCHNEIER, *Data and Goliath*, *Id.*, p. 95, et l'auteur poursuit *"[…], Keith Alexander started his own internet security consulting firm, and filed patent for security technologies he claimed to have invented on his own time. He's hired the NSA's Chief technology officer, who continues to work for the NSA as well*".

[1594] F. PASQUALE, *The Black Box Society*, *Ibid.,* p. 50.

[1595] Hacking Team - Rely on Us: The Hacking suite for governmental interception: "We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities": http://www.hackingteam.it

and keystrokes. It can take screenshots, record audio to monitor either calls or ambient noise, snap photos, and monitor the phone's GPS coordinates. It then surreptitiously sends all of that back to its handlers »[1596]. C'est une hypothèse raisonnable que de supposer que la plupart des pays possèdent ces capacités de piratage, d'interception et de surveillance.

En effet, les produits d'intrusion et de surveillance des ordinateurs et des téléphones portables proposés par l'entreprise Hacking Team sont utilisées par les autorités des pays suivants : Azerbaïdjan, Colombie, Égypte, Éthiopie, Hongrie, Italie, Kazakhstan, Corée, Malaisie, Mexique, Maroc, Nigeria, Oman, Panam, Pologne, Arabie Saoudite, Soudan, Thaïlande, Turquie, Émirats Arabes Unis et Ouzbékistan[1597]. Certains de ces gouvernements sont connus pour tenir un régime oppressif ou autoritaire, alors même que la loi sur les technologies duales interdit des ventes à ces régimes[1598]. L'entreprise française Bull SA a pourtant coopéré et aidé le gouvernement libyen dans la construction de son centre de surveillance, le Nigeria a utilisé les produits et services de la société israélienne Elbit Systems, la Syrie a eu recours à la compagnie allemande Siemens, à l'entreprise italienne Area SpA, et beaucoup d'autres[1599]. La dualité qui existait entre le secteur public et le secteur privé semble être, dans ce contexte, une façade plus qu'une réalité.

Il paraît désormais évident que les commandes du marché sont influencées par les décisions politiques, qui sont, à leur tour, influencées par le marché, puisque les bénéficiaires des décisions politiques passées utilisent les fonds gagnés dans le commerce pour promouvoir et poursuivre des fins politiques futures : « *Many call business's influence here "capture," since industry has more power over its regulators than the regulators have over industry. But "capture" is too static a term for what is really going on. […]. The Yale social scientist Charles E. Lindblom suggested a better term than capture for this mutual influence and transformation: "circularity"* »[1600]. Alors que s'installe de façon dominante l'âge de l'information, l'alliance

---

[1596] B. SCHNEIER, *Data and Goliath*, *Ibid.*, p. 87.

[1597] B. SCHNEIER, *Data and Goliath*, *Ibidem*, p. 96, et Hacking Team - Solutions "Our historical solution, Remote Control System, is used by 50+ major governmental institutions for critical investigations, in more than 35 countries": http://www.hackingteam.it/solutions.html

[1598] *Cf.* p. 342 ; Voir aussi, Rapport d'information n° 3581 (2019-2020) fait par la Commission des affaires étrangères en conclusion des travaux d'une mission d'information constituée le 31 octobre 2018 sur le contrôle des exportations d'armement, par M. Jacques MAIRE et Mme Michèle TABAROT, enregistré à la présidence de l'Assemblée Nationale le 18 novembre 2020.

[1599] B. SCHNEIER, *Data and Goliath*, *Ibidem.*, p. 96.

[1600] F. PASQUALE, *The Black Box Society*, *Ibid.,* p. 207, où l'auteur explique "*There is not a stable "Wall Street" capturing an equally inert SEC or Fed. Rather, certain parts of industry skillfully outmaneuver rivals, gain power in agencies, and change their agendas. The new regulatory environment favors certain firms and disadvantages others. The firms boosted by the new order have even more cash to influence newer orders. Those adept at shuttling between Washington, New York, and (now) Silicon Valley can drive an agency (and an industry) far from its original set of values, aims, and strategies*."

existante entre État et commerce évolue en se renforçant de sorte qu'il est utile de s'interroger quant à leur future interchangeabilité. Finalement, « *it is **people**, not some nameless abstraction like "industry", who've set up the rules of our black box society* »[1601].

L'intégralité des autorités aspire, toujours plus, à modifier les technologies à la source pour insérer des malwares ou des portes dérobées ou tout autre technique permettant d'intercepter et de surveiller ; les entreprises coopèrent, ont également accès aux données interceptées et en profitent toujours davantage et les États, tout comme les entreprises, acquièrent et utilisent l'intégralité de ces produits et services indifféremment ; le tout en tenant à l'écart le produit même à l'essence de ce système et des alliances en découlant, les individus et leurs données, qui aspirent, de leurs côtés, à toujours plus de transparence sans savoir réellement où la chercher et vers quel secteur ou entité se retourner, générant par conséquent un paradoxe de transparence ainsi qu'un géant casse-tête.

Autrement dit, « *this transparency paradox is part of a much wider present-day confusion. Over the past few years we have been presented with scandals that seem to be evidence of powerful forces that are busy undermining both individual freedoms and the political system that is supposed to protect those freedoms. These range from the NSA and GCHQ, to global banks, private equity, giant international energy corporations, and parts of the media-industrial complex - like News International (and probably lots of other newspapers as well). But the scandals do not join up to make a bigger picture. And our reactions are sometimes confused and contradictory - as in the case of transparency and surveillance. It is as if the scandals are part of a giant jigsaw puzzle - and what we are waiting for is someone to come along and click those pieces together to give a clear, big picture of what is happening* »[1602].

Section 2 – La tension entre les notions de liberté et de sécurité

De la nouvelle alliance et de la nouvelle architecture de surveillance ainsi mises en place entre les secteurs privé et public, une tension découle et s'exprime conséquemment entre les notions fondamentales de liberté et de sécurité qui se traduit, de manière pragmatique, par l'insouciance

[1601] F. PASQUALE, *The Black Box Society*, *Ibidem,* p. 207, et, F. Pasquale, "Reclaiming Egalitarianism in the Political Theory of Campaign Finance Reform," University of Illinois Law Review 45, Vol. 2008 N° 2, p. 599-660: https://core.ac.uk/download/pdf/56355704.pdf

[1602] A. CURTIS, "What the Fluck! The point at which journalism fails and modern power begins", BBC UK, BBC Blog, publié le 5 décembre 2013: https://www.bbc.co.uk/blogs/adamcurtis/entries/44122901-c2e8-34f5-93e0-d4402c163966

des structures et modèles émergents (§1), mais aussi par l'insouciance des algorithmes de traitement fréquemment et massivement employés (§2).

§1. L'insouciance des structures et modèles émergents

L'insouciance des structures et des modèles émergents, observée progressivement ces dernières décennies, s'accentue et se justifie à l'ère du numérique au nom, d'une part, du développement et de l'intérêt général (A), et, d'autre part, de la prévention et de l'application de la loi (B).

A. Au nom du développement et de l'intérêt général

Les développements précédents mettent en évidence la disparition progressive de la dichotomie traditionnelle État-marché fortement aidée par le recours au secret protégé au nom de la loi et par les besoins de surveillance. Sous l'égide de l'intérêt général ou celle du développement, une multitude de technologies, toujours plus perfectionnées, a vu le jour et irrigue le quotidien des individus, sans que les choix informatiques derrière ces produits et services ne soient jamais révélés, et tout en faisant leur promotion au titre du développement technologique, de la sécurité ou de la sécurité informatique, ou bien de la croissance économique. La surveillance et le secret représentent, à l'heure actuelle, deux des composantes fondamentales guidant la quasi-totalité des opérations qui entourent les personnes dans leur quotidien, qu'elles soient d'origine étatique ou commerciale, à des fins de promotions et de marketing ou bien d'administration, de sécurité et de défense.

Grâce à l'effort combiné de ces deux secteurs classiquement séparés, la constitution des matériels et logiciels qui structurent ce que le Professeur Lessig nomme le *Code*[1603], que toute personne utilise dans la vie courante, qu'elle le veuille, le sache ou pas, est gardée secrète alors même que ces matériels et logiciels génèrent, après surveillance, collecte, traitement et calcul, des analyses, profils et décisions automatisées que ces mêmes personnes subissent. C'est la nouvelle architecture du cyberespace qui se construit actuellement, où le code informatique fait la loi définissant et déterminant la manière dont l'individu vit au sein du cyberespace, mais aussi dans l'espace physique, et, nous apprend Lessig, ce fut un choix à faire.

À ses balbutiements, le cyberespace comportait aux yeux de ceux qui l'ont compris un espace de liberté, un espace où l'échange d'informations se ferait de manière libre, non régulée, et ne pouvant être atteint par la loi ou les autorités gouvernementales. Les événements du début du XXI[e] Siècle ont apporté un sursaut sécuritaire, demandé par les citoyens, à la suite des différents

[1603] L. LESSIG, *Code – Version 2.0*, Ed. Basic Books, New York, 2006.

attentats subis[1604]. En réponse à la demande et dans le but de fournir plus de sécurité, qu'elle soit à titre individuel ou collectif, informatique ou physique, contre une large variété de menaces perçues, allant du terrorisme à la fraude à l'usurpation d'identité ou au vol des données, les acteurs publics et privés se sont employés à étendre les capacités de surveillance et d'authentification à travers un éventail tout aussi large d'acteurs et d'instruments. Les grandes restructurations de la société de l'information dues d'une part au piratage et de l'autre à la sécurité, donc dans un but privé pour la protection d'une propriété ou public pour la protection de l'État, visent ensemble, semble-t-il, à produire une architecture de contrôle : « *configurations that define in a highly granular fashion ranges of permitted conduct* »[1605].

L'architecture, qui se réfère généralement à l'art de construire, d'édifier, désigne le « principe d'organisation d'un ensemble, agencement, structure », « un ensemble structuré, organisé » construit, « ce qui constitue l'ossature, les éléments essentiels d'une structure » ou encore l'organisation « des divers éléments constitutifs d'un système informatique, en vue d'optimiser la conception de l'ensemble pour un usage déterminé »[1606]. L'architecture initiale du monde du web aspirait à ce qui est aujourd'hui qualifié d'utopiste et d'irréaliste, comme il a été vu. En lieu et place, l'architecture actuelle semble plutôt être dessinée par une « main invisible », selon Lessig, propre au cyberespace, impulsée par les gouvernements et le commerce au titre de l'intérêt général et du développement numérique, construisant *ipso facto* une architecture capable de perfectionner le contrôle et de rendre possible une réglementation hautement efficace. En effet, les technologies de l'information et de la communication se sont transformées depuis la création du cyberespace, passant des échanges parcellisés à des communications mises en réseau et constamment interconnectées ; de plus, le pouvoir des calculs et des mathématiques a trouvé son essor avec les développements technologiques facilitant les analyses, le profilage et la prévention. Or, si l'intégralité de ces mutations n'a pas fait l'objet de discussions ou d'examens approfondis, elles ont constamment été promues au nom de l'intérêt général et de l'évolution. En effet, « *while once it seemed obvious and easy to declare the rise of a "networked society" in which individuals would realign themselves, empower themselves, and undermine traditional methods of social and cultural control, it seems clear that networked digital communications need not serve such liberating ends* »[1607].

[1604] *Cf.* p. 472.

[1605] J. E. COHEN, *Configuring the networked self – Law, Code, and the play of everyday practice*, Yale University Press, 2012, p. 155.

[1606] CNRTL, « Architecture » : http://www.cnrtl.fr/definition/architecture, et Dictionnaire Larousse, « Architecture » : https://www.larousse.fr/dictionnaires/francais/architecture/5078

[1607] S. VAIDHYANATHAN, "Remote Control: The rise of electronic cultural policy", *In* Annals of the American Academy of political and social science Vol. 597, Issue 1, du 1er janvier 2005 (p. 122-133), p. 122.

Le socle de ces nouvelles technologies de communication est le Code qui est, selon Lessig et d'autres auteurs adoptant la même vision, le « *salient regulator - régulateur saillant* » de la nouvelle architecture édifiant le cyberespace tout en le composant. Selon le Professeur Lessig, il est utile de reconnaître et de savoir comment chaque "code" différent régit et régule dans le cyberespace : *« how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is* »[1608]. Reprenant les propos de W. Mitchell « *the code is cyberspace's law* » et de J. Reidenberg « *Lex Informatica* », il les résume avec simplicité et brillance en affirmant que, désormais, « *code is law* »[1609]. Dans le monde actuel du cyberespace, le code et les choix technologiques continuellement renouvelés et mis à jour, gardés pourtant secrets et employés constamment pour plus de surveillance, semblent bien faire la loi et s'imposent de plus en plus avec force tout en étant subtils, non concrets, invisibles pour les citoyens les employant chaque jour, perdus dans un espace que beaucoup peinent à saisir.

Pourtant, dès 1977, à l'occasion des débats parlementaires relatifs à la loi informatique et libertés, les députés déploraient et soulignaient déjà que « *tous les abus sont donc permis lorsque la technique n'est pas contrôlée* »[1610]. Et dans l'univers numérique, les techniques et pratiques employées échappent à la transparence et au contrôle juridique, se cachant derrière des annonces de sécurité, de défense, d'évolution de la société de l'information ou du marché numérique unique, de développement informatique, de simplification des procédures, de liberté ou de croissance économique. Se maintenir dans cette lignée mènerait indéniablement à une société dans laquelle les technologies employées au quotidien détecteraient et arbitreraient, en toute autonomie, ce qui est juste ou faux, bon ou mauvais, recommandé ou non, autorisé ou interdit au détriment de tout débat ou examen politique ou social. Autrement dit, « *les algorithmes et les programmes informatiques deviendraient les démiurges du corps social* »[1611] promettant d'éradiquer tout doute, dérive, corruption, fraude, atteinte, excès ou abus de pouvoir, ravivant ainsi une vieille histoire entre l'homme et son organisation sociale[1612].

[1608] L. LESSIG, *Code – Version 2.0*, *Id.*, p. 5.
[1609] L. LESSIG, *Code – Version 2.0*, *Ibid.*, p. 5.
[1610] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit.,* p. 5784.
[1611] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, op. cit*., p. 248.
[1612] Reprenant les propos du Conseil d'État, « *Les figures de Socrate ou Sénèque idéalisées par la postérité nous rappellent que la citoyenneté antique exaltait le dévouement des hommes prêts à se sacrifier au nom du respect des lois ou du refus de la tyrannie. La Renaissance italienne a été marquée par l'éloge de la vertu dont le Prince de Machiavel doit faire preuve pour s'abstraire des factions et même de la morale, afin de promouvoir l'intérêt supérieur de la Cité. Et, bien sûr, la réflexion sur les vertus ou les devoirs civiques est centrale dans la pensée des Lumières, qui en font la condition nécessaire à l'édification d'une société libre.* », Conseil d'État, La citoyenneté – Être (un) citoyen aujourd'hui, Les rapport du Conseil d'État (ancienne collection Études et Documents du Conseil d'État), 2018, p. 53 ; et la vertu, disait Rousseau, « *n'est que cette conformité de la*

Précisément, notait Tocqueville, les hommes *« sentent le besoin d'être conduits et l'envie de rester libres* » ne sachant lequel primer et ne voulant éliminer ni l'un ni l'autre ; par conséquent, « *ne pouvant détruire ni l'un ni l'autre de ces instincts contraires, ils s'efforcent de les satisfaire à la fois tous les deux* »[1613]. C'est le choix des lois et de la démocratie où le peuple élit son souverain, son maître. En outre, selon une formule, devenue célèbre, inspirée du Contrat social de Rousseau « *la loi n'est que la déclaration de la volonté générale* »[1614], formule reprise par la Déclaration des droits de l'homme[1615], et dans la mesure où elle est l'expression de la volonté générale du peuple, « *la loi peut tout faire, la loi ne peut mal faire* »[1616] ou, comme l'a pu écrire Hugo, « *le Droit incarné, c'est le citoyen* »[1617]. L'architecture du cyberespace, telle qu'elle se structure actuellement, semble être le contexte idéal pour satisfaire ces instincts humains et cette volonté générale des individus : elle mène à ce que le code devienne la loi et *vice versa,* aboutissant à une illusion de liberté au sein d'une démocratie conduite principalement par le code[1618]. Dans cette perspective, « *la gouvernance par les algorithmes s'apparenterait alors à une nouvelle forme d'un despotisme doux, conçu dans l'intérêt général, associant à la fois le contrat social de Rousseau et la démocratie en Amérique de Tocqueville* »[1619].

Les capacités et l'assouvissement des tendances et désirs qu'offrent aujourd'hui le cyberespace et son code en font un objet d'enthousiasme et d'acceptation chez beaucoup de personnes, privées comme publiques. Compte tenu des développement précédents, il paraît évident que les

---

volonté particulière à la générale », J.-J. Rousseau, Discours sur l'Économie Politique, Texte publié comme article dans l'Encyclopédie, 1755, p 252.

[1613] A. DE TOCQUEVILLE, *De la démocratie en Amérique*, t. II, Hachette Bnf, Ed. 1848, Chap. 6 – Quelle espèce de despotisme les nations démocratiques ont à craindre, p. 315-316, et l'auteur souligne : « *Ils imaginent un pouvoir unique, tutélaire, tout-puissant, mais élu par les citoyens. Ils combinent la centralisation et la souveraineté du peuple. Cela leur donne quelque relâche. Ils se consolent d'être en tutelle, en songeant qu'ils ont eux-mêmes choisi leurs tuteurs. Chaque individu souffre qu'on l'attache, parce qu'il voit que ce n'est pas un homme ni une classe, mais le peuple lui-même, qui tient le bout de la chaîne. Dans ce système, les citoyens sortent un moment de la dépendance pour indiquer leur maître, et y rentrent* », et A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, Id.*, p. 248.

[1614] J.-J. ROUSSEAU, Du Contrat Social ou Principes du Droit Politique, Ed. Marc Michel Rey, Amsterdam, 1762, Ed. Hachette Livre Bnf du 1er juin 2012, Livre III, Chap. XV – Des députés ou des Représentants, p. 217 « *La loi n'étant que la déclaration de la volonté générale, il est clair que dans la puissance législative le peuple ne peut être représenté ; mais il peut et doit l'être dans la puissance exécutive, qui n'est que la force appliquée à la loi.* »

[1615] Déclaration des droits de l'homme et du citoyen de 1789, Art. 6 : *« La Loi est l'expression de la volonté générale. Tous les Citoyens ont droit de concourir personnellement, ou par leurs Représentants, à sa formation.* »

[1616] Formule inspirée de J.-J. Rousseau exposée par Carré de de Malberg dans son ouvrage, La loi expression de la volonté générale, publié en 1921.

[1617] V. HUGO, Actes et Paroles II – Pendant l'exil (1852-1870), Œuvres complètes, Paris, J. Hetzel & Cie et A. Quantin, 1883, p. 3 ; Disponible en ligne : https://gallica.bnf.fr/ark:/12148/bpt6k37457b/f5.image

[1618] *Cf.* p. 487 et 557 et s.

[1619] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, Id.*, p. 248.

services de sécurité, publics comme privés, recourent de plus en plus au traitement et à l'analyse du Big data, leur permettant, à terme, de repérer et d'identifier les individus dangereux, ceux qui vont potentiellement commettre un crime : « *ainsi la criminalité devient-elle le produit de ces nouveaux savoirs. À quoi nous invitent les caméras de surveillance, les contrôles électroniques, les systèmes d'alarme, si ce n'est à nous penser comme des victimes potentielles ? nous ne sommes plus face à la dangerosité d'un individu cliniquement constatée mais à la violence imprévisible de son profil. On peut alors s'engager dans une recherche folle de la causalité du mal. Steven Spielberg, dans son film Minority Report, a poussé jusqu'au bout le fantasme de la toute-puissance de l'investigation policière en quête d'un futur totalement transparent : le policier peut intervenir avant même que les crimes soient commis grâce à des « precog » (précognitifs) qui peuvent les anticiper. Pure fiction ? Pas autant qu'on pourrait le penser* »[1620]. De même pour les services d'identification et d'authentification privés ou publics qui proposent un large éventail de produits et services permettant de centraliser utilement les informations de leurs clientèles - citoyens, alimentant leurs bases de données réciproques, et leur servant, à l'avenir, pour une multitude de finalités aussi diverses que variées : gestion des identités numériques, gestion de la e-réputation et de la notoriété en ligne (personnelle ou professionnelle), services administratifs simplifiés, identification, authentification et recensement et ainsi de suite[1621] ; le tout au titre de l'intérêt général et du développement et de la croissance économique, numérique ou sociale. Ces activités et opérations contribuent à la structure actuelle que prend le cyberespace et représentent la « main invisible » qui guide l'élaboration de son code.

Ce sont donc, *in fine*, des hommes qui participent à cette construction, faisant primer leurs propres volontés et intérêts, qu'ils soient publics ou privés ; elle ne naît pas seule, divinement, c'est une construction, une constitution, un choix à faire : « *we can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building. Code is never found; it is only ever made, and only ever made by us* »[1622]. Comme en matière commerciale ou politique, la décision revient finalement aux hommes qui conduisent le corps social et la structure choisie ; et ce choix

---

[1620] D. SALAS, *La volonté de punir : Essai sur le populisme pénal*, Fayard, Pluriel, 2010, p. 196 ; et *Cf.* p. 464.
[1621] *Cf.* p. 94 et 120 et s.
[1622] L. LESSIG, *Code – Version 2.0*, *Ibid.*, p. 6, et l'auteur poursuit : « *As Mark Stefik puts its, "Different versions of [cyberspace] support different kinds of dreams. We choose, wisely or not". Or again, code "determines which people can access which digital objects… How such programming regulates human interactions… depends on the choices made". Or, more precisely, a code of cyberspace, defining the freedoms and controls of cyberspace, will be build. About that there can be no debate.* »

et la décision afférente semblent avoir été faits dans le nouveau monde numérique, sans se référer aux peuples qui devraient pourtant choisir leurs lois pour pouvoir être libres, au nom de leurs droits et libertés. Ce n'était pourtant pas l'esprit des hommes de France de 1977 qui, étudiant le problème de l'informatique et des libertés, avaient élaboré une variété de mesures qui « *ont pour but de promouvoir une société ouverte, où chacun peut connaître les fondements sur lesquels sont prises les décisions qui l'affectent* »[1623].

Ce code, le nouveau régulateur saillant du cyberespace, se réfère en réalité, dans la vision de Lessig, à quatre régulateurs différents, distincts mais interdépendants, contribuant simultanément à la création de celui-ci ; quatre facteurs régulant seul ou collectivement, et portant diverses atteintes aux droits et libertés fondamentales, à prendre nécessairement en compte. Ceux-ci constituent les modalités de régulation, les mécanismes régulateurs à l'œuvre dans le code affectant et régissant, *in concreto*, la vie et le comportement des personnes. Composant l'ossature de ce 'code', ces modalités caractérisent des « *Newtonian forces acting to shift individual behavior this way or that* » indique la Professeure[1624]. Ces modalités « contraignantes » sont les *lois*, promulgués par les autorités publiques et réglementant la vie de tous les jours ; les *normes*, notamment les normes sociales dictées par la société qui finalement s'imposent de manière collective régissant nos comportements ; le *marché*, une force en soi découlant des demandes individuelles ou collectives, privées ou publiques, affectant ainsi nos choix et comportements ; et, enfin, l'*architecture*, la constitution des technologies, services et produits, qui guide et façonne le monde physique et numérique à la fois. Le Professeur Lessig adopte la métaphore du « *pathetic dot* », métaphore devenue fameuse depuis, pour illustrer la personne réglementée, et donc contrôlée : « *that someone regulated is represented by this (pathetic) dot – a creature (you or me) subject to different regulations that might have the effect of constraining (or as we'll see, enabling) the dot's behavior* »[1625].

Les quatre modalités composant le code régulent alors ensemble ce « *pathetic dot* », et la "réglementation" de celui-ci représente la somme de ces quatre contraintes. Toute modification dans l'un d'eux affectera la régulation de l'ensemble : « *thus, "changes in technology may usher in changes in… norms", and the other way around* »[1626]. Cet ensemble caractérise ainsi la structure du code et le monde que ce code crée, et les codes constituent par ailleurs le cyberespace, or les espaces valident ou invalident, approuvent ou désapprouvent les individus

[1623] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *Id*., p. 5788.
[1624] J. E. COHEN, *Configuring the networked self*, *Id.,* p. 155.
[1625] L. LESSIG, *Code – Version 2.0*, *Id.*, p. 122.
[1626] L. LESSIG, *Code – Version 2.0*, *Ibid.*, p. 123.

et les groupes : « *the selections about code are therefore in part a selection about who, what, and, most important, what ways of life will be enabled and disabled* »[1627]. Par conséquent, tout choix ou changement effectué dans l'une de ces nouvelles modalités régulatrices et 'gouvernantes' impacte, à l'heure actuelle, tout choix ou toute modification dans notre quotidien, notre comportement, notre façon de nous voir et de percevoir les autres, nos personnalités, nos goûts et intérêts ; *in fine*, nos identités physiques et numériques.

À travers le temps, l'histoire de l'homme reflète une méfiance constante justifiée vis-à-vis des gouvernements, des personnes élues pour conduire les actions publiques, caractérisés dans l'opinion publique comme étant les principales menaces à la liberté ; le secteur privé, commercial n'inspirant néanmoins pas autant d'inquiétude. Toute l'architecture politique, constitutionnelle de nos sociétés contemporaines a été fondée sur l'idée d'instituer un équilibre des pouvoirs, une séparation des pouvoirs, un pouvoir de contrôle égal entre les autorités, de sorte à tempérer les actions des personnes au pouvoir et à réduire les abus, laissant de côté le secteur privé. Pourtant, les avertissements contre le monde entrepreneurial et commercial ont commencé depuis un certain temps : déjà, en 1859, J. S. Mills écrivait sur la liberté, et « *liberty, in Mill's view, was threatened as much by norms as by government, as much by stigma and intolerance as by the threat of state punishment* »[1628] ; dans les années 70, les parlementaires français affirmaient qu' « *en effet, les dangers inhérents aux procédés modernes d'enregistrement et à l'informatique ne sont pas limités aux organes de l'État. Le risque est grand, en particulier dans l'ordre économique et social : mise sur ordinateur de tous les éléments relatifs à un ouvrier, à un cadre ; recours à des agences spécialisées qui prolifèrent depuis quelques années et procèdent à des enquêtes, de façon souvent inqualifiable, avant l'embauche et au cours de la carrière des intéressés. […]. Nous n'en sommes pas arrivés au monde prophétique annoncé par George Orwell dans « 1984 ». Mais le laisser-faire sur ce point précis des traitements privés pourrait nous en approcher* »[1629] ; et, en 2019, le Président de la CNCDH indiquait qu' « *en apparence, nous sommes un État de droit et l'on s'en flatte assez, nous avons un corpus juridique étoffé, des juges chargés de protéger nos libertés… En apparence, rien de tout ça n'est menacé. Dans la réalité, c'est autre chose. Au nom de la sécurité, toutes nos libertés le sont* »[1630].

[1627] L. LESSIG, *Code – Version 2.0*, *Ibid.*, p. 88.

[1628] L. LESSIG, *Code – Version 2.0*, *Ibidem*, p. 120, et l'auteur nous apprend que « *His objective was to argue against these private forces of coercion* »

[1629] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *Id*., p. 5785.

[1630] Le Monde, « Jean-Marie Delarue : « Au nom de la sécurité, toutes nos libertés sont menacées » », Propos recueilli par L. Couvelaire, publié le 29 avril 2019 : https://www.lemonde.fr/societe/article/2019/04/29/jean-marie-delarue-au-nom-de-la-securite-toutes-nos-libertes-sont-menacees_5456075_3224.html

Dans le monde actuel où presque tout devient numérique, au nom de l'intérêt général, du bien-être collectif et du développement, des choix politiques, sociaux et économiques, des technologies d'interception et de surveillance, des modifications techniques et sociales, ou encore des pratiques et modèles politiques, sociaux, économiques ou culturels, donc autant de 'codes', sont élaborés à des fins particulières en fonction de la volonté d'une élite se trouvant en position de force et de domination : c'est l'architecture actuelle du cyberespace qui guide et contrôle l'Homme du XXIe Siècle. Mais ces choix et modalités sont l'expression d'une volonté particulière, celles des autorités publiques et des entreprises privées, écrasant subtilement la volonté générale des individus qui se retrouvent alors dans l'illusion de participer, de contribuer à la société et au corps social, et pensent avoir garanti leurs droits et libertés ; le tout sous couvert de la loi, du secret, de l'intérêt général de la société, de la sécurité, de la croissance, de l'innovation ou du développement. Or, prévenait Rousseau « *quand l'État, près de sa ruine ne subsiste plus que par une forme illusoire et vaine, que le lien social est rompu dans tous les cœurs, que le plus vil intérêt se pare effrontément du nom sacré du bien public ; alors la volonté générale devient muette, tous guidés par des motifs secrets n'opinent pas plus comme Citoyens que si l'État n'eut jamais existé, et l'on fait passer faussement sous le nom de Loix des décrets iniques qui n'ont pour but que l'intérêt particulier* »[1631].

L'architecture du cyberespace ainsi émergente, caractérisée désormais par une architecture de contrôle, trouve principalement son origine dans le désir d'obtenir et d'utiliser les informations ainsi que les technologies de l'information et de la communication pour gérer le risque et structurer la prise de risque ; ce qui s'assemble à la théorie du risque cultivée dans les dispositions du RGPD mais aussi dans celles de la directive 2016/680 dite directive police-justice[1632]. Plus généralement, cette architecture suit donc les désirs et tendances sociales du moment à l'ère de la révolution numérique, de manière graduelle, notamment là où les intérêts des acteurs institutionnels puissants s'alignent, en ce sens que « *the architectures of control now emerging within information networks are embedded within broader changes in patterns of social ordering in the emerging information society* »[1633].

Il est important de relever, en outre, que ce 'code' et ses modalités régulatrices constituent un ensemble de facteurs, d'éléments non concrets, et non une personne ou une entreprise qu'il serait possible de désigner pour responsable et d'engager sa responsabilité. C'est un paradoxe

[1631] J.-J. ROUSSEAU, *Du Contrat Social*, *Id.*, Livre IV, Chap. I – Que la volonté générale est indestructible, p. 235-236.
[1632] *Cf.* p. 232 et s.
[1633] J. E. COHEN, *Configuring the networked self, Ibid.,* p. 156.

en ce que ce 'code' caractérise finalement un corps irresponsable tout en étant le souverain tout puissant. Pourtant, indiquait Tocqueville, n'importe quelle constitution est « *infiniment préférable à celle qui, après avoir concentré tous les pouvoirs, les déposerait dans les mains d'un homme ou d'un corps irresponsable. De toutes les différentes formes que le despotisme démocratique pourrait prendre, celle-ci serait assurément la pire* »[1634].

Et nous abordons le pire en ce que l'enjeu actuel, notamment en ce qui concerne les données personnelles (dans leurs acceptions la plus large), ne se résume plus à la simple atteinte à la vie privée et à l'intimité des personnes. Cet enjeu est désormais dépassé englobant davantage la possibilité de faire valoir ses intérêts, ses motivations, sa légitimité à agir, son auto-détermination, voire de « *maintenir une pluralité de modes de production de la réalité* »[1635]. Face au nouveau règne du 'code', qui fait désormais la loi, les libertés se trouvent être profondément menacées puisque, comme le disait Rousseau, *« en un mot, la liberté suit toujours le sort des Loix, elle règne ou périt avec elles* »[1636]. En effet, les lois et les régulations, quelque soient leurs objectifs, « *can introduce a set of incentives or reward systems for people to behave in a desirable way, or they can impose a system of punishment or sanctions for those who behave in nondesirable ways* »[1637]. Et celles-ci consacrent et suivent principalement une formule devenue célèbre « *la sécurité est la première de nos libertés* » ; or « c'est faux » déclare l'ancien président du CNCDH, « *la sécurité est éventuellement l'une des conditions de nos libertés. Cet aphorisme est une dangereuse illusion qui pousse depuis plusieurs décennies les gouvernements à grignoter nos libertés toujours davantage* »[1638], au nom du développement, de l'évolution et de l'intérêt général ou encore au nom de la prévention et de l'application de la loi.

B. Au nom de la prévention et de l'application de la loi

La nouvelle architecture de contrôle que représente désormais le cyberespace a été graduellement mise en place mais paraît, en raison des diverses applications en résultant, s'orienter vers une pérennisation de sa structure, de son code et de ses pratiques au nom de la

---

[1634] A. DE TOCQUEVILLE, *De la démocratie en Amérique*, t. II, *Id.*, p. 316.
[1635] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, Ibid*., p. 247.
[1636] ROUSSEAU, « Huitième lettre écrite de la montagne » (1764), *In Œuvres complètes*, Gallimard, Coll. Bibliothèque de la Pléiade, t. 3, 1966, p. 842.
[1637] P. DE FILIPPI et A. WRIGHT, *Blockchain and the Law – The Rule of Code*, Harvard University Press, 2018, p. 193-194, et les auteurs précisent: "*Markets and regulations both implement a particular payoff structure around a specific set of activities, which might give rise to a specific reward or punishment. While punishments are generally more effective than rewards in the context of regulation, they can nonetheless be used to enhance compliance with the law*" (note de bas de p. n° 2, p. 282)
[1638] Le Monde, « Jean-Marie Delarue : « Au nom de la sécurité, toutes nos libertés sont menacées » », *Id.*

prévention, de la lutte contre la criminalité mais surtout de l'application de la loi. Il est vrai qu'à l'heure actuelle « *authority is increasingly expressed algorithmically* »[1639] : des décisions qui auparavant été fondées sur une appréciation et une réflexion humaines sont dorénavant générées automatiquement, par le biais d'un recours massif et quotidien à des données et des logiciels qui codent des dizaines de milliers de règles et d'instructions calculées en une fraction de seconde, à des machines et des matériels continuellement perfectionnés et gagnant chaque jour un peu plus d'autonomie, et ce grâce à l'efficience de la science et de la technologie. C'est ce qui a amélioré la qualité de vie des humains : l'évolution et le développement de la science et des technologies, comme ce fut le cas avec les avions, les trains, les ordinateurs, les portables (devenues des mini-ordinateurs) et moyens de communication, la création d'internet et ainsi de suite.

En revanche, ce sont les mêmes modèles, protocoles et technologies qui ont permis et facilité la généralisation de la surveillance ubiquiste observée, ainsi que la quête et l'installation d'une architecture de contrôle recherchées par les secteurs désormais hybridés[1640] pour des motifs de prévention, de recommandation, d'analyse de risque et/ou de profit au nom de l'application de la loi, du 'code' et ses modalités de régulation *in fine*. C'est ce qui a ouvert la porte à l'installation de ce vaste système de surveillance et de contrôle dans lequel tous les abus semblent possibles, « *d'autant plus que la violence meurtrière des attaques terroristes contribuera à faire disparaître, dans une partie de l'opinion, le sang-froid indispensable à la sauvegarde d'un système juridique libéral. Le pire tient dans le fait que cet abandon puisse apparaître comme légitime : s'armer pour se défendre, quoi de plus naturel* »[1641]. Et pour ce faire, l'individu renonce progressivement à sa liberté face aux dangers considérables des attaques subies suivant les préconisations des institutions et autorités du moment, arguant de manière redoutable, quoiqu'efficace, l'existence des menaces et dangers pouvant affecter la société et le corps social, et donc impacter les libertés. C'est une sorte de cycle incessant, un paradoxe, dans lequel l'individu renonce à des libertés pour gagner en sécurité et pour être dans

---

[1639] F. PASQUALE, *The Black Box Society*, *op. cit.,* p. 8.

[1640] P. MUSSO, *Le temps de l'État-Entreprise : Berlusconi, Trump, Macron*, Ed. Fayard, 2019 (352 p.), p. 3 et 6 : « *Avec l'industrialisation accélérée et généralisée, la formation de la grande Entreprise et la Révolution managériale du XX^e^ siècle, la société occidentale se dote d'une institution toujours plus puissante capable de contester la souveraineté étatique et d'en limiter le rôle : il s'agit de l'Entreprise qui, aujourd'hui, s'allie, voire investit l'État dans une nouvelle institution hybride que nous nommons l'État-Entreprise, en écho à l'État-Église du Moyen Âge* » ; « *C'est à un jeu à trois qu'invite la politique contemporaine (État-Entreprise-société civile), comme après le « big bang » du XII^e^ siècle (Église-État-société), tel que le figure notre schéma ci-dessus. Berlusconi, Trump et Macron ne sont nullement un épiphénomène, mais bien le révélateur d'une image (encore) invisible, celle de l'État-Entreprise, nouvelle institution du gouvernement des hommes en mode gouvernance* ».

[1641] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, Id.*, p. 251.

le respect des règles promulguées à ce titre, mais finit, sous l'égide de ce vaste système et de ce nouveau code ainsi mis en place, par être constamment soupçonné[1642].

Pour Agamben, une des conséquences de la mise en place de ce système de surveillance et de contrôle est caractérisée par la notion de « dispositif », au sein duquel l'individu ne cesse d'être saisi, qui tend à le gouverner et le guider ; une « positivité » comme l'avait initialement nommée Foucault influencé par J. Hyppolite qui avait montré « *comment l'opposition entre nature et positivité correspond, en ce sens, à la dialectique de la liberté et de la contrainte comme à celle de la raison et de l'histoire* »[1643]. Sans jamais définir le terme de « dispositif » en soi, Foucault avait néanmoins précisé que celui-ci représente « *un ensemble résolument hétérogène comportant des discours, des institutions, des aménagements architecturaux, des décisions règlementaires, des lois, des mesures administratives, des énoncés scientifiques, des propositions philosophiques, morales, philanthropiques ; bref, du dit aussi bien que du non-dit, voilà les éléments du dispositif. Le dispositif lui-même c'est le réseau qu'on établit entre ces éléments […], des stratégies de rapports de force supportant des types de savoir, et supportés par eux* »[1644].

La transposant à l'âge moderne et « en donnant une généralité encore plus grande à la classe déjà très vaste des dispositifs de Foucault », Agamben qualifie de dispositif « *tout ce qui a d'une manière ou d'une autre, la capacité de capturer, d'orienter, de déterminer, d'intercepter, de modeler, de contrôler et d'assurer les gestes, les conduites, les opinions et les discours des êtres vivants* »[1645]. Dans la société de l'information, et à la lumière de cette définition, la vie de tous les jours est envahie par une multitude de dispositifs vis-à-vis desquels l'individu devient, consciemment ou inconsciemment, accommodant, se conformant régulièrement à ses influences et orientations de sorte que ce comportement sème le doute chez les agents du pouvoir, menant à ce que tout le monde soit considéré comme suspect : « *de là surtout, l'étrange inquiétude du pouvoir au moment où il se trouve face au corps social le plus docile et le plus soumis qui soit jamais apparu dans l'histoire de l'humanité. Ce n'est que par un*

[1642] *Cf.* p. 463 et s., 480 et s.

[1643] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?,* Ed. Payot & Rivages, Paris, 2014, p. 14.

[1644] M. FOUCAULT, *Dits et écrits*, t. III (1976-1979), Ed. Gallimard, Coll. Bibliothèque de philosophie, 1994, p. 299 et *sq.* : « *[…] par dispositif, j'entends une sorte – disons – de formation qui, à un moment donné, a eu pour fonction majeure de répondre à une urgence. Le dispositif a donc une fonction stratégique dominante… j'ai dit que le dispositif était de nature essentiellement stratégique, ce qui suppose qu'il s'agit là d'une certaine manipulation de rapports de force, d'une intervention rationnelle et concertée dans ces rapports de force, soit pour les développer dans telle direction, soit pour les bloquer, ou pour les stabiliser, les utiliser. Le dispositif, donc, est toujours inscrit dans un jeu de pouvoir, mais toujours lié aussi à une ou à des bornes de savoir, qui en naissent, mais, tout autant, le conditionnent. […]*»

[1645] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Id.*, p. 31.

paradoxe apparent que le citoyen inoffensif des démocraties postindustrielles (le bloom comme on a suggéré avec efficacité de l'appeler), celui qui exécute avec zèle tout ce qu'on lui dit de faire et qui ne s'oppose pas à ce que ses gestes les plus quotidiens, ceux qui concernent sa santé, ses possibilités d'évasion comme ses activités, son alimentation comme ses désirs soient commandés et contrôlés par des dispositifs jusque dans les détails les plus infimes, que ce citoyen donc (et peut-être précisément à cause de cela) soit considéré comme un terroriste potentiel »[1646].

En effet, la force des algorithmes ne réside pas seulement dans leur pouvoir de calcul ou leur capacité de prédire ou encore de générer des décisions de manière objective, c'est bien le fait de traiter le tout techniquement, de manière insensible, impersonnelle, subtile et non agressive, faisant donc primer la prouesse technique sur la raison ou la logique. Là où la loi qualifie les personnes humaines de sujets de droit, les algorithmes les appréhendent « *comme des fragments de données appartenant à un vaste flux qu'il s'agit de représenter, calculer et modéliser* »[1647]. Toutefois, ce flux de données n'est jamais totalement exact pour la totalité des personnes existantes dans le cyberespace, « *car des risques existent. L'ordinateur se trompe rarement sur le plan technique, mais il peut se glisser des erreurs dans les données qui lui sont fournies, entraînant des conséquences fâcheuses* »[1648].

Une autre aporie générant également de nombreuses conséquences et impacts sur le corps social réside dans l'idée qu'au nom de la prévention et de la sécurité, et donc de l'application de la loi réformée et modifiée, l'État-entreprise[1649] conduisant la « main invisible » de la nouvelle architecture du cyberespace, a manipulé celui-ci, son code et ses dispositifs pour surveiller, contrôler, prédire et prévenir de façon à servir ses propres intérêts et volontés particulières, rendant le réseau et ses composantes *ipso facto* précaires et sensibles aux failles de sécurité. Autrement dit, « *everyone wants you to have security, except from them* »[1650], les failles de sécurité ainsi implémentées servant, à terme, l'intérêt des autorités publiques et des entreprises privées. Ainsi qu'il a pu être observé à travers les développements précédents, Google sécurise ses produits et services et intègre des mécanismes et protocoles de sécurité du moment qu'il arrive à surveiller et à utiliser les informations qu'il collecte pour vendre de la publicité, faire des suggestions ou des recommandations personnalisées et ainsi de suite. *Idem* pour Facebook

[1646] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Ibid.*, p. 47-48.
[1647] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, Ibid*., p. 253.
[1648] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*., p. 5786.
[1649] P. MUSSO, *Le temps de l'État-Entreprise, Id.*
[1650] B. SCHNEIER, *Click here to kill everybody: Security and survival in a Hyper-connected world*, Ed. W. W. Norton & Company, New-York, 2018, p. 56.

qui offre un réseau social sécurisé, du moment qu'il peut suivre et surveiller toute trace, toute activité entreprise sur le réseau à des fins commerciales, de marketing mais aussi à des fins politiques et de contrôle social, ce qui a été constaté à travers les différents scandales et les récentes révélations médiatiques, notamment à travers l'affaire « Cambridge Analytica »[1651]. En effet, « *Facebook has grown into the most pervasive surveillance system in the world. It's also the most reckless and irresponsible surveillance system in the commercial world. […]. In early 2018, when journalists revealed the extent to which a sleazy British political firm called Cambridge Analytica had Hoovered up Facebook data from more than fifty million Americans in preparation for its work to elect a president of the United States, the full range of Facebook abuse finally generated widespread popular attention and condemnation* », alors qu'une large communauté scientifique et plusieurs défenseurs de la vie privée et des droits de l'homme soulèvent des préoccupations et manifestent leurs inquiétudes depuis au moins 2010[1652]. De même, les services de renseignement veulent assurer la sécurité du moment qu'ils peuvent l'enfreindre et l'outrepasser s'ils le souhaitent, au nom de l'application de la loi, du contrôle social, de l'espionnage international ou de la cybersécurité et la cyberdéfense[1653].

Cette quête d'insécurité entraîne dès lors de nombreuses conséquences et influences, au titre d'intentions potentiellement louables mais qui, de manière pragmatique, semblent être abusives, frôlant la catastrophe. Le but premier et ultime s'avère être continuellement la surveillance, qui devient extrêmement facile étant donné que les machines et ordinateurs l'assurent naturellement, que les données sont un sous-produit d'un processus informatique y compris de tout rapport social entrepris à l'aide de l'informatique, et que « *we're all leaving digital exhaust as we go through our lives* »[1654] : c'est l'avènement de ce qui a été qualifié de « capitalisme de surveillance »[1655]. Ce « *surveillance capitalism* », dans lequel « *companies*

[1651] *Cf.* p. 380.

[1652] S. VAIDHYANATHAN, *Anti-social media: How Facebook disconnects us and undermines Democracy*, Oxford University Press, New York, 2018, p. 55: "*If you have been active on Facebook since before 2014 and you interacted with games or applications like Farmville, Mafia Wars, or Words with Friends, then Facebook exported not only a rich collection of your profile and activities on Facebook but also those of your Friends. Facebook has been sanctioned by governments around the world for its practices of collecting, using, and sharing personal data without full or clear disclosure. Yet the company continues to abuse its users, comforted by its popularity and power*."

[1653] *Cf.* p. 498 et s.

[1654] B. SCHNEIER, *Click here to kill everybody, Id.,* p. 57 où l'auteur explique que "*Everything we do that involves a computer creates a transaction record. This includes browsing the Internet, using – and even just carrying – a cell phone, making a purchase online or with a credit card, walking past a computerized sensor, or saying something in the same room as Amazon's Alexa. Data is also a by-product of any socializing we do using computers. Phone-calls, e-mails, text messages, and Facebook chatter all create transaction records*".

[1655] S. ZUBOFF, *The Age Of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, Ed. Public Affairs, 2019, p. IV "*THE DEFINITION - Sur-veil-lance Cap-i-tal-ism, n.: 1. A*

build systems that spy on people in exchange for services »[1656], émergeant au nom de l'insécurité pour la sécurité et au nom du profit, a été adopté par les autorités publiques qui emploient les mêmes technologies créées pour le capitalisme de surveillance. Il en résulte que, « *modern government surveillance piggybacks on existing corporate surveillance* »[1657] tout en recourant aux technologies développées en grande partie par le secteur privé, engendrant, à terme, des abus mais surtout des risques et des enjeux devenant progressivement désastreux. C'est bien la manière dont les ordinateurs, les machines informatiques en général, sont utilisés dans la société qui change de nos jours et cause autant de risques et enjeux : l'ampleur et l'importance de leurs décisions, l'autonomie de leurs actions et de leurs interactions avec le monde physique aggravant ces risques et enjeux à plusieurs égards.

La sécurité informatique est traditionnellement décrite comme une triade composée de la confidentialité, l'intégrité et la disponibilité ou mise à disposition (et donc la lisibilité) de l'information. Jusqu'à récemment, les menaces et les dangers portaient surtout sur la confidentialité des informations entraînant, selon le contexte, des coûts et des pertes, de l'embarras et de la honte, voire des dégâts néfastes, et pouvant même constituer une menace pour la sécurité. En revanche, « *once you give computers the ability to affect the world, though, the integrity and availability threats matter more* » : la manipulation de l'information constitue un risque croissant à mesure que les systèmes deviennent plus capables et plus autonomes ; le déni de service représente également une menace croissante à mesure que les systèmes deviennent plus indispensables et revêtent une importance plus critique ; le piratage et les intrusions informatiques constituent aussi un danger croissant étant donné que les systèmes ont

---

new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; 2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification; 3. A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history; 4. The foundational framework of a surveillance economy; 5. As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth; 6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; 7. A movement that aims to impose a new collective order based on total certainty; 8. An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty."

[1656] B. SCHNEIER, *Click here to kill everybody, Id.,* p. 57: "*Corporations want your data. The websites you visit are trying to figure out who you are and what you want, and they're selling that information. The apps on your smartphone are collecting and selling your data. The social networking sites you frequent are either selling your data, or selling access to you based on your data. Harvard Business School professor Shoshana Zuboff calls this "surveillance capitalism", and it's the business model of the Internet."*

[1657] B. SCHNEIER, *Click here to kill everybody, Ibid.,* p. 65: "*It isn't that the NSA woke up one morning and said: "let's spy on everyone." It said: "Corporate America is spying on everyone. Let's get ourselves a copy." And it does – through bribery, coercion, threats, legal compulsion, and outright theft – collecting cell phone location data, Internet cookies, e-mails and text messages, log-in credentials, and so on. Other countries operate in a similar fashion.*"

des incidences et des répercussions sur la vie et les biens[1658]. Dans ce contexte, les atteintes à la confidentialité de l'information affectent la vie privée, alors que les atteintes à l'intégrité ou à la disponibilité de l'information peuvent affecter la sécurité ou la vie d'une personne. En effet, violer la confidentialité d'un dossier médical est certes préoccupant, mais modifier le groupe sanguin ou la liste des allergies de ce dossier (risque/menace d'intégrité) voire arrêter ou éteindre du matériel d'importance vital (risque/menace de disponibilité/mise à disposition) représentent des préoccupations d'une importance majeure et vitale : « *one way of thinking about this is that confidentiality threats are about privacy, but integrity and availability threats are really about safety* »[1659].

L'histoire de l'homme illustre clairement et pragmatiquement les multiples épisodes d'abus systématiques des pouvoirs de surveillance. Les systèmes et techniques de surveillance ont ainsi été invariablement et abusivement utilisés contre des syndicalistes et des personnes soupçonnées d'être communistes après la Première guerre mondiale, contre des défenseurs des droits civils, contre des protestataires de la guerre au Vietnam, contre Martin Luther King, contre des musulmans, des militants pour les droits de l'homme ou pour la paix, des militants pour ou contre l'avortement, des groupes minoritaires ou ethniques et ainsi de suite, comme il a pu être observé à travers cette étude. Il semble bien qu' « *aux yeux de l'autorité, rien ne ressemble autant à un terroriste qu'un homme ordinaire* »[1660]. Bien plus de cas pourraient être cités relayant les abus effectués par des entreprises nationales et internationales, des services de renseignement particuliers élargissant secrètement leurs missions, des écoles, des forces de l'ordre et agents de police nationale, des collectivités locales et fonctionnaires publics, voire par des centres de fusion. À cet égard, « *Boston's fusion center spied on Veterans for peace, the women's anti-war organization Code Pink, and the Occupy movement* »[1661].

Les « *fusion centers* » ou centres de fusion ne cessent de se multiplier depuis peu, considérés comme étant le futur des centres d'échange et de fusion de données dans les domaines de sécurité, de lutte contre le terrorisme et de prévention des crimes, plus communément appelés en Europe 'coordinateurs nationaux ou internationaux'. Ils sont définis comme étant des « *organisations tasked with interagency coordination in the field of preventing and countering*

[1658] B. SCHNEIER, *Click here to kill everybody, Ibidem,* p. 79, et l'auteur donne un exemple: "*My car has an Internet connection. And while I am worried that someone will hack into the car and eavesdrop on my conversations through the Bluetooth connection (a confidentiality threat), I am much more worried that they will disable the brakes (an availability threat) or modify the parameters of the automatic lane-centering and following-distance systems (an integrity threat). The confidentiality threat affects my privacy; the availability and integrity threats can kill me. It's the same with databases."*

[1659] B. SCHNEIER, *Click here to kill everybody, Ibidem,* p. 79.

[1660] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Id.*, p. 48-49.

[1661] B. SCHNEIER, *Data and Goliath*, *op. cit.*, p. 123.

terrorism. As such, most fusion centres are responsible for coordinating, analysing, combining, and facilitating information sharing with regard to terrorism, and in some cases in relation to broader security threats »[1662], ou encore comme « *a collaborative effort of two or more agencies that provide resources, expertise and information to the centre with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity* »[1663]. Six centres de fusion sont pour le moment recensés en Europe[1664], et 79 sont reconnus et listés par le Ministère de la Sécurité Intérieure des États-Unis[1665], sans compter le Cyber Fusion Centre d'Interpol[1666], le UNCCT - United Nations Counter-Terrorism Centre ou encore le ECTC - European Counter Terrorism Centre[1667]. Ces centres de fusion visent à établir un environnement de partage et d'échange d'informations, qu'elles soient d'origines publique ou privée, pour les traiter et les analyser de manière plus efficace afin de lutter contre le

[1662] R. VAN DER VEER, W. BOS et L. VAN DER HEIDE, ICCT Report "Fusion Centres in Six European Countries: Emergence, Roles and Challenges", International Centre for Counter-Terrorism – The Hague, Février 2019, p. 2: https://icct.nl/wp-content/uploads/2019/02/ICCT-VanderVeer-Bos-VanderHeide-Fusion-Centres-in-Six-European-Countries.pdf

[1663] Department of Homeland Security of the United States, "National Network of Fusion Centers Fact Sheet": "*fusion centers serve as primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, and territorial (SLTT) partners. Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection and private sector security personnel to lawfully gather and share threat-related information. They provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. Fusion centers conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners [...]*": https://www.dhs.gov/national-network-fusion-centers-fact-sheet

[1664] "*Belgium (CUTA), Germany (GTAZ and GETZ), Italy (CASA), The Netherlands (NCTV), Spain (CITCO), and the United Kingdom (JTAC)*": R. VAN DER VEER, W. BOS et L. VAN DER HEIDE, ICCT Report "Fusion Centres in Six European Countries: Emergence, Roles and Challenges", *Id.,* p. 2.

[1665] Department of Homeland Security of the United States, "2017 National Network of Fusion Centers - Final Report", October 2018: https://www.hsdl.org/?view&did=817528

[1666] Interpol – Investigative support for Cybercrime, "*Cyber Fusion Centre – actionable intelligence: Our Cyber Fusion Centre brings together cyber experts from law enforcement and industry to gather and analyze all available information on criminal activities in cyberspace and provide countries with coherent, actionable intelligence. The Centre publishes reports to alert countries to new, imminent or evolving cyber threats; these include malware, phishing, compromised government websites, social engineering fraud and more. In 2017, we provided 183 reports to police in nearly 70 member countries worldwide, while in the first half of 2018 alone, we disseminated 187 reports to 138 countries*.": https://www.interpol.int/Crimes/Cybercrime/Investigative-support-for-cybercrime

[1667] European Counter Terrorism Centre – ECTC: *"[...] in January 2016 Europol created the European Counter Terrorism Centre (ECTC), an operations centre and hub of expertise that reflects the growing need for the EU to strengthen its response to terror.*
Designed as a central hub in the EU in the fight against terrorism, the ECTC focuses on: providing operational support upon a request from a EU Member State for investigations; tackling foreign fighters; sharing intelligence and expertise on terrorism financing (through the Terrorist Finance Tracking Programme and the Financial Intelligence Unit); online terrorist propaganda and extremism (through the EU Internet Referral Unit); illegal arms trafficking; international cooperation among counter terrorism authorities.": https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc

terrorisme, prévenir les crimes et les menaces à la sécurité conformément, notamment, aux nouvelles lois mises en vigueur.

À l'aube de la révolution numérique, les systèmes, dispositifs et technologies deviennent déjà plus performants, plus capables, plus automatisés et plus autonomes au nom du développement de la science et de la technologie pouvant, à terme, entraîner des conséquences réelles, voire destructives, sur la vie des personnes étant donné que les systèmes ont été conçus avec des failles de sécurité pour assurer la viabilité et la continuité du système et du modèle de surveillance, d'interception et de contrôle mis en place, au nom de la prévention et de l'application de la loi. Il est important de noter que « *as long as companies are free to gather as much data about us as they possibly can, they will not sufficiently secure our systems. As long as they buy, sell, trade and store that data, it's at risk of being stolen. And as long as they use it, we risk it being used against us* »[1668], et cela comprend l'Etat-entreprise émergent.

Cela dit, des nouvelles technologies ne cessent d'être créées et développées et des centres de fusion sont de plus en plus mis en place pour centraliser les échanges d'informations afin de traiter et d'analyser efficacement la masse de données à leurs dispositions, pour investiguer et prévenir les menaces à la sécurité et les cyber-menaces, lutter contre le crime et les cyber-crimes. Leurs rôles et missions ont progressivement évolué au fil du temps, incluant par exemple la coordination des programmes régionaux, nationaux de prévention de l'extrémisme violent[1669], voire pour prévenir tous les crimes et risques potentiels[1670]. En résumé, « *fusion centers allow the government, in the name of "information sharing," to supplement its constitutionally constrained data-gathering activities with the unregulated collections of private industry. In return, the government amplifies the limited reach of local law enforcement, and sometimes even of private industry, with its greater power and larger scope. […]. Thus the combined resources of essentially unregulated industry data collecting, the close surveillance*

[1668] B. SCHNEIER, *Click here to kill everybody, Ibidem,* p. 59.

[1669] R. VAN DER VEER, W. BOS et L. VAN DER HEIDE, ICCT Report "Fusion Centres in Six European Countries: Emergence, Roles and Challenges", *Id.,* Section 4.1. Development of the Role of Fusion Centres, p. 13.

[1670] F. PASQUALE, *The Black Box Society*, *Id.,* p. 46 où l'auteur indique : "*Even many civil libertarians would not object to fusion centers if they restricted themselves to the responsible deployment of antiterrorist intelligence. But they do not. The Center for Investigative Reporting notes that "since so many states are unlikely to be struck by terrorists, fusion centers have had to expand their intelligence mission to cover all crimes and potential hazards, partly to convince local legislators they're worth financing with taxpayer money into the future." Pork-barrel politics trumps sensible security policy. […]. Expansion of the antiterror mission helped generate "buy in" from local and state agencies that did not themselves feel threatened by terrorism. This is a common outcome in many fusion centers. [According to the CRS report, "less than 15% of fusion centers interviewed for [the report] described their mission as solely counterterrorism. In the last year, many counterterrorism-focused centers have expanded their mission to include all-crimes and/or all-hazards." Rollins, Fusion Centers: Issues and Options, p. 21]*'

capacities of local law enforcement, and the massive power of the federal government are at each other's disposal, and largely free from their own proper constraints »[1671].

Ayant accès aux données du secteur public comme du secteur privé et ayant la capacité de surveiller et de récolter systématiquement des données sur des personnes, activistes, militants ou communautés, ces centres semblent plus renforcer l'alliance État-entreprise, les systèmes et modèles de surveillance et de contrôle établis, et contribuent à la création massive de « *unified digital dossiers* » sur les individus, « *in other words, to "connect the dots"* »[1672], centralisant *in fine* leurs identités numériques.

§2. L'insouciance des algorithmes de traitement

Les algorithmes de traitement employés dans la nouvelle architecture du cyberespace dénotent une insouciance en ce qu'ils soulignent l'importance de l'étude de l'aspect comportemental pour répondre au mieux à son nouveau 'code' (A), générant, *de facto*, un sentiment de négociation continue de l'identité en vue d'éviter toute atteinte ou tout abus (B).

A. L'importance de l'aspect comportemental

Les structures et modèles mis en place par l'État-entreprise, nouveaux alliés secrets, ont révélé l'importance de l'étude de l'aspect comportemental des individus découlant des technologies et des algorithmes de traitement employés par les deux secteurs hybridés. Le monde du numérique s'avère être ainsi influencé et caractérisé par le « capitalisme de surveillance » émergeant dans le cyberespace, touchant à terme, le monde physique. L'objectif de Zuboff à travers son étude est d'analyser et de décrire l'obscurcissement du rêve numérique, et sa mutation rapide en un projet commercial vorace et totalement innovant qu'elle nomme « *surveillance capitalism* ». Selon la Professeure, « *surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data* »[1673]. C'est un nouvel ordre économique qui revendique l'expérience humaine comme étant une matière première libre et gratuite à utiliser pour des pratiques commerciales et computationnelles dissimulées, telles que l'extraction, la prédiction, la prévision ou la vente, afin de les traduire en données comportementales et, *in fine,* engendrer la pérennisation d'une logique économique

[1671] F. PASQUALE, *The Black Box Society*, *Ibid.,* p. 46-47.
[1672] R. VAN DER VEER, W. BOS et L. VAN DER HEIDE, ICCT Report "Fusion Centers in Six European Countries: Emergence, Roles and Challenges", *Ibid.,* Conclusion, p. 17.
[1673] S. ZUBOFF, *The Age of Surveillance Capitalism, op. cit.*, p. 8.

parasitaire, disruptive et liberticide dans laquelle le développement des produits et services serait subordonné à « *a new global architecture of behavioral modification* »[1674].

Certaines de ces données comportementales générées par les algorithmes de traitement et d'analyse sont employées pour l'amélioration des produits et services, le reste en revanche est déclaré comme étant des « surplus comportementaux à propriété exclusive » alimentant les « machines intelligentes », puis transformés en « produits de prédiction » qui anticipent ce qu'une personne va faire à l'instant présent, bientôt, mais aussi plus tard[1675]. Enfin, ces « produits de prédiction » servent le nouveau marché des données et modèles comportementaux largement exploité par les géants du web, les start-ups, et même les autorités publiques. Ceux-ci, que la Professeure nomme les « capitalistes de la surveillance », ont augmenté leurs chiffres d'affaires, pour certains de manière radicale, grâce à l'exploitation et à l'analyse des réservoirs de données en masse, les *data exhaust*[1676], non utilisées, récoltées massivement dans le monde du Big data et du capitalisme de surveillance. Les détenteurs du pouvoir dans cette nouvelle ère ont, désormais, la capacité de modifier les comportements des individus à travers des interventions numériques en temps réel, en plein état de jeu, suggérant discrètement aux consommateurs certains comportements, les amadouant, les poussant, les ajustant voire les initiant à adopter des comportements plus rentables, tout en leur fournissant les données comportementales les plus prédictives[1677]. C'est ce qui les conduit à vouloir surveiller, récolter ou acheter toujours plus de données, issues de nombreuses sources et technologies encore plus prédictives (comme la voix, le visage, les personnalités ou les émotions), pouvant générer des surplus comportementaux, tirés des excédents des expériences humaines appropriés par les capitalistes de surveillance.

Selon Zuboff, les pressions concurrentielles ont entraîné ce changement, dans lequel les algorithmes et processus informatiques automatisés connaissent non seulement les comportements des personnes, mais les façonnent et les modèlent également à grande échelle. Par conséquent, « *with this reorientation from knowledge to power, it is no longer enough to automate information flows about us; the goal now is to automate us* »[1678]. Ce capitalisme de surveillance émergeant affecte non seulement l'internet et le cyberespace, mais aussi le capitalisme tel qu'il a été historiquement conçu et connu, amorçant dès lors un nouveau monde

[1674] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. IV "The Definition".
[1675] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. 8.
[1676] *Cf.* p. 345.
[1677] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. 8, l'auteur affirme ainsi « *Eventually, surveillance capitalists discovered that the most-predictive behavioral data come from intervening in the state of play in order to nudge, coax, tune, and herd behavior toward profitable outcomes.* »
[1678] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Ibid.*, p. 8.

« où pratiquement chaque produit ou service se proclamant "*intelligent*" ou "*personnalisé*", chaque *dispositif*[1679] ou véhicule dotés de fonctions internet, chaque "*assistant personnel numérique*" ou *objet connecté* est une interface de la chaîne d'approvisionnement, la *value chain*[1680], qui génère un flux ininterrompu de données comportementales »[1681].

Le concept du capitalisme s'est donc métamorphosé au XXI^e^ Siècle, ravivant les anciennes images et théories qu'il portait, focalisé principalement sur l'exploitation du travail et la consommation en masse, tout en prenant une tournure inattendue avec d'autres phénomènes entrant en compte, produisant alors un jeu d'influences réciproques. Déjà, au XIX^e^ Siècle en Europe, les systèmes de solidarité traditionnelle ont été brisés et pulvérisés par la dynamique du capitalisme : « *fondés sur des affinités familiales, religieuses, paroissiales ou professionnelles, ces solidarités ont été remises en cause à des degrés divers dès la première industrialisation, puis avec non moins de brutalité dans le cadre de la colonisation et de la traite négrière. Aujourd'hui, ce sont les formes étatiques de solidarité qui sont à leur tour déstabilisés, celles qui ont été édifiées à l'échelle nationale précisément pour pallier cet affaiblissement des solidarités traditionnelles* », ce qui mène, affirme Supiot, à un projet de globalisation qui « *est celui d'un Marché total, peuplé de particules contractantes n'ayant entre elles de relations que fondées sur le calcul d'intérêt* »[1682]. Au lieu du travail, le capitalisme de surveillance, nouveauté du XXI^e^ Siècle, se nourrit de et exploite tous les aspects de chaque expérience humaine, caractérisant par conséquent « *a rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history* »[1683]. La connexion numérique semble représenter, à l'heure actuelle, un moyen au service d'une fin commerciale et/ou sécuritaire, le capitalisme de surveillance caractérisant le cadre fondateur d'une économie de surveillance qualifié, selon Zuboff, de fondamentalement parasitaire et autoréférentiel, centré sur soi[1684].

Sans surprise, ce fut Google le pionnier de ce nouveau modèle économique, en théorie et en pratique, l'inventant et le perfectionnant, initialement pour accroître ses revenus en exploitant l'accès exclusif qu'il détenait aux données de masse collectées mais inutilisés provenant des traces numériques, du « sillage numérique », laissés par les historiques de recherche ou les

[1679] *Cf.* p. 371.
[1680] *Cf.* p. 135.
[1681] S. ZUBOFF, « Le nouveau visage du capitalisme », Financial Times (extraits), Londres publié le 25 janvier 2019, Courrier International – n° 1487 du 2 au 8 mai 2019, p. 36.
[1682] A. SUPIOT, *La gouvernance par les nombres*, *op. cit.,* p. 15.
[1683] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. IV "The Definition".
[1684] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Ibid.*, p. 9.

activités en ligne des utilisateurs[1685]. Google s'est ainsi appliqué à mettre en place de nouvelles pratiques permettant d'analyser ces données, jusqu'à présent délaissées, pour en tirer des schémas prédictifs servant à adapter l'offre à la demande, à savoir, dans ce cas initial, les publicités aux centres d'intérêt des internautes. L'entreprise a, ainsi, induit une nouvelle forme d'exploitation des données ainsi qu'un nouvel usage à ce surplus de données à connotation comportementale, et a, par la suite, activement agi pour mettre au point des pratiques et des techniques agressives et intrusives afin d'en extraire de plus en plus de données comportementales à partir de nouvelles sources et de nouveaux dispositifs, comme les capteurs présents dans les machines mobiles tels que les téléphones portables ou les tablettes, ou encore les objets connectés qui, une fois équipés de capteurs et de dispositifs de transmission, deviennent « *à leur tour des vecteurs de nouveaux services à valeur ajoutée* »[1686].

La banalisation de la captation automatique des données a ainsi largement contribué à la mise en place et à la valorisation de ce système et ses pratiques, complétée par la valeur des nouvelles méthodes et techniques de Google qui « *tenait à leur capacité à collecter des données que les utilisateurs avaient choisi de ne pas partager et à en déduire des informations personnelles détaillées que les internautes ne fournissaient pas* »[1687]. Ces méthodes et opérations, développées et déployées dans le plus grand secret jusqu'à l'entrée en bourse de Google en 2004[1688], ont été à l'origine élaborées pour tromper la vigilance ou la prudence et l'attention des internautes et, conséquemment, écarter tout risque de réticence à utiliser leurs services. Dans ce cadre, il est donc évident que « *dès le début, Google a bâti son succès sur un miroir sans tain : la surveillance* »[1689], et son nouveau modèle a par la suite été largement adopté par les entreprises ayant envahi la Silicon Valley, tels que Facebook, Amazon ou Microsoft, puis a débordé affectant une multitude de secteurs privés comme publics, tels que l'assurance, la santé, l'éducation, le commerce de détail, le divertissement et ainsi de suite. Google a ainsi réussi à lancer une opération de marché sans précédent dans les espaces inexploités d'internet où il a rencontré peu d'obstacles juridiques ou concurrentiels, conduisant la cohérence systémique de son entreprise à un rythme effréné que ni les institutions publiques ni les individus ne pouvaient suivre.

[1685] S. ZUBOFF, « Le nouveau visage du capitalisme », *Id.*, p. 35.
[1686] CESE – E. PERES, *Les données numériques : un enjeu d'éducation à la citoyenneté*, *op. cit.*, p. 52.
[1687] S. ZUBOFF, « Le nouveau visage du capitalisme », *Id.*, p. 35.
[1688] « *Ce n'est qu'avec l'entrée en bourse de Google, en 2004, que le monde a appris que ces nouvelles pratiques avaient permis au groupe d'accroître son chiffre d'affaire de 3 590 %* » : S. ZUBOFF, « Le nouveau visage du capitalisme », *Ibid.*, p. 35-36.
[1689] S. ZUBOFF, « Le nouveau visage du capitalisme », *Ibidem*, p. 35.

En outre, Google a également su tirer profit des évènements du début du XXI[e] Siècle, notamment du 11 septembre américain, qui ont poussé les services de sécurité et les autorités publiques à être enclins à nourrir, imiter, abriter et à utiliser les capacités émergentes du capitalisme de surveillance dans un souci de connaissance totale, « *for the sake of total knowledge and its promise of certainty* »[1690] . Pionnier du capitalisme de surveillance, Google a dès lors initié un mouvement qui vise à imposer un nouvel ordre collectif fondé sur la certitude totale, tout en étant gratuit et présenté comme une contrepartie à la gratuité de ses produits et services. Ceci donne lieu à un véritable échange commercial et ressemble à la notion de *« travail abstrait* » au sens que lui accorde Marx, « *c'est-à-dire d'un travail défini non par sa valeur d'usage, mais par sa valeur d'échange. Le contrat de travail – et avec lui le marché du travail – a précisément pour objet de ramener à des quantités commensurables (et donc échangeables) de temps et d'argent l'infinie diversité des activités humaines et le sens particulier que nous prêtons à chacune d'elle* »[1691].

De nos jours, il est pratiquement impossible d'échapper à ce nouveau marché qui atteint tous les secteurs, toutes les technologies, tous les outils informatiques ou objets connectés que les personnes utilisent dans leur quotidien et pour n'importe quelle activité, qu'elle soit sociale, personnelle ou professionnelle, générant de manière illimitée une masse de données, de métadonnées et de *data exhaust*. Les pratiques de ce nouveau modèle économique influencent, ainsi, non seulement le choix du trajet pour aller vers un restaurant, mais aussi quel restaurant choisir grâce aux recommandations de Google, de Yelp ou de Siri ; le jeu Pokémon Go guide discrètement et subtilement les pas de ses joueurs pour aller consommer dans les restaurants, les cafés, les bars ou magasins ayant payé pour assurer leur place dans ce nouveau « méta-marché des comportements »[1692] ; l'expropriation et l'exploitation acharnées par Facebook du surplus tiré des profils de ses utilisateurs façonnent leur comportement individuel, qu'il s'agisse d'acheter une crème particulière à 17h45 le vendredi, de cliquer « oui » sur une offre pour des nouvelles chaussures de course pendant que les endorphines traversent encore le cerveau après une longue course du dimanche matin, ou d'aller voter la semaine prochaine, voire détournent ces surplus comportementaux afin de « dresser des "*profils psychologiques*" détaillés permettant à un annonceur de repérer le moment précis pendant lequel un adolescent a besoin

[1690] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. 9.
[1691] A. SUPIOT, *La gouvernance par les nombres*, *Id.,* p. 353.
[1692] S. ZUBOFF, « Le nouveau visage du capitalisme », *Id.*, p. 36.

de "*reprendre confiance en lui*" et est, par conséquent, plus vulnérable à une configuration particulière d'incitations publicitaires »[1693].

Dans ce contexte, indique Zuboff, « *just as industrial capitalism was driven to the continuous intensification of the means of production, so surveillance capitalists and their market players are now locked into the continuous intensification of the means of behavioral modification and the gathering might of instrumentarian power* »[1694]. Or, toutes ces suggestions et recommandations personnalisées fournies grâce aux règles codées dans les algorithmes de traitement et d'analyse, guidant désormais le comportement et la vie de tous les jours, sont traitées et proclamées par les détenteurs de ces pouvoirs et les agents de ces modèles et systèmes émergents comme étant de simples problèmes purement techniques, pendant que les valeurs et prérogatives que ces règles encodées édictent restent cachées dans des boîtes noires : « *Without knowing what Google actually does when it ranks sites, we cannot assess when it is acting in good faith to help users, and when it is biasing results to favor its own commercial interests. The same goes for status updates on Facebook, trending topics on Twitter, and even network management practices at telephone and cable companies. All these are protected by laws of secrecy and technologies of obfuscation* »[1695].

Cela a d'ailleurs été également les pratiques et les méthodes adoptées lors de l'affaire de Cambridge Analytica[1696]. En 2016, A. Nix, directeur général de l'entreprise d'étude de marché Cambridge Analytica, présenta lors du Sommet Concordia, « *a member-based organization dedicated to actively fostering, elevating, and sustaining cross-sector partnerships for social impact* »[1697], ses développements sur « *The power of Big Data and Psychographics* »[1698]. Définies dans la science comme étant une « *description psychologique d'un individu* » et synonyme de « *profils psychologiques* »[1699], les psychographies représentent, selon Nix, une compréhension et une connaissance exacte des traits de personnalité des personnes[1700]. Pour

[1693] S. ZUBOFF, « Le nouveau visage du capitalisme », *Ibid.*, p. 36.
[1694] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. 8-9.
[1695] F. PASQUALE, *The Black Box society*, *op. cit.,* p. 9.
[1696] *Cf.* p. 371.
[1697] Concordia – About us, "Building partnerships for social impact": https://www.concordia.net/about/
[1698] Concordia, 2016 Concordia Summit Agenda, Session Description - The Power of Big Data and Psychographics: "*In this 10 minute presentation, Mr. Alexander Nix will discuss the power of big data in global elections Cambridge Analytica's revolutionary approach to audience targeting, data modeling, and psychographic profiling has made them a leader in behavioral microtargeting for election processes around the world*.": https://www.concordia.net/the-summit-2016/2016-concordia-summit-agenda/#rdv-calendar
[1699] CNRTL, « Psychographie », et une remarque « Psychographique, adj. Qui utilise les descriptions psychologiques d'individus. » : https://www.cnrtl.fr/definition/psychographie//0
[1700] S. VAIDHYANATHAN, *Anti-social media*, *op. cit.*, p. 151-152, et A. NIX, « The Power of Big Data and Psychographics » (Concordia Summit), *Id.* : *"[...]probably more important are psychographics, that is, un*

établir un profil psychographique, il faut recourir au modèle dit « OCEAN » : « *psychographic profiling uses character designations such as "openness" (how welcoming a person is to new experiences), "conscientiousness" (how much one prefers order and regularity or change and fluidity), "extroversion" (how social a person is), "agreeableness" (one's willingness to put other people's needs above their own), and "neuroticism" (how much a person worries)* »[1701].
L'entreprise, pour réussir son modèle et alimenter efficacement son système, avait donc besoin d'une quantité volumineuse de données personnelles, comportementales, révélant la personnalité et les inclinations des individus, et s'est donc simplement retournée vers les *data brokers*, les courtiers en données, et les agrégateurs de données privés qui les fournissent et les vendent. Ces derniers possèdent des données et des dossiers personnels sur des millions de consommateurs à travers le monde, basés sur leurs historiques d'achats et leurs caractéristiques démographiques notamment. Mais cela s'est révélé ne pas être suffisant pour bien mener la réussite du système et l'usage des profils psychographiques, objet même du scandale qui a mouillé Cambridge Analytica, mais surtout Facebook. L'ampleur de l'affaire fut ainsi dévoilée grâce à un article initialement paru en Suisse dans *Das Magazin* en décembre 2016[1702], puis traduit et publié par le journal en ligne *Motherboard* en janvier 2017[1703].
Dans les années 80, des psychologues ont établi le domaine d'étude que représente la psychométrie, parfois également appelée psychographie, qui se concentre sur la mesure des traits psychologiques, tels que la personnalité, et ont élaboré un modèle visant à évaluer les êtres humains en fonction de cinq traits de personnalité qui ont fourni les initiales de OCEAN devenu le standard technique des psychométries : « *Based on these dimensions—they are also known as OCEAN, […]—we can make a relatively accurate assessment of the kind of person in front of us. This includes their needs and fears, and how they are likely to behave* »[1704], générant, *in fine*, des modèles de prédiction de comportements.

---

understanding of your personality. […]. If you know the personality of the people you are targeting you can nuance your message to resonate more effectively with those key audience groups. A different collection of personality traits might demand a different sort of advertisement, […]. So, some voters might be moved by a warm and family-oriented video that reminds a voter about the pleasures of hunting with a grandchild, for instance. Some voters need to be nudged to the left to support a particular candidate, while others might need to be nudged to the right to support the same candidate. With enough data and subtle psychographic profiles, […], a firm or campaign could develop just the right message for a particular voter or narrow set of voters."
[1701] S. VAIDHYANATHAN, *Anti-social media*, *Id.*, p. 151.
[1702] H. GRASSEGGER et M. KROGERUS, "Ich habe nur gezeigt, dass es die Bombe gibt", Das Magazin, Publié le 3 décembre 2013: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/
[1703] H. GRASSEGGER et M. KROGERUS, "The Data That Turned the World Upside Down", Motherboard Vice, publié le 28 janvier 2017: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win
[1704] H. GRASSEGGER et M. KROGERUS, "The Data That Turned the World Upside Down", *Id.*

Néanmoins, pendant longtemps, le problème de cette approche fut la collecte des données qui impliquait des questionnaires à remplir, long, complexes et très personnels, limitant par conséquent les capacités de ce modèle. Puis vint internet et le cyberespace, Facebook et ses services, ainsi que les réflexions et études du chercheur au centre de psychométrie de l'université de Cambridge M. Kosinsky qui eut l'idée d'utiliser l'application *MyPersonality* de Facebook. Les médias et les tabloïds ont, depuis longtemps, publié des articles et des histoires séduisantes sur la manière dont certains comportements ou certaines préférences "révèlent votre personnalité" sans compter l'existence de l'importante industrie des tests de personnalité, appliquant le Myers-Briggs system[1705], consacrée aux tests de personnalité pour aider la performance des employés, les capacités de gestion d'un manager ou les capacités de recrutement d'un recruteur ; les individus étaient ainsi plus que disposés et désireux de répondre aux questionnaires de personnalité. Kosinsky a dès lors développé une application qui fonctionnerait à l'intérieur de Facebook que ses utilisateurs seraient heureux de partager, en ayant le choix de partager leurs données de profil Facebook, y compris leurs historiques des "j'aime", ainsi que les réponses du questionnaire, avec le chercheur. Celui-ci pouvait ensuite analyser et corréler l'ensemble de ces données, « *to connect the dots* », pour générer des modèles de prédictions pouvant révéler de nombreux aspects de l'identité d'une personne, allant bien au-delà des mesures de l'échelle OCEAN[1706]. Développant ces modèles incessamment,

[1705] The Myers & Briggs Foundation, Myers-Briggs type indicator – MBTI: "*The purpose of the Myers-Briggs Type Indicator (MBTI®) personality inventory is to make the theory of psychological types described by C. G. Jung understandable and useful in people's lives. The essence of the theory is that much seemingly random variation in the behavior is actually quite orderly and consistent, being due to basic differences in the ways individuals prefer to use their perception and judgment*.": https://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/home.htm?bhcp=1; Pour des exemples des tests de personnalité fondés sur le système Myers-Briggs : Jung Typology Test – a free personality test : http://www.humanmetrics.com/cgi-win/jtypes2.asp; NERICS Analytics, 16personalities – Free personality test: https://www.16personalities.com/free-personality-test; Truity, The TypeFinder® Personality Test – Free personality test: https://www.truity.com/test/type-finder-personality-test-new

[1706] H. GRASSEGGER et M. KROGERUS, "The Data That Turned the World Upside Down", *Id.*: "*The approach that Kosinski and his colleagues developed over the next few years was actually quite simple. First, they provided test subjects with a questionnaire in the form of an online quiz. From their responses, the psychologists calculated the personal Big Five values of respondents* [les valeurs de l'échelle OCEAN]. *Kosinski's team then compared the results with all sorts of other online data from the subjects: what they "liked," shared or posted on Facebook, or what gender, age, place of residence they specified, for example. This enabled the researchers to connect the dots and make correlations.*
Remarkably reliable deductions could be drawn from simple online actions. For example, men who "liked" the cosmetics brand MAC were slightly more likely to be gay; one of the best indicators for heterosexuality was "liking" Wu-Tang Clan. Followers of Lady Gaga were most probably extroverts, while those who "liked" philosophy tended to be introverts. While each piece of such information is too weak to produce a reliable prediction, when tens, hundreds, or thousands of individual data points are combined, the resulting predictions become really accurate. Kosinski and his team tirelessly refined their models. In 2012, Kosinski proved that on the basis of an average of 68 Facebook "likes" by a user, it was possible to predict their skin color (with 95 percent accuracy), their sexual orientation (88 percent accuracy), and their affiliation to the Democratic or Republican party (85 percent). But it didn't stop there. Intelligence, religious affiliation, as well as alcohol, cigarette and drug use, could all be determined. From the data it was even possible to deduce whether

Kosinski a été rapidement en mesure d'évaluer une personne mieux que le collègue de travail moyen, simplement sur la base de 10 "j'aime" de Facebook : « *Seventy "likes" were enough to outdo what a person's friends knew, 150 what their parents knew, and 300 "likes" what their partner knew. More "likes" could even surpass what a person thought they knew about themselves* » ; et ces modèles ne se sont aucunement limités à la simple étude des "j'aime"[1707].
À la suite de la publication de ces recherches et modèles, un de ces collègues de l'université, A. Kogan, devenu depuis Dr. Specter, l'a abordé pour établir une collaboration et un contrat de licence exclusif sur ses questionnaires et ses modèles avec l'entreprise SCL – Strategic Communication Laboratories[1708] – société mère de Cambridge Analytica, ce qu'il a refusé[1709].
Les suspicions du chercheur quant à l'utilisation dissimulée de ses modèles de prédictions par l'entreprise en question ont commencé avec les résultats de l'élection de Trump et du vote du Brexit en 2016, corroborés par les revendications de Cambridge Analytica, puis confirmés en 2018 par l'ancien ingénieur de l'entreprise devenu lanceur d'alerte, C. Wylie, et les révélations médiatiques. Les investigations ont ainsi montré l'implication de Kogan qui avait effectivement copié les données des utilisateurs Facebook, et vendu l'accès à celles-ci à l'entreprise en cause qui a, alors, pu construire des modèles pour prédire les comportements des électeurs ; de plus, Cambridge Analytica « *had convinced campaigns in the United States and around the world that the models would help target and persuade voters* »[1710], ce qui fut bien le cas à deux reprises en 2016.
Le capitalisme de surveillance, mis en place initialement pour accroître les profits à travers les publicités en ligne adaptées et personnalisées, s'est bel et bien étendu ne se limitant plus au jeu compétitif des grandes entreprises numériques. Les modèles et produits prédictifs d'aujourd'hui

---

someone's parents were divorced. The strength of their modeling was illustrated by how well it could predict a subject's answers."

[1707] H. GRASSEGGER et M. KROGERUS, "The Data That Turned the World Upside Down", *Id.*: "*But it was not just about "likes" or even Facebook: Kosinski and his team could now ascribe Big Five values based purely on how many profile pictures a person has on Facebook, or how many contacts they have (a good indicator of extraversion). But we also reveal something about ourselves even when we're not online. For example, the motion sensor on our phone reveals how quickly we move and how far we travel (this correlates with emotional instability).* ***Our smartphone, Kosinski concluded, is a vast psychological questionnaire that we are constantly filling out, both consciously and unconsciously***.
Above all, however—and this is key—it also works in reverse: not only can psychological profiles be created from your data, but your data can also be used the other way round to search for specific profiles: all anxious fathers, all angry introverts, for example—or maybe even all undecided Democrats? Essentially, what Kosinski had invented was sort of a people search engine."

[1708] SCL - Strategic Communication Lab: Aligning communication with intended results: https://www.scl.us.com/index.html

[1709] S. VAIDHYANATHAN, *Anti-social media*, *Ibid.*, p. 154, et, H. GRASSEGGER et M. KROGERUS, "The Data That Turned the World Upside Down", *Ibid.*

[1710] S. VAIDHYANATHAN, *Anti-social media, Ibidem*, p. 155, et, H. GRASSEGGER et M. KROGERUS, "The Data That Turned the World Upside Down", *Ibidem.*

sont négociés dans le méta-marché des comportements qui vont au-delà du secteur des annonces en ligne ciblées pour inclure de nombreux autres secteurs, y compris l'assurance, la vente en détail, la finance et un éventail toujours plus vaste d'entreprises de biens et de services déterminées à participer à ces nouveaux marchés rentables : « *Eventually, competitive pressure drove expansion into the offline world, where the same foundational mechanisms that expropriate your online browsing, likes, and clicks are trained on your run in the park, breakfast conversation, or hunt for a parking space. […]. Whether it's a "smart" home device, what the insurance companies call "behavioral underwriting," or any one of thousands of other transactions, we now pay for our own domination* »[1711].

Les capitalistes de surveillance produisent et opèrent à travers des asymétries sans précédent, et se révélant être antidémocratiques, en matière de connaissance, de savoir, et du pouvoir découlant de ce savoir. Ceux-ci savent « tout de nous, et font tout pour que nous ne sachions absolument rien de leurs pratiques ; ils prédisent notre avenir et manipulent notre comportement, mais pour le compte de tiers qui en tireront un profit financier ou l'exploiteront à leurs fins. C'est le pouvoir sans précédent de connaître et de modifier le comportement humain […], souvent confondu avec le "totalitarisme" et redouté comme une nouvelle incarnation de Big Brother, c'est un type nouveau de pouvoir que Zuboff appelle "l'instrumentalisme" »[1712].

Les surplus comportementaux déduits des données personnelles touchant tous les aspects de la vie quotidienne, laissant de côté tout ce qui donne du sens au corps, à l'esprit, et à l'affect humains, sont la source et la valeur d'échange qui créent le produit ; l'humain n'étant plus "le produit" mais bien la « carcasse abandonnée », "le produit" provient désormais du surplus extrait de sa vie et de ses expériences personnelles : « *il fut un temps où nous étions les sujets de notre vie ; nous en sommes maintenant les objets* »[1713].

C'est finalement la dépendance des personnes aux services, produits et outils numériques et au cyberespace devenu fondamental, notamment pour la participation et l'inclusion sociale, qui est au cœur de ce capitalisme de surveillance, dans lequel l'efficacité, les capacités et les besoins ressentis rivalisent avec la tendance à résister à ses ingérences et incursions audacieuses[1714]. Or

---

[1711] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. 10.

[1712] S. ZUBOFF, « Le nouveau visage du capitalisme », *Id.*, p. 37, et, S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. 8: "*Instrumentarian power knows and shapes human behavior toward others' ends. Instead of armaments and armies, it works its will through the automated medium of an increasingly ubiquitous computational architecture of "smart" networked devices, things, and spaces*."

[1713] S. ZUBOFF, « Le nouveau visage du capitalisme », *Ibid.*, p. 36-37.

[1714] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Id.*, p. 10-11: "***Consider that the internet has become essential for social participation, that the internet is now saturated with commerce, and that commerce is now subordinated to surveillance capitalism***. *Our dependency is at the heart of the commercial surveillance project, in which our felt needs for effective life vie against the inclination to resist its bold incursions. This conflict*

Zuboff précise que « *just as industrial civilization flourished at the expense of nature and now threatens to cost us the Earth, an information civilization shaped by surveillance capitalism and its new instrumentarian power will thrive at the expense of human nature and will threaten to cost us our humanity* »[1715].

B. La négociation de l'identité (numérique)

Cette négociation de l'identité, notamment numérique, s'inscrit dans la continuité de l'âge documentaire[1716] qui s'est également transformé avec la mise en place de la nouvelle architecture du cyberespace et des pratiques, méthodes et dispositifs employés. La e-documentation semble être plus complète dans les mains des capitalistes de surveillance que dans celles dont elle fait l'objet : la documentation de soi se trouve alors complétée et perfectionnée par d'autres pour des finalités aussi diverses que variées ne se résumant plus seulement à des valeurs marchandes, à du profit et aux publicités ciblées et personnalisées, mais dépendra, *in fine*, de l'intérêt et de la volonté particulière de l'entité ou de l'organisation qui l'exploite. En effet, la e-documentation se cultive et s'établit à travers les efforts de l'individu aspirant à avoir une présence numérique, à créer son image et sa réputation numériques telles qu'il les perçoit et en suivant l'image voulue. Néanmoins, l'individu, avec les nouvelles pratiques et structures, est dépassé se trouvant être aujourd'hui l'objet exploité tout en vivant dans l'illusion qu'il cultive et affermit son image selon sa propre volonté.

La e-documentation de soi et la réputation développée restent ainsi à un niveau individuel, sociétal, perçues par ses pairs et collègues, pendant que se met en place, en amont, un dossier numérique unifié retraçant la biographie complète et détaillée de ce même individu, y compris sa propre documentation de soi et les efforts relatifs à sa e-réputation, à l'abri de son regard ou de son savoir. Or, même les outils d'aide à la construction et à la gestion de sa e-réputation et les techniques de *personal branding*[1717] employées fonctionnent par le biais d'algorithmes secrets et inaccessibles traitant une masse de données, pour la plupart inconnues de la personne

---

produces a psychic numbing that inures us to the realities of being tracked, parsed, mined, and modified. It disposes us to rationalize the situation in resigned cynicism, create excuses that operate like defense mechanisms ("I have nothing to hide"), or find other ways to stick our heads in the sand, choosing ignorance out of frustration and helplessness. In this way, surveillance capitalism imposes a fundamentally illegitimate choice that twenty-first-century individuals should not have to make, and its normalization leaves us singing in our chains."

[1715] S. ZUBOFF, *The Age of Surveillance Capitalism*, *Ibid.*, p. 11, et The Definition p. IV "*5. As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth*;"

[1716] *Cf.* p. 103 et s.

[1717] *Cf.* p. 120 et s.

concernée. En effet, « *in ever more settings, reputation is determined by secret algorithms processing inaccessible data. Few of us appreciate the extent of ambient surveillance, and fewer still have access either to its results—the all-important profiles that control so many aspects of our lives—or to the "facts" on which they are based* »[1718].

La nouvelle architecture du cyberespace permet d'observer les informations concernant les personnes, de les enregistrer et de les analyser, moyennant les algorithmes et les pratiques computationnelles calculatoires développés, pour déterminer des modèles de comportement communs, des profils comportementaux, aux criminels, aux activités terroristes, aux activistes ou manifestants, à une communauté ou un groupe minoritaire ; *in fine*, des modèles de comportement communs à une catégorie en particulier. Le résultat de ces analyses et calculs secrets entraînent des effets palpables dans la vie de la personne concernée sans que le processus de la méthode, de la pratique employée ne soit visible à la personne victime du résultat généré. La surveillance produit des informations, qui sont de nos jours facilement sauvegardées et réutilisées pour de nouvelles finalités, souvent dissimulées, de sorte que « *being watched and inhibited in one's behavior is only one part of the problem ; the other dimension is that the data is warehoused for unknown future uses. This is where Orwell meets Kafka* »[1719].

La révolution numérique a grandement facilité la collecte et la combinaison des informations, y compris des informations d'une apparence superficielle ou incomplète qui, finalement, trouvent leur place idéale dans la société de l'information et du Big data, se révélant être très utiles pour obtenir plus de données personnelles sur les individus. *De facto*, les informations produisent des informations qui, prises séparément ne divulguent pas beaucoup sur l'individu, mais peuvent induire ou produire d'autres informations repérant ou accordant l'accès à d'autres informations bien plus personnelles et intimes. Autrement dit, « *viewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities* »[1720].

La valeur des données collectées, y compris celles partagées volontairement sur les réseaux, ne peut être réellement estimée de manière certaine, pouvant différer selon les finalités pour

---

[1718] F. PASQUALE, *The Black Box society*, *op. cit.,* p. 14.

[1719] D. SOLOVE, *The Digital Person*, *op. cit.,* p. 42 où l'auteur cite F. Dürrenmatt qui, selon lui, saisit le mieux l'interrelation existante entre surveillance et bureaucratie à l'ère de l'information : « *[W]hat was even worse was the nature of those who observed and made a fool of him, namely a system of computers, for what he was observing was two cameras connected to two computers observed by two further computers and fed into computers connected to those computers in order to be scanned, converted, reconverted, and, after further processing by laboratory computers, developed, enlarged, viewed, and interpreted, by whom and where and whether at any point by human beings he couldn't tell.* » [Friedrich Dürrenmatt, The Assignment: Or, on the Observing of the Observer of the Observed, Joel Agee translation, 1988, University Chicago Press, p. 109].

[1720] D. SOLOVE, *The Digital Person*, *Id.,* p. 146.

lesquelles les données sont traitées. Et ce problème d'évaluation est aggravé par le caractère trivial et incrémental de chaque information personnelle découverte ou communiquée, qui tend dans ces conditions à minimiser l'étendue de son impact final, alors que « *a comprehensive collection of data about an individual is vastly more than the sum of its parts* »[1721].

Les pratiques et techniques utilisées à notre époque ont facilité et accéléré les agrégations des données et leurs analyses permettant la mise au point de dossiers numériques détaillés unifiés remplis d'informations combinées en vue de créer des biographies complètes sur les personnes, des biographies « non autorisées » ; les dossiers numériques étant « *a way of representing the individual to the gaze of the world* »[1722]. Toute trace de donnée rendue visible fait l'objet d'une surveillance, menant à la création de nouvelles traces dévoilant plus d'informations personnelles sur la personne, qui initialement ne comptait pas les révéler, et aboutissant à l'établissement d'un portrait complet de sa personne, sa personnalité, ses opinions et intérêts ou ses comportements. C'est « l'effet de l'agrégation », selon le Professeur Solove, « *similar to a Seurat painting, where a multitude of* ***dots*** *juxtaposed together form a picture, bits of information when aggregated paint a portrait of a person* »[1723].

Toute donnée, toute trace de donnée est porteuse de sens, de savoirs et de révélations intimes sur l'individu la générant, volontairement ou involontairement, après avoir fait l'objet d'un traitement, donc d'une collecte, d'une agrégation, d'une corrélation, d'une analyse. Les méthodes et techniques de traitement et d'analyse des données créent alors les biographies numériques suivant une procédure standard, normalisée, définie par l'organisation les ayant adoptées (entreprise, association, gouvernement etc.), qui, pour la plupart, consiste à classer les données et profils de leurs utilisateurs-consommateurs en catégories ou en types, fondés pour la plupart sur des stéréotypes.

En effet, il semble qu'à travers les nombreux choix qu'un individu a quotidiennement, que ce soit pour choisir un service, un bien, un produit, une destination ou une trajectoire, le service choisi ou le produit consumé se révèle être l'expression de son identité : « *the relationship between consumption and identity is stronger than incidental linkages. Consumption patterns*

[1721] J. E. COHEN, « Examined Lives: Informational Privacy and the Subject as Object », Stanford Law Review Vol. 52, Mai 2000 (p. 1373-1438), p. 1397, où l'auteur cite en note de bas de page A. M. Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases, 15 J.L. & COM. 395, 1996 (p. 479-505), p. 492 *"[A]s long as in each individual transaction the cost of not providing the information is disproportionate to the loss (which is a function of the cumulation of the transactions, not any single transaction)* ***a property rights approach appears unlikely to have much real influence on database creation.***"

[1722] J. E. COHEN, *Configuring the networked self*, *op. cit.,* p. 124.

[1723] D. SOLOVE, *The Digital Person, Id.,* p. 44.

that define a "cluster identity" strongly correlate with political and social views. [... And], the identity of many subcultures is directly related to distinctive patterns of consumption. [...]. To summarize, consumption patterns, as revealed by consumer records, are related to individuals' identities »[1724].

La documentation de soi combinée à la collecte des métadonnées et du *data exhaust* et donc de toute trace numérique laissée dessinent, *in fine*, une biographie numérique complète sur l'individu concerné, révélant indéniablement son identité qui, ensuite, fera l'objet de négociation constante, que ce soit du côté de l'individu, alors qu'il essaie de construire ou d'améliorer son image et sa présence numérique, ou alors du côté des capitalistes de surveillance qui ont le choix de la négocier, de manière interne, pour la catégoriser, lui vendre un produit ou le pousser subtilement à adopter un certain comportement, ou alors de la négocier avec une autre organisation qui souhaite acquérir la biographie en question ou y avoir accès. Un des exemples les plus parlant concerne les systèmes publicitaires en ligne qui fonctionnent « *sur la base d'un système d'enchères en temps réel (real-time bidding).* [Ainsi] *pendant que l'internaute est en train de charger la page web qu'il désire consulter, son profil est mis aux enchères par un automate afin que des robots programmés par les annonceurs se disputent le meilleur prix pour placer leur bandeau publicitaire. L'opération dure moins de 100 millisecondes* »[1725].

Il est important de noter qu'en dépit du fait qu'une biographie numérique contient une foule de données concernant une personne, elle ne saisit finalement qu'une « *distorted persona* »[1726], une image déformée de celle voulue et perçue par la personne concernée, composée d'une variété de détails externes et hétérogènes et dépendante de l'algorithme de traitement adopté. En revanche, avec les avancées technologiques observées, une biographie numérique représente désormais un dossier plus exhaustif et plus détaillé saisissant non seulement la personnalité, l'identité humaine, mais ayant également une plus grande capacité de contrôle sur la vie de la personne.

Dans la société numérique ainsi mise en place, toute information a une importance, a de la valeur, et peut être traitée, classée, catégorisée mais surtout négociée et entraîne un impact sur la personne ; et l'ensemble de ces informations sont uniformisées dans des dossiers

[1724] S. KARAS, « Privacy, Identity, Databases », American University Law Review, Vol. 52-Issue 2, 2002 (p. 393-445), p. 438-439; disponible en ligne: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1734&context=aulr
[1725] D. CARDON, *À quoi rêvent les algorithmes*, *op. cit.,* p. 49.
[1726] D. SOLOVE, *The Digital Person*, *Ibid.,* p. 45.

individualisés. Ces dossiers étant constamment sollicités et utilisés pour rendre des décisions souvent importantes, les problèmes que les erreurs, les coquilles ou les mauvais calculs peuvent causer ne feront qu'augmenter en fréquence et en ampleur. En effet, un rapport de la Maison Blanche souligne à ce titre que « *the technologies of automated decision-making are opaque and largely inaccessible to the average person. Yet they are assuming increasing importance and being used in contexts related to individuals' access to health, education, employment, credit, and goods and services* »[1727]. Par ailleurs, les anciens députés français indiquaient en ce sens que « *l'informatique repose sur des combinaisons de oui et de non. Elle entraîne une catégorisation des situations et des individus. Elle tend à donner des étiquettes aux individus, à juger les situations sociales. L'informatique affirme la culpabilisation et nie la réinsertion sociale qui a pu être une réalité. Depuis la mise sur fiches, un chèque sans provision poursuivra ainsi un individu pendant toute sa vie. C'est une atteinte à la liberté de se renouveler. Des dossiers scolaires pourraient également suivre les intéressés toute une vie* »[1728].

Selon l'exactitude des dossiers numériques, les vies des personnes ne sont pas seulement révélées et enregistrées mais aussi exploitées, analysées et examinées de sorte que, au nom du développement, du profit, de l'intérêt général ou encore de la sécurité, des enquêtes automatisées sont effectuées sur les personnes « *on a nationwide scale by both the government and the private sector* »[1729]. Cela peut alors produire plusieurs effets et dangers, tels que la discrimination, la mauvaise cotation, l'atteinte à la réputation, la stigmatisation, le fichage en individu dangereux ou en terroriste potentiel et ainsi de suite, chacun porteur de nombreuses conséquences réelles, physiques.

En outre, à un niveau plus abstrait, la mise en place et l'existence des dossiers numériques modifie la nature de la société dans laquelle l'individu vit, se construit et évolue. Le Professeur Miller prévoyait déjà, en 1971, « [the] *possibility of constructing a sophisticated data center capable of generating a comprehensive womb-to-tomb dossier on every individual and transmitting it to a wide range of data users over a national network* », et alertait de cette possibilité en envisageant les dangers potentiels[1730]. L'affaire SAFARI précitée évoquant la « chasse aux français »[1731] avait entraîné des débats et une loi ayant également tenté de prévenir

[1727] Executive Office of the President, White House Report "Big Data: Seizing opportunities, preserving Values", Mai 2014, The White House, Washington, p. 64.
[1728] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*., p. 5786.
[1729] D. SOLOVE, *The Digital Person*, *Ibid.,* p. 47, qui precise « *[…]. Collectively, millions of biographies can be searched, sorted, and analyzed in a matter of seconds.* »
[1730] A. R. MILLER, *The assault on privacy: Computers, Data banks and Dossiers*, Ann Harbor-The University of Michigan Press, 1971, p. 39.
[1731] *Cf.* p. 72, 182 et 320.

contre les dangers de l'informatique. Or, il s'avère que, bien que ces propositions aient été à l'époque interrompues en raison des contestations soulevées, la société de l'information actuelle se dirige et se pérennise, *de facto*, dans un système et une structure de surveillance et de contrôle social où toute personne peut être identifiée, authentifiée, connue intimement, catégorisée, analysée, prédite ; le tout caractérisant, par conséquent, une négociation permanente de l'identité humaine sur plusieurs niveaux et degrés.

Avant les évènements de 2001 ayant facilité l'implémentation de la nouvelle architecture du cyberespace, les dangers liés aux systèmes d'identification et de documentation avaient fait l'objet de nombreuses études et discussions avertissant contre leur recours systématique et les abus que cet usage pouvait engendrer. En effet, *« identity systems and documents have a long history of uses and abuses for social control and discrimination* », l'histoire des systèmes d'identification et des dossiers d'information dénonçant les dangers et les abus qu'une telle pratique peut engendrer : ce fut le cas des esclaves noirs en Amérique, des juifs pendant la période Nazi, de la création des passeports après la Révolution pour contrôler les mouvements et la dissidence, ou du génocide des Tutsis facilité par leur identification[1732].
En plus de faciliter la surveillance et le contrôle des personnes, de tels dossiers peuvent faire des personnes concernées des prisonniers de leurs passés enregistrés, défiant *ipso facto* l'application et le respect du droit à l'oubli nouvellement instauré[1733]. Les dossiers de

[1732] R. SOBEL, "The Degradation of Political Identity under a National Identification System," Boston University Journal of Science and Technology Law, Vol. 8:1, Winter 2002, p. 48 et p. 49-55, l'auteur indique ainsi "*Through the Civil war, slaves were required to carry passes in order to travel outside of plantations. […]. Criminal identification through the use of fingerprints was often to track and control increasingly mobile, diverse populations whose race or ethnicity made them suspect in the eyes of authorities. Fingerprint identification offered a way to individualize ethnic minorities, particularly African and Asian Americans, […]. State bureaucracies also implemented passports in order to control citizens, particularly their right to travel. The passport was first used in post-Revolutionary France, in order to "stymie the assembly of anti-government forces, prevent infiltration by foreign agents, and suppress vagrancy and crime. Other European states soon followed France's lead and began using the passport as a method of "suppressing dissent and controlling crime…" […]. A system of identification cards was used to isolate and round up Jews in Germany and other Nazi-occupied territories prior to World War II and in the occupied countries once the war began. […]. The identification system was a potent weapon at police disposal, allowing them to arrest Jews at will. The system "had a paralyzing effect on its victims … and induced the Jews to be even more docile". The identification system was abetted by the use of punch card technology developed by IBM. […]. in the 1930s, the U.S.S.R. began requiring its citizens to carry internal passports. […]. The passport system was established not only for security purposes, but also to control movement within the U.S.S.R., which served to maintain a class system. […]. For over 30 years from 1958 for men, and from 1963 for women, the South African government required Blacks to carry passes that prohibited them from moving around the country freely. The small green reference books that all black citizens carried regulated where they had the right to travel and settle in the country. […], over a ten-year period, blacks were arrested 637,584 times under the law, while there were no instances of whites arrested under the same law. In Rwanda, a system of identity cards that distinguished Hutus from Tutsis contributed to the killings. […].";* Disponible en ligne: https://www.bu.edu/law/journals-archive/scitech/volume81/sobel.pdf
[1733] *Cf.* p. 213.

renseignements personnels peuvent largement être utilisés par les autorités publiques pour une surveillance inappropriée des individus, les données peuvent aisément et rapidement être exploitées quelle que soit la tâche à accomplir et suivant les intérêts particuliers du moment, et le partage et l'accès auxdites informations est grandement récurrent entre les secteurs publics et privés doublant les dangers et les abus que ces usages peuvent produire, et signifiant l'enjeu fondamental, concret, en cause, celui de la structure de la société. À l'heure actuelle, « *the issue concerns more than isolated threats and harms, but is fundamentally about the structure of our society* »[1734].

Par ailleurs, l'existence ou la création de ces dossiers peut être connue des individus mais l'ampleur de leurs contenus ou la manière dont ils sont utilisés reste, pour la majorité, inconnue. Cette réalité suscite alors un sentiment de malaise, de vulnérabilité ou d'impuissance, et, comme a pu l'annoncer la Cour européenne une « sensation d'être constamment surveillé », voire « *a deepening sense that one is at the mercy of others, or, perhaps even more alarming, at the mercy of a bureaucratic process that is arbitrary, irresponsible, opaque, and indifferent to people's dignity and welfare* »[1735].

Les pratiques et les technologies de surveillance peuvent ainsi être employées comme tactique, stratégie d'intimidation, l'histoire des journalistes publiant des articles relatifs aux services de renseignement, à la sécurité nationale ou encore à l'application de la loi par les forces de l'ordre, représente un des exemples les plus signifiants. Mais cette tactique est également employée à un niveau individuel, induisant une peur chez les personnes non seulement concernant leurs informations ou leurs agissements actuels, mais aussi concernant leurs informations et actions passées. L'ancien président de la République française Nicolas Sarkozy a en 2012, par exemple, ouvertement dit lors d'un discours de campagne que « toute personne qui consulte régulièrement des sites internet faisant la promotion de la terreur, de la haine ou de la violence sera condamné à la prison »[1736], provoquant *de facto* un sentiment commun d'être surveillé de manière générale et indifférenciée, et un besoin commun d'être en conformité.

De manière fondamentale, les entreprises privées, en catégorisant et en classant les informations en vue de promouvoir ou de vendre leurs produits et services sur le fondement de ces catégories, utilisent les données de surveillance pour faire de la discrimination et influencer les comportements. Ainsi, les banques font de la discrimination en traitant les données de leurs

[1734] D. SOLOVE, *The Digital Person*, *Id..,* p. 148.
[1735] D. SOLOVE, *The Digital Person*, *Ibid.,* p. 149.
[1736] B. SCHNEIER, *Data and Goliath*, *op. cit.*, p. 114.

clients afin de déterminer si un prêt peut être accordé, le montant du prêt accordé, la zone ou le quartier autorisé en cas de prêt pour un logement, et ainsi de suite ; c'est l'intégralité du secteur financier qui semble être touché, les prises de décisions relevant de plus en plus, *in fine,* de simples procédures informatiques, computables et programmables. Le Professeur Pasquale indique à ce propos « *Big data enables complex pattern recognition techniques to analyze massive data sets. Algorithmic methods of reducing judgment to a series of steps were supposed to rationalize finance, replacing self-serving or biased intermediaries with sound decision frameworks* », or cela n'a pas été le cas[1737]. De même, les entreprises pratiquent la discrimination par les prix qui consiste à faire payer à des personnes différentes des prix différents pour réaliser autant de profit que possible, l'exemple le plus marquant étant celui des billets d'avions, mais ceci transparaît également dans les prix des menus des restaurants et brasseries proposant les mêmes menus midi et soir, à des prix différents toutefois. Plus généralement, « *Big data technologies will be transformative in every sphere of life. The knowledge discovery they make possible raises considerable questions about how our framework for privacy protection applies in a big data ecosystem. Big data also raises other concerns. [...] big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace* »[1738].

Ces méthodes et pratiques s'observent, désormais, facilement en ligne où chaque internaute est confronté à des publicités différentes, personnalisées, des suggestions ou recommandations ciblées et personnalisées, ou encore des services particuliers ou un flux d'information donné, le tout en fonction de son "code de consommateur", qui ressemble dans ce contexte à une côte de crédit, déterminé grâce à son dossier numérique accédé *via* les courtiers en données généralement. Il semble bien que, « *in many industries, the options you're offered, the price you pay, and the service you receive depend on information about you: bank loans, auto insurance, credit cards, and so on. Internet surveillance facilitates a fine-tuning of this practice* »[1739].

[1737] F. PASQUALE, *The Black Box society, Id.*, p. 15, et l'auteur affirme ainsi: "*The black boxes of finance replaced familiar old problems with a triple whammy of technical complexity, real secrecy, and trade secret laws. [...]"*

[1738] Executive Office of the President, White House Report "Big Data: Seizing opportunities, preserving Values", *Id.*, p. III; Cité également par B. SCHNEIER, *Data and Goliath*, *Id.*, p. 128-129 et l'auteur rajoute "*I think the report understated the risk*"; et F. PASQUALE, *The Black Box society, Ibid.*, p. 38 et l'auteur indique "*Already disadvantaged groups may be particularly hard hit.*"

[1739] B. SCHNEIER, *Data and Goliath*, *Id.*, p. 129.

Ces risques et dangers ne se limitent pas au secteur privé, marchand, ils comprennent de même les discriminations, catégorisations, fichages, stigmatisations ou incarcérations effectués par les gouvernements, ainsi qu'il a pu être précédemment observé. Les dossiers numériques existants dans cette nouvelle architecture du cyberespace paraissent, dans ce contexte, comporter l'intégralité de nos biographies, y compris nos personnalités, nos goûts, nos préférences, nos comportements, nos opinions, fondamentalement, nos identités. Selon le Professeur Pasquale, « *in his book Turing's Cathedral, George Dyson quipped that "Facebook defines who we are, Amazon defines what we want, and Google defines what we think." We can extend that epigram to include finance, which defines what we have (materially, at least), and reputation, which increasingly defines our opportunities. Leaders in each sector aspire to make these decisions without regulation, appeal, or explanation. If they succeed, our fundamental freedoms and opportunities will be outsourced to systems with few discernible values beyond the enrichment of top managers and shareholders* »[1740].

L'enjeu ne concerne plus seulement les atteintes individuelles à la réputation, à la notoriété ou au respect de la vie privée, ni même la divulgation d'informations nominatives ; avec les développements récents des technologies et des pratiques déployées, l'enjeu touche dorénavant la structure et le type d'environnement, de société dans laquelle les individus vivent et évoluent. Par conséquent, interroge Solove, « *do we want to live in a Kafkaesque world where dossiers about individuals circulate in an elaborate underworld of public- and private-sector bureaucracies without the individual having notice, knowledge, or the ability to monitor or control the ways the information is used?* »[1741]. Et ce, sans oublier les pouvoirs de contrôle et de manipulation que confère le pouvoir de surveillance : « *someone who knows things about us has some measure of control over us, and someone who knows everything about us has a lot of control over us. Surveillance facilitates control* »[1742].

Dans cette perspective, il semble alors que c'est la réussite et la concrétisation, à l'époque de la révolution numérique, du phénomène de « propagande » introduit en 1929 par E. Bernays, pionnier de l'industrie des relations publiques. Selon cet auteur, l'Homme est gouverné par un tout petit nombre d'individus, une fraction insignifiante, pour la plupart inconnus du public, conséquence logique de la structure et de l'organisation des sociétés démocratiques modernes,

[1740] F. PASQUALE, *The Black Box society, Ibid.*, p. 15.
[1741] D. SOLOVE, *The Digital Person*, *Id.,* p. 149.
[1742] B. SCHNEIER, *Data and Goliath*, *Ibid.*, p. 133.

qu'il faut accepter et coopérer avec, pour vivre dans une société humaine fonctionnant efficacement et correctement.

Selon Bernays, « *the conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country. We are governed, our minds are molded, our tastes formed, our ideas suggested, largely by men we have never heard of. […].*

Whatever attitude one chooses to take toward this condition, it remains a fact that in almost every act of our daily lives, whether in the sphere of politics or business, in our social conduct or our ethical thinking, we are dominated by the relatively small number of persons – a trifling fraction […]– who understand the mental processes and social patterns of the masses. It is they who pull the wires which control the public mind, who harness old social forces and contrive new ways to bind and guide the world. […]. There is consequently a vast and continuous effort going on to capture our minds in the interest of some policy or commodity or idea. »[1743] ; un effort vaste et continu qui se traduit, de manière concrète, par une lutte d'influence en vue d'accumuler et de détenir toujours plus d'informations personnelles.

[1743] E. BERNAYS, *Propaganda*, Introduction by Mark Crispin Miller, Ig Publishing, New York, 2005 (publication parue initialement en 1928), p. 37-38 ; N. Chomsky, en commentant son livre, indique « *[…]. The propaganda system of the first World War and this commission that he was part of showed, he says, it is possible to "regiment the public mind every bit as much as an army regiments their bodies."* ***These new techniques of regimentation of minds, he said, had to be used by the intelligent minorities in order to make sure that the slobs stay on the right course. We can do it now because we have these new techniques*** »: N. CHOMSKY, "What Makes Mainstream Media Mainstream", Z Magazine, Octobre 1997: https://chomsky.info/199710__/

Chapitre II. Le traitement des données personnelles : Une lutte d'influences

« *Surveillance capitalists […] dressed in the fashions of advocacy and emancipation, appealing to and exploiting contemporary anxieties, while the real action was hidden offstage. […]. They were protected by the inherent illegibility of the automated processes that they rule, the ignorance that these processes breed, and the sense of inevitability that they foster. […].*
Surveillance capitalism operates through unprecedented asymmetries in knowledge and the power that accrues to knowledge. »[1744]

Le traitement, visant l' « *action de résoudre une question par des opérations de l'esprit et de façon méthodique;* [l']*ensemble des moyens matériels et opérations matérielles et logiques correspondantes* »[1745], désigne, en matière informatique, le traitement des données. Celui-ci, dans ce cadre, se réfère particulièrement aux « traitements automatiques des données », à savoir l' « *ensemble des opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et d'une façon générale leur exploitation* »[1746], se rapportant, alors, à la science de l'information – objet principal de la lutte actuelle qui transparaît.

Une lutte, qui s'entend comme un « *affrontement entre des forces rivales* »[1747], distinctes, indique une « opposition vive, un conflit entre deux personnes ou deux groupes de personnes cherchant à faire triompher leurs intérêts, leur cause, à imposer leur volonté, leur suprématie »[1748], supposant donc l'action de « *se mesurer,* [d']*entrer en compétition ([…] dans un domaine quelconque) pour chercher à emporter l'avantage* »[1749]. Plus particulièrement, dans le domaine de l'économie et de la santé notamment, une lutte correspond à l' « *action organisée en vue de venir à bout de certains fléaux par l'emploi de méthodes appropriées* »[1750], facilitée de nos jours par la masse de données disponible et conservée pouvant être rapidement exploitée pour en tirer de nombreux profits et avantages, y compris des jugements, analyses et prédictions, voire des études comportementales, des profils et dossiers numériques. Néanmoins,

---

[1744] S. ZUBOFF, *The Age of Surveillance Capitalism*, *op. cit*. p. 10-11, la Professeure precise à ce titre « *Theirs was an invisibility cloak woven in equal measure to the rhetoric of the empowering web, the ability to move swiftly, the confidence of vast revenue streams, and the wild, undefended nature of the territory they would conquer and claim.* » (p.10)
[1745] CNRTL, « Traitement » : *op. cit.*
[1746] CNRTL, « Traitement » : *Id.*
[1747] Dictionnaire de l'Académie Française, 9ème Ed., « Lutte » : https://www.dictionnaire-academie.fr/article/A9L1399
[1748] CNRTL, « Lutte » : https://www.cnrtl.fr/definition/lutte
[1749] CNRTL, « Lutter » : https://www.cnrtl.fr/definition/lutte
[1750] CNRTL, « Lutte » : *Id.*

« *la conservation massive et systématique des données relatives à chaque personne tend aussi à juger les situations en attachant aux individus des étiquettes jadis plus rares et plus approximatives, et dont il leur était plus facile de se débarrasser* »[1751].

Mais à l'ère de la société de l'information, il semble qu'une lutte d'influence s'est déclarée entre des secteurs et des entités publics et privés, afin de détenir toujours plus d'informations et de valeurs extraites de leurs traitements et exploitations, aboutissant ainsi à la nécessité de recourir à des stratégies et pratiques pluridisciplinaires. Ceci entraîne un changement radical dans les approches et les techniques de gestion, d'administration, de surveillance, de science économique ou sociale, liées, fondamentalement, aux nouveaux outils informatiques et numériques, ainsi qu'au développement des capacités de calcul et d'analyse désormais disponibles permettant de traiter rapidement, de manière quantitative et qualitative, la masse de données récoltées et conservées. Or, « *le recours à ces techniques, fondées sur la logique formelle et sur les mathématiques, renforce en effet une tendance de notre civilisation à la catégorisation des situations et des individus* »[1752].

De quelle manière le traitement des données personnelles représente-t-il une lutte d'influence ? Quels sont *in concreto* les logiques et les stratégies guidant les opérations de traitement de données et suscitant la rivalité et la chasse aux données, et aux profits en découlant, qui s'observent au XXI^{e} Siècle ?

Le but de ces développements est ainsi de montrer que le traitement des données représente une lutte d'influences diverses, initiée par l'ère de la révolution numérique, qui se traduit par une lutte silencieuse et discrète pour une gouvernance numérique, particulièrement des données et, par extension, des identités (Section I), ainsi que par une chasse au profit des capacités et des applications du Big data (Section II); caractérisant, *ergo*, la compétition entourant désormais les données à caractère personnel et leurs traitements compte tenu de leur valeur et de leur valorisation.

[1751] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*., p. 5782.
[1752] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *Id*., p. 5782.

Section 1 – La lutte silencieuse pour une gouvernance (des identités) numérique

L'environnement numérique actuellement mis en œuvre offre la possibilité de recourir, finement et massivement, à des logiques techniques et économiques (§1) ainsi qu'à des stratégies publiques et privées, développées *ab initio* séparément, (§2) qui s'avèrent être respectivement disruptives traduisant la lutte silencieuse qui s'installe en vue d'une gouvernance pérenne du numérique et de ses objets, donc, *in fine*, des identités numériques et des individus les employant quotidiennement.

§1. Des logiques économiques et techniques de rupture

Ce sont des logiques qui rompent avec l'usage, avec ce qui a été connu et vécu jusqu'à présent, à travers la manifestation et l'essor, d'une part, du pouvoir du calcul et des nombres (A) et, d'autre part, du pouvoir des données et de la quantification (B) ; des pouvoirs étayant, par conséquent, les logiques dites de rupture.

A. Le pouvoir du calcul et des nombres

La statistique descriptive allemande ainsi que l'arithmétique politique, anciennement développées et utilisées pour des recensements et des dénombrements[1753], ont, combinées, souligné dans l'environnement numérique actuel l'importance ainsi que le pouvoir du calcul et des nombres.

Que ce soit dans le domaine de la science, de la recherche, de la politique ou du commerce, avoir les bons chiffres et les bonnes statistiques, c'est faire preuve de compétence et de connaissance concrètes et approfondies. Il est d'adage courant que les chiffres et les nombres ne mentent pas, deux ne pouvant faire quatre par exemple, ils seraient alors transparents, objectifs et réels évoquant le raisonnement du vrai-faux appuyé par une représentation, une démonstration, par les nombres. En effet, compte tenu des calculs et des statistiques effectués et avancés, une représentation par les nombres constitue un appui et un soutien aux idées et aux théories initiées ou débattues, acquérant une sorte de statut de preuve en raison même du concept selon lequel les chiffres sont vrais et ne mentent pas, tout en apportant un visuel souvent nécessaire à l'homme et son raisonnement puisque « *bodies exist in spaces that are concrete and particular ; vision is general and abstract, linked metaphorically with the transcendent power of reason. […]. Within Western culture, vision is linked metaphorically with both*

[1753] *Cf.* p. 149-153.

knowledge and power »[1754]. Les nombres répondent donc par une vérité certaine et irréfutable, or, pour être efficace en termes de démonstration et de représentation de cette vérité poursuivie, ils doivent également tenir compte du système complexe des discours et formulations portés par la subjectivité et la volonté d'une personne, mais aussi du système complexe de réception des destinataires de la vérité en question.

L'arithmétique politique appréhende ces trois variables : les nombres, le réel et la subjectivité (le moi). Selon Diderot, comme il a été susmentionné, l'arithmétique politique est « *celle dont les opérations ont pour but des recherches utiles à l'art de gouverner le peuple* », des opérations « *telles que celles du nombre des hommes qui habitent un pays ; de la quantité de nourriture qu'ils doivent consommer ; du travail qu'ils peuvent faire ; du temps qu'ils ont à vivre ; de la fertilité des terres ; de la fréquence des naufrages, etc.* »[1755]. L'alliance entre politique et arithmétique transparaît dans cette définition appuyée par celle de Robinet qui explique que « *l'arithmétique politique est l'application de l'arithmétique et de ses opérations à des objets qui tiennent à l'administration publique* » [1756]. C'est donc « *l'art de raisonner, par le moyen des chiffres et du calcul, sur des objets qui tiennent à l'administration publique* » et ces objets sont nommément « la population, les subsides, les opérations de finance, l'armée et la marine »[1757].

Selon ces objets, Robinet partage en quatre classes « *les fondements du calcul politique* »[1758] : la liste des naissances et des morts, les dénombrements, les capitations et impôts personnels, les besoins ou dépenses de l'État, sans oublier les contributions extraordinaires, telles que les productions territoriales, l'industrie, le commerce etc., le nombre des troupes de terre et de mer[1759]. La liste de tout ce qui peut être compté est donc longue comprenant le calcul de ce qui existe mais aussi de ce qui pourrait ou devrait exister, en faisant des prédictions sur ce qui est possible comme « la quantité de nourriture que [les hommes] doivent consommer ; le travail

---

[1754] J. E. COHEN, *Configuring the Networked self*, *op. cit.,* p. 124.

[1755] D. DIDEROT, « Arithmétique Politique », article de *l'Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers, par une société de gens de lettres*, *op. cit.,* p. 678.

[1756] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, Tome premier[-trentième], À Londres, Chez les libraires associés. M.DCC.LXXVII [-M.DCC.LXXXIII], 1777-1778, reproduit par Gallica-Bnf, p. 127 où l'auteur réitère les mêmes exemples d'opérations cités par Diderot ; disponible en ligne : https://gallica.bnf.fr/ark:/12148/bpt6k940850/f139.image

[1757] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Id.,* p. 154 et pour la description détaillée des objets : p. 154 à 157.

[1758] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Id.,* p. 157.

[1759] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Ibid.,* p. 157-161.

qu'ils peuvent faire ; le temps qu'ils ont à vivre », pour reprendre les exemples de Diderot. Le but final des opérations entreprises par les calculateurs politiques, les arithméticiens politiques, n'est donc pas celui des statistiques ou des dénombrements et dépouillements, mais plutôt celui de réaliser des calculs à partir des données dont ils disposent leur permettant d'aboutir à des généralisations ; or, les calculs partent toujours d'une hypothèse.

L'arithmétique politique aspire à être objective, acquise « *par des calculs fondés sur quelques expériences bien constatées* »[1760], suivant une méthode scientifique, mathématique, se basant sur les nombres, les poids et les mesures qui permettent de dresser une image empirique de la réalité de la situation, exempte par conséquent de subjectivité, en tenant à l'écart les idées, opinions, passions ou désirs changeants des personnes. Néanmoins, « *on serait trop heureux si tous les différents calculs politiques, […], pouvaient se faire avec une précision parfaite ; mais il s'en faut de beaucoup qu'ils soient susceptibles d'une certitude mathématique* »[1761]. La portée de l'arithmétique politique doit alors être nuancée en raison même de l'aspect politique qu'elle comporte, l'alliance entre arithmétique et politique étant, selon Diderot, difficile à assurer compte tenu, d'une part, de la lenteur de la méthode arithmétique à cette époque qui réclamait le besoin de « *passer par des combinaisons et des suites d'opérations arithmétiques, […] une marche si lente et si pénible* » alors que les gouvernements, s'imaginant « *doués d'un grand génie naturel* » s'en dispensaient pour atteindre leurs buts plus rapidement, et, d'autre part, c'est surtout « *sans compter que la nature des affaires ne permet ni ne demande presque jamais la précision géométrique* »[1762]. Ces deux notions semblent, dans ce contexte, porter une contradiction, une sorte d'oxymore, suggérée également par Robinet qui précise que « *la politique n'a pas besoin d'une certitude mathématique. Elle peut se contenter très bien d'une théorie vraisemblable sur tous ces objets, pourvu que cette théorie soit aussi approchante de la vérité qu'il est possible ; et c'est à quoi tendent tous les efforts des calculateurs politiques qui devraient être fécondés, dans les pays bien policés, par le Gouvernement même. […]. L'arithmétique politique a cela d'avantageux pour l'homme d'État, que ses opérations le*

[1760] D. DIDEROT, « Arithmétique Politique », *Id.,* p. 678.

[1761] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Ibid.,* p. 162.

[1762] D. DIDEROT, « Arithmétique Politique », *Ibid.,* p. 678-679 : « […]. *On conçoit aisément que ces découvertes et beaucoup d'autres de la même nature, étant acquises par des calculs fondés sur quelques expériences bien constatées, un ministre habile en tirerait une foule de conséquences pour la perfection de l'agriculture, pour le commerce tant intérieur qu'extérieur, pour les colonies, pour le cours et l'emploi de l'argent, etc. Mais souvent les ministres (je n'ai garde de parler sans exception) croient n'avoir pas besoin de passer par des combinaisons et des suites d'opérations arithmétiques : plusieurs s'imaginent être doués d'un grand génie naturel, qui les dispense d'une marche si lente et si pénible, sans compter que la nature des affaires ne permet ni ne demande presque jamais la précision géométrique.* »

conduisent à des principes vrais qui servent de base aux arrangements qu'il fait pour toutes sortes d'objets ; mais il n'a pas besoin de s'engager toujours dans les détails du calcul même [...] »[1763].

Un autre aspect affaiblissant la portée de l'arithmétique politique a également été avancé par ces auteurs qui sous-tendent que les chiffres et les nombres n'ont aucune valeur prédictive puisqu'il ne faut pas « *oublier qu'il arrive des révolutions, soit en bien, soit en mal, qui changent en un moment la face des États, et qui modifient et même anéantissent les suppositions ; et que les calculs et leurs résultats ne sont pas moins variables que les événements* »[1764]. En effet, à l'époque du développement de cette méthode scientifique, les données qui servaient de base aux calculs étaient peu disponibles et peu fiables, dépendant entièrement du travail humain, ce qui pouvait entraîner des calculs faux et, conséquemment, des théories ou conclusions fausses. Les principes guidant une telle méthode peuvent souvent être mal pensés, mal fondés ou arbitraires de sorte qu'ils ne peuvent qu'aboutir à des résultats erronés, comme ce fut le cas avec l'ouvrage « Essai de politique et de morale calculée » paru en 1752 qui eut l'idée de « *réduire une science au calcul et de prouver tous ses principes par des démonstrations mathématiques* »[1765] ; ouvrage vivement critiqué par Robinet. Celui-ci démontre que les mathématiques, qu'il qualifie d' « êtres de raison », seules ne peuvent s'appliquer aux choses et aux objets de la nature, de manière proportionnelle, alors que ceux-ci ne suivent pas un ordre mathématique ; il faudrait prendre en compte plus de paramètres et d'éléments, fondés sur la réalité des faits et les expériences vécues[1766]. Robinet soulève ainsi la dangerosité d'une telle méthode de raisonner qui est « *d'autant plus spécieuse qu'on la croit fondée sur un calcul infaillible* » où le recours à l'arithmétique semble garantir la vérité irréfutable du résultat[1767].

L'aspect du destinataire d'une étude arithmétique ou encore la volonté de l'émetteur de l'étude ne peuvent donc être mis de côté, d'autant qu'influencer un destinataire ou appliquer sa propre

---

[1763] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Id.,* p. 167.
[1764] D. DIDEROT, « Arithmétique Politique », *Id.,* p. 679.
[1765] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Id.,* p. 147.
[1766] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Ibid.,* p. 148 : « *[...]. Avec des suppositions destituées de tout fondement on peut prouver les propositions les plus fausses, et résoudre les plus grands paradoxes. Comment peut-on supposer qu'il se trouve dans le monde deux terres qui rapportent tout ce qu'elles peuvent rapporter ? De telles terres sont des êtres de raison. Comment peut-on supposer encore que le nombre de personnes qui composent chaque famille puisse augmenter continuellement ! Tout cela est contraire à l'ordre établi dans la nature.* »
[1767] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Ibidem,* p. 148.

volonté, l'intérêt particulier souhaité, est susceptible de l'emporter sur « *l'amour de la vérité* »[1768], l'auteur de l'étude arithmétique étant souvent plus attaché à parler le langage voulu que celui de la vérité. En effet, disait J. Duhamel, lors d'un débat parlementaire sur la loi de finances, « si *les chiffres ne mentent pas, les menteurs eux chiffrent* »[1769].

L'arithmétique politique, depuis ses balbutiements et ses premiers tâtonnements, s'appuie principalement sur le sémantisme des « poids, nombres et mesures » pour garantir l'objectivité de son analyse et la vérité de ses résultats et conclusions. Or, la combinaison entre la précision et l'objectivité de l'arithmétique et le domaine politique était, jusqu'à récemment, difficile voire irréalisable, menant plutôt au « vraisemblable » et non à la précision, invoquant par conséquent, selon les auteurs précités, les notions de « Hasard », « Jeu », « Probabilité », « Combinaison », « Vie », « Mort », « Naissance », « Annuité », « Rente », ou « Tontine », par exemple[1770]. Cependant, note Diderot, « *si la nature des affaires la demandait et la permettait, je ne doute point qu'on ne parvînt à se convaincre que le monde politique, aussi bien que le monde physique, peut se régler à beaucoup d'égards par poids, nombre et mesure* »[1771]. Les critiques et la formulation de l'auteur mènent à un constat selon lequel à partir du moment où les nombres et le calcul entrent dans une argumentation, une représentation, ou une démonstration à finalité particulière, ils ne portent plus de « précision géométrique » mais se transforment en manipulateurs et en objets de manipulation, soulignant par conséquent le succès de l'arithmétique politique et ses méthodes de raisonnement à l'ère du Big data et de l'architecture actuelle du cyberespace où les données sont disponibles en masse et les pratiques computationnelles intrusives facilitent la précision de l'évaluation et du traitement des données. Au XXI[e] Siècle, elle implique dans cette perspective l'essor de la « gouvernance par les nombres » qui n'est pas un accident de l'histoire : « *la recherche des principes ultimes qui*

[1768] J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Ibid.,* p. 131.

[1769] Citation célèbre de Jacques Duhamel (1924-1977), Ministre des affaires culturelles françaises de janvier 1971 à avril 1973, prononcée lors des débats parlementaires sur la Loi de finances pour 1967, séance du 13 octobre 1966, JO Année 1966-1967 – N° 79 A.N. du 14 octobre 1966, p. 3381 : sa formulation exacte étant « *si les menteurs chiffrent, les chiffres, eux, ne mentent pas* » ; disponible en ligne : http://archives.assemblee-nationale.fr/2/cri/1966-1967-ordinaire1/012.pdf

[1770] D. DIDEROT, « Arithmétique Politique », *Ibid.,* p. 680 ; et, J.-B.-R. ROBINET, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, *Ibid.,* p. 162 « *[…]. L'inconvénient est que, dans les dates sur lesquelles se fondent ces calculs, on est obligé toujours de substituer l'apparent ou le vraisemblable au vrai et d'admettre pour fondement des extraits baptistaires ou mortuaires, des dénombrements, des registres de douane, et autres pièces pareilles qui ont été faites par des hommes, ou trop pressés dans leurs opérations, ou trop négligents, ou trop ineptes, ou trop intéressés à déguiser la vérité à leurs Souverains, pour s'insinuer, en présentant sous un aspect favorable les objets qui sont sous leur direction.* »

[1771] D. DIDEROT, « Arithmétique Politique », *Ibidem,* p. 678.

président à l'ordre du monde combine depuis longtemps la loi et le nombre au travers de la physique et des mathématiques, s'agissant de l'ordre de la nature ; et du droit et de l'économie s'agissant de l'ordre social »[1772]. C'est l'art de gouverner par les nombres et le calcul, un pouvoir qui jusqu'au développement du web et du Big data était considéré comme irréalisable et inatteignable. Mais les attentes à l'égard des nombres n'ont cessé de s'étendre passant de simples « *objets de contemplations* » à des « *moyens de connaissance* » puis à des « *moyens de prévision* », instaurant une croyance illusoire en un monde entièrement régulé par les nombres, et suscitant la sensation qu' « *aujourd'hui comme hier, les mathématiques seraient la clé d'intelligibilité – et donc de la maîtrise – du monde* »[1773].

Au cours des développements de la statistique et de l'arithmétique politique, et avant l'arrivée du XXI^e^ Siècle et des avancées technologiques et algorithmiques, les données disponibles étaient quantitativement limitées, les méthodes et techniques de recensements étaient surtout opérées par des agents humains, les données ne portaient jamais sur l'ensemble de la population, méconnaissant volontairement les comportements minoritaires au profit de ceux plus fréquents. Désormais, « *plus question d'éviter les points de données trop écartées de la moyenne, le big data prend tout en compte, indistinctement* »[1774]. Contrairement aux méthodes et aux moyens statistiques et de raisonnement arithmétique traditionnels, la gouvernance par les nombres, aidée par l'architecture du cyberespace telle que mise en place, repère et décèle tout ce qui était jadis, inaperçu, non observable, non calculable, non quantifiable.

Toute donnée, toute expérience, tout comportement peut être dorénavant calculé et chiffré, ce qui fut observé notamment par le passage d'un marketing de masse, présentant des solutions uniformisées, à un marketing personnalisé présentant des recommandations et suggestions individualisées. Pour ce faire, il s'agit de recourir aux techniques de *data mining,* devenues automatiques pour extraire de la connaissance, à la recherche de corrélations, d'associations, de répétitions, de modèles de comportements, etc. ; ces informations étant par la suite agrégées et homogénéisées pour constituer des dossiers individualisés[1775], et peuvent également servir aux outils et techniques de *data visualization*, dit aussi *dataviz*, représentant un puissant outil de communication permettant de mieux visualiser les données pour mieux piloter et mieux éclairer les décisions[1776]. La gouvernance par les nombres promet ainsi de réguler le monde et

[1772] A. SUPIOT, *La gouvernance par les nombres, op. cit.,* p. 103.
[1773] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 104-105.
[1774] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, op. cit.,* p. 60.
[1775] *Cf.* p. 390.
[1776] Le Big Data – Le Magazine I.A., Cloud et Big data, « Le Dataviz, Qu'est-ce que c'est ? – Définition, outils essentiels », publié le 26 octobre 2017 : « *La dataviz, ou la visualisation de données, est une pratique que l'on côtoie au quotidien sans se rendre compte, ne serait-ce qu'en ouvrant un journal ou en regardant la télévision.*

la société en représentant les faits et la réalité tels qu'ils se présentent, de manière empirique et arithmétique : « *plus besoin de science, plus besoin de théorie, la vérité numérique serait déjà là* »[1777], d'autant que « *la gouvernance par les nombres n'emporte pas du reste la disparition des lois, mais la soumission de leur contenu à un calcul d'utilité, en sorte qu'elles servent les « harmonies économiques » qui présideraient au fonctionnement des sociétés humaines* »[1778]. Une nouvelle sorte de savoir véridique et irréfutable semble ainsi s'être mis en œuvre au profit des autorités publiques et des entreprises privées grâce à l'exploitation, d'une part, de l'arithmétique politique, des statistiques et du pouvoir des calculs et des nombres, et, d'autre part, de larges quantités et volumes de données désormais massivement disponibles et accessibles, « *reflétant le monde jusque dans ses moindres évènements sous une forme éclatée, segmentée, distribuée, décontextualisée, déhistoricisée* », qui ont la caractéristique d'être des « données a-signifiantes mais quantifiables »[1779], marquant, *in fine*, l'avènement d'un art de raisonner et de gouverner innovant, ainsi que l'essor du « fétichisme de la donnée à caractère personnel »[1780].

B. Le pouvoir des données et de la quantification

Un renversement du pouvoir des données s'observe alors avec les pratiques et les pouvoirs émergents, introduisant le monde de la « vérité numérique », qui est une prise de pouvoir numérique, informatique, et particulièrement opaque, caractérisant une « subversion des normes existantes » et un bouleversement du rôle des données : « *c'est un véritable « coup*

L'exemple le plus simple reste le sondage. Avec l'ère numérique, elle est devenue un puissant outil de communication. Dans une société de plus en plus attirée par l'aspect graphique, la visualisation de données prime sur la donnée brute. Elle aide à éclairer des informations en apparence complexes ou noyées dans une grande quantité de paramètres. Le terme dataviz désigne donc l'ensemble des représentations visuelles de ces données brutes. » : https://www.lebigdata.fr/dataviz-qu-est-ce-que-c-est ; l'ISM propose des formations courtes « Datavisualisation: visualiser ses données pour mieux piloter » : « *Transformer vos restitutions de données : La prise de décision est facilitée lorsque l'on s'appuie sur une représentation synthétique et visuelle des données. Cette formation vous apporte une méthode pour présenter vos données sous une forme lisible et impactante.* » : https://www.ism.fr/formation/datavisualisation-visualiser-ses-donnees-pour-mieux-piloter ; l'entreprise SAS propose des outils et techniques de data vizualisation et explique que « *Because of the way the human brain processes information, using charts or graphs to visualize large amounts of complex data is easier than poring over spreadsheets or reports. Data visualization is a quick, easy way to convey concepts in a universal manner – and you can experiment with different scenarios by making slight adjustments.*
Data visualization can also: Identify areas that need attention or improvement; Clarify which factors influence customer behavior; Help you understand which products to place where; Predict sales volumes.» : https://www.sas.com/en_us/insights/big-data/data-visualization.html

[1777] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, Id.,* p. 59.

[1778] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 103.

[1779] A. ROUVROY, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des big data », *In* Conseil d'État - Étude annuelle 2014, *Le numérique et les droits fondamentaux, op. cit.,* p. 407.

[1780] A. ROUVROY, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des big data », *Id.,* p. 407.

data » sur la gouvernance du monde »[1781]. Le traitement et l'analyse des données en masse, disponibles abondamment dans le quotidien de la société du XXI[e] Siècle, permettant désormais de prédire et d'anticiper les comportements humains et élaborant des dossiers numériques unifiés individuels, soulignent l'importance croissante accordée aux données et traduit leur pouvoir sans cesse grandissant. Cette vérité numérique que porte le pouvoir des données introduit également le pouvoir de la quantification où toute expérience vécue, tout comportement effectué, toute opinion exprimée ou recherche effectuée, peut être quantifié, chiffré, mesuré et évalué, formant une donnée interprétable, analysable et utilisable.

Désormais, tout peut devenir une donnée, c'est bien la « datafication »[1782] même d'éléments ou de paramètres qui peuvent paraître exagérés ou farfelus produisant une masse d'information utilisables et réutilisables. À cet égard, IBM a révolutionné le rôle et les capacités des capteurs et obtint en 2012 un brevet portant sur des systèmes transformant les sols et planchers en surfaces "intelligentes" multi-tactiles intitulé « *securing premises using surface-based computing technology* »[1783]. Ce système permet donc d'identifier tous les objets se trouvant sur le sol, et sous forme basique, d'ouvrir les portes quand une personne entre dans l'établissement équipé de cette technologie et d'allumer ou éteindre les lumières en fonction. Ce système a également les capacités d'identifier les individus par leur poids ou par leur manière de se tenir et de marcher, repérant par conséquent les anomalies, les personnes s'introduisant dans les lieux frauduleusement, accroissant *de facto* la sécurité de l'établissement en question, objectif souvent recherché par les secteurs publics comme privés. Cette technologie peut aussi être très utile pour les commerçants, leur servant à analyser le flux de trafic ayant lieu dans leurs magasins par exemple. Elle sert aussi au secteur médical, puisqu'en déterminant qu'un individu est tombé au sol chez lui, par exemple, en se basant sur l'empreinte du poids et de la

---

[1781] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, Ibid.,* p. 20.

[1782] *Cf.* p. 144.

[1783] Patent nº 8138882, "Securing premises using surfaced-based computing technology", Patents Google: https://patents.google.com/patent/US8138882B2/en#patentCitations; JUSTIA Patents, Patents n° 7983452, "Using a surface based computing device for verification of an identification document", Date of Patent: July 19, 2011, Abstract: "*The current invention discloses a solution for using a surface based computing device for verification of an identification document, such as a driver's license. A surface-based computing device can be a device capable of scanning an identification document, comparing the scanned document against a set of conditions for a valid document, and reporting comparison results. A secured resource can be granted based at least in part upon identity verifications conducted by the surface-based computing device. The surface-based computing device can include a MICROSOFT SURFACE device or any other computing device able to scan an identification document and to process scanned results. In one embodiment, the surface based computing device can be used in conjunction with a human agent for added security*.": https://patents.justia.com/inventor/kathryn-j-lemanski ; M. C. O'CONNOR, "IBM patent sees sensors as high-tech floor boards", ZDNet, publié le 23 avril 2012: https://www.zdnet.com/article/ibm-patent-sees-sensors-as-high-tech-floor-boards/ ; Relative Home Systems, "Future Automation of Multi-Touch Floor From IBM", publié le 10 avril 2012: https://www.relativehomesystems.com/blog/item/future-automation-of-multi-touch-floor-from-ibm

configuration de la personne, le système pourrait accéder à ses signes vitaux et appeler automatiquement une aide médicale ; ce qui s'avère être également utile et attrayant pour les personnes âgées, ou les familles voulant gagner en indépendance et ainsi de suite. Les utilisations potentielles de ce système sont abondantes et le tout génère des données ; *in fine*, « *when the floor is datafied, there is no ceiling to its possible uses* »[1784].

Dans l'architecture actuelle du cyberespace, il est possible de tout transformer en données, affectant les analyses, les statistiques, les calculs, les perceptions, les structures, où la « norme devient l'énorme » invitant le développement de nouvelles techniques, méthodes et pratiques pour gérer la masse de quantité et de volume de données et « l'infobésité »[1785], la surcharge informationnelle disponible. En effet, « *le règne de la statistique n'a pas été imposé à des pauvres sociétés qui n'en pouvaient, mais il a été appelé par l'état de ces sociétés. […]. Lorsque la démesure et la disproportion s'installent partout, de la taille des villes, des entités politiques, aux quantités d'énergie en circulation, au maillage technique, à l'intensité des échanges et de la consommation, lorsque la norme devient l'énorme, lorsque nos capacités d'émotion, d'évaluation et de représentation, prises de court par le gigantesque, ne sont plus à même de nous orienter dans la vie et dans la pensée, la seule ressource pour conserver un semblant de maîtrise est de nous en remettre aux nombres […]* »[1786].

C'est le cas du mouvement du « quantified self » précité[1787] et les technologies développées y afférentes qui sont des systèmes permettant aux individus d'effectuer une quantification et une mesure de soi pour de multiples objectifs aussi divers que variés, qu'ils soient sportifs, médicaux, nutritionnels, génétiques, de productivité ou de performance. Autrement dit, l'essor du mouvement du « quantified self » « *refers to a disparate group of fitness aficionados, medical maniacs, and tech junkies who measure every element of their bodies and lives in order to live better – or at least, to learn new things they couldn't have known in an enumerated way before* »[1788]. C'est le pouvoir de la mesure et de la quantification qui accompagne fidèlement le pouvoir des données poursuivant, ensemble, des finalités innombrables et illimitées. Il s'avère

---

[1784] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *op. cit.,* p. 94.

[1785] A. VULBEAU, « Contrepoint - L'infobésité et les risques de la surinformation », *Informations sociales*, Vol. 191, N° 5, 2015 (p. 35-35), p. 35 : « *Le terme d'« infobésité » est un mot-valise qui associe l'information et l'obésité. Cette analogie avec une maladie due à un fort surpoids désigne les effets pathologiques de la surconsommation d'informations. Selon des enquêtes menées auprès de managers, près des trois quarts souffrent de surinformation et du sentiment d'être pris dans une urgence généralisée et presque tous pensent que cette situation ne peut qu'empirer. Le sentiment de surcharge vient du fait que l'information s'ajoute à la production et que la part communicationnelle du travail ne cesse de croître* » ; Mis en ligne sur Cairn.info le 20/06/2016 : https://www.cairn.info/revue-informations-sociales-2015-5-page-35.htm

[1786] O. REY, *Quand le monde se fait nombre*, *op. cit*., p. 297.

[1787] *Cf.* p. 159-162.

[1788] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Id.,* p. 94-95.

ainsi que *« toute quantification est une construction qui installe un dispositif de commensuration des enregistrements et établit des conventions pour les interpréter »*[1789]. À l'heure actuelle, compte tenu des avancées technologiques, des développements des techniques et pratiques computationnelles, de la réduction des frais liés au stockage, à l'agrégation ou au traitement, de l'efficacité et de l'automaticité des algorithmes de traitement et de la diversification toujours plus étendue des finalités poursuivies, la « datafication », la « donnéification » des actes de la vie, des plus primordiaux aux plus importants ou aux plus bénins, n'a jamais été aussi facile.

À ce titre, une entreprise a créé une des plus grandes bases de données mondiales sur l'activité du sommeil à travers des systèmes de « sleep manager », leur permettant de découvrir, *inter alia*, des différences dans la quantité de sommeil REM[1790], de sommeil paradoxal, vécue par les hommes et les femmes[1791]. Depuis, des objets connectés ou des applications sur les smartphones ont pris le relais permettant aux individus de s'auto-tracer, s'autoévaluer et s'auto-mesurer, même en étant inconscients, tout en alimentant les bases de données de nombreuses entreprises, ce qui semble donc profiter à tout le monde. Des entreprises telles que Fitbit et Jawbone permettent aux personnes de mesurer leur activité physique ainsi que leur sommeil et autres signes vitaux. La montre Fitbit Blaze, développée par l'entreprise du même nom, « *[...] analyse automatiquement une grande variété de statistiques dès lors que vous la portez. Utilisez l'écran Aujourd'hui pour accéder à des statistiques telles que vos pas, votre fréquence cardiaque, la distance parcourue, les calories brûlées et les étages gravis* »[1792]. L'entreprise a par ailleurs perfectionné son modèle et mis au point la montre Fitbit Versa édition spéciale, une montre intelligente « *forme et bien-être qui vous aident à tirer le meilleur de votre vie* », qui analyse automatiquement une plus grande variété d'éléments et effectue des suggestions et des

---

[1789] D. CARDON, *À quoi rêvent les algorithmes*, *op. cit*., p. 56.

[1790] « Le sommeil paradoxal ou sommeil REM (Rapid Eye Movement) du nom des mouvements oculaires rapides qui se manifestent pendant cette phase de sommeil » : CENAS – centre du sommeil, « Organisation du sommeil (les phases) », dernière mise à jour le 12/06/2018 : http://www.cenas.ch/le-sommeil/comprendre-le-sommeil/phases-du-sommeil/

[1791] Zeo Inc., entreprise lancée à Boston en 2003, fermée en 2013, Voir par ex. : Bloomberg : « *As of May 2013, Zeo, Inc. went out of business. Zeo, Inc. develops sleep management software solutions. It offers SoftWave, a solution that enable users to measure sleep. The company also provides Sleep Manager mobile, which enables consumers to track sleep quantity and sleep quality, as well as helps people manage and improve their sleep using their iPhone, iPod Touch, and iPad. [...]* »: https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=20632735 ; J. ORLIN, « Sleep Tracking Startup Zeo Says Goodnight », Techcrunch.com, 2013 : https://techcrunch.com/2013/05/22/sleep-tracking-startup-zeo-says-goodnight/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=TJ4V83HjVbblRHpfVSisjQ

[1792] Premiers pas avec Fitbit Blaze – Découvrez toutes les choses formidables que vous réserve votre Fitbit Blaze!, « Consulter votre progrès » : https://www.fitbit.com/fr/blaze/blaze-101

notifications couvrant ainsi « les pas et calories ; le suivi du sommeil ; le suivi de la fréquence cardiaque 24/7 ; le suivi de la santé féminine ; le suivi des étages gravis en marches ou en ascensions ; le suivi des longueurs ; adapté à la nage ; suggère plus de 15 modes d'exercices ; propose des rythmes à distance en temps réel ; transmet les notifications des smartphones et objets connectés ; propose des centaines d'applications ; propose d'enregistrer et d'écouter la musique ; recommande des exercices à l'écran ; effectue des paiements aux poignets »[1793].
Une autre entreprise a mis au point un bracelet, Basis Peak, qui contient des capteurs nouvellement mis à jour, le plus évident étant le capteur de fréquence cardiaque optique « *[…], which uses a more powerful light to blast through your skin, allowing for more accurate measurements, including the ability to measure your pulse during a workout, a feature that was starkly missing from the previous model. Beyond that, the Peak's motion sensor is better able to track what kind of exercise you're up to (and thus give you a better idea of how many calories you're burning) and how much you roll around in bed while it's tracking your sleep* », mais est également capable d'analyser la conductance cutanée, le tout constituant des mesures de stress[1794]. Et l'ensemble de ces produits est proposé à la vente sur Amazon par exemple.

Il est, dès lors, pragmatiquement évident qu'obtenir les données devient plus facile et moins intrusif que jamais. Les informations sont constamment saisies et retranscrites sous forme de données ce qui permet de les réutiliser facilement, alimentant par conséquent l'objectif principal partagé désormais par tous les secteurs, à savoir celui de transformer le monde en données, ce qui transparaît par exemple à travers l'enthousiasme entourant les objets connectés, les « Internet of Things », intégrant des puces, capteurs et modules de communication dans les objets et les actes du quotidien ; objectif qui concerne en partie la mise en réseau des individus mais tout autant la mise en données de tout ce qui les entoure. En effet, « *once the world has been datafied, the potential uses of the information are basically limited only by one's ingenuity* »[1795] ; ce qui se matérialise à l'ère du Big data où les outils, méthodes, techniques et équipements développés sont largement disponibles, facilitant la réalisation de tâches aussi variées que possible beaucoup plus rapidement, à grande échelle et dans de nombreux contextes différents, parfois, simultanément. C'est en quelque sorte la concrétisation du grand projet

[1793] Fitbit versa – Gamme de montres intelligentes : https://www.fitbit.com/fr-ca/versa
[1794] K. RUSSELL, "Basis Unveils The Peak, A Smarter Fitness Tracker", Techncrunch.com, 2014: https://techcrunch.com/2014/09/30/basis-unveils-the-peak-a-smarter-fitness-tracker/ & "Basis Launches A Limited Edition Titanium Peak, Updates Bands And App", Techncrunch.com, 2014: https://techcrunch.com/2015/05/19/basis-launches-a-limited-edition-titanium-peak-updates-bands-and-app/
[1795] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Id.,* p. 96.

d'infrastructure dans lequel la société de l'information se retrouve qui, à certains égards, rivalise avec les infrastructures du passé, des aqueducs romains à l'Encyclopédie des Lumières, mais qui s'avère être difficile à apprécier en raison de sa nouveauté et de ses caractéristiques, traits et produits innovants et intangibles. Cependant, tout comme les autres progrès infrastructurels, la nouvelle infrastructure émergente provoquera certainement des changements fondamentaux au sein de la société : « *aqueducts made possible the growth of cities; the printing press facilitated the Enlightenment, and newspapers enabled the rise of the nation state. But these infrastructures were focused on flows – of water, of knowledge. So were the telephone and the Internet. In contrast, datafication represents an essential enrichment in human comprehension. With the help of Big data, we will no longer regard our world as a string of happenings that we explain as natural or social phenomena, but as a universe comprised essentially of information* »[1796].

De nos jours, la société détient les capacités et les pouvoirs de collecte et de calcul des aspects physiques et intangibles de l'existence à une échelle beaucoup plus complète, accordant les moyens et donc le pouvoir, à l'instar des infrastructures précédentes, de cartographier et dessiner le monde d'une manière quantifiable et analysable. En effet, « *today, we are a numerate society because we presume that the world is understandable with numbers and math. And we take for granted that knowledge can be transmitted across time and space because the idea of the written word is so ingrained. Tomorrow, subsequent generations may have a "big-data consciousness" – the presumption that there is a quantitative component to all that we do, and that data is indispensable for society to learn from* »[1797]. Il paraît alors que c'est l'avènement du monde calculable au sein duquel toute information est quantifiée et mise en donnée pour qu'elle puisse 'parler'[1798] en fonction des interrogations, des volontés et des intérêts de ceux qui interrogent. Et ce monde permet d'adapter l'offre à la demande, d'ajuster les primes aux risques, d'aligner les demandes de crédit aux profils des demandeurs, de détecter les erreurs ou les injustices médicales, d'adapter et de rationaliser les dépenses et ainsi de suite. Finalement, « *persuadés que la quantité peut se substituer à la qualité, les zélotes des big data assurent qu'un monde plus mesurable deviendrait aussi plus calculable* »[1799].

[1796] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Ibid.,* p. 96.
[1797] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Ibidem,* p. 97, et les auteurs rajoutent que "*the notion of transforming the myriad dimensions of reality into data probably seems novel to most people at present. But in the future, we will surely treat it as given (which, pleasingly, harks back to the very origin of the term "data")*".
[1798] *Cf.* p. 135 et s.
[1799] D. CARDON, *À quoi rêvent les algorithmes*, *Id*., p. 58.

Le pouvoir des données et de la quantification, tirant principalement leur force de logiques techniques, économiques et mathématiques, marque une rupture avec les logiques, les modèles et les paradigmes anciennement adoptés ou existants, largement facilitée par l'avènement de ce que C. Christensen nomme les « *disruptive technologies* », les technologies de rupture, et la « *disruptive innovation* », l'innovation disruptive, évoquant par là même le caractère disruptif, perturbateur et innovant, de la révolution numérique et l'avènement du Big data.

Selon l'auteur, les technologies de rupture mettent sur le marché une proposition de valeur très différente de celle qui existait auparavant : « *Generally, disruptive technologies underperform established products in mainstream markets. But they have other features that a few fringe (and generally new) customers value. Products based on disruptive technologies are typically cheaper, simpler, smaller, and, frequently, more convenient to use. […]. Small off-road motorcycles introduced in North America and Europe by Honda, Kawasaki, and Yamaha were disruptive technologies relative to the powerful, over-the-road cycles made by Harley-Davidson and BMW. Transistors were disruptive technologies relative to vacuum tubes. Health maintenance organizations were disruptive technologies to conventional health insurers. In the near future, "internet appliances" may become disruptive technologies to suppliers of personal computer hardware and software* »[1800]. En ce sens, la mention du caractère disruptif évoque et renvoie au caractère innovant du numérique, dont les effets sur les environnements économiques, politiques ou sociaux peuvent s'avérer être radicaux et intransigeants. Ce qui évoque également le concept de « destruction créatrice », « *creative destruction* », forgé en 1942 par J. Schumpeter, capitaliste renommé qui percevait l'entreprenariat comme la pierre angulaire du capitalisme, et qui qualifiait le processus de « *creative destruction* » comme étant « *the essential fact about capitalism* »[1801].

La numérisation des informations, la dématérialisation des données, l'intensification démesurée des capacités de stockage et de traitement, tout autant que l'augmentation de la vitesse et des capacités de partage et de transmission en temps réel, rompant avec l'unité de lieu, de temps et d'espace, remettent en question les modèles et structures classiques et alimentent le

---

[1800] C. M. CHRISTENSEN, *The innovator's dilemma: When new technologies cause great firms to fail*, Harvard Business School Press, Boston, Massachusetts, 1997, p. 11.

[1801] J. A. SCHUMPETER, *Capitalism, Socialism and Democracy*, Routledge, London and New York, the Taylor & Francis group, 1994 (1ère publication: Royaume-Uni, 1943), p. 83: "*The opening up of new markets, foreign or domestic, and the organizational development from the craft shop and factory to such concerns as U.S. Steel illustrate the same process of industrial mutation—if I may use that biological term—that incessantly revolutionizes the economic structure* ***from within****, incessantly destroying the old one, incessantly creating a new one. This process of Creative Destruction is the essential fact about capitalism. It is what capitalism consists in and what every capitalist concern has got to live in*."; disponible en ligne: https://eet.pixel-online.org/files/etranslation/original/Schumpeter,%20Capitalism,%20Socialism%20and%20Democracy.pdf

« fétichisme du chiffre » ainsi que le « fétichisme de la donnée »[1802] amorcés avec la montée du pouvoir des données et de la quantification, façonnant par ailleurs les stratégies adoptées à l'ère du numérique.

§2. Des stratégies publiques et privées de rupture

Des stratégies et pratiques gouvernementales, institutionnelles, bureaucratiques, économiques ou marchandes, développées et utilisées initialement dans des secteurs distincts, sont désormais employées de manière indifférenciée, marquant une rupture avec l'usage et la norme tout en mettant en exergue des stratèges d'harmonisation et de science économique (A), d'une part, et, concurrentiels et de bureaucratie (B), d'autre part.

A. Des stratèges d'harmonisation et de science économique

En droit de l'Union européenne, la notion d'harmonisation a toujours occupé une place quasi-centrale visant continuellement la conciliation et la coordination entre le droit, la protection des libertés, la sécurité, le progrès économique et social, ou encore la promotion du marché intérieur unique, et se présente « *tantôt comme la réalisation juridique des libertés économiques garanties* [par le droit de l'Union], *tantôt comme un processus spontané résultant de l'usage de ces libertés* »[1803]. Ainsi, le RGPD, rappelant que l'ancienne directive 95/46/CE « *vise à harmoniser la protection des libertés et droits fondamentaux des personnes physiques en ce qui concerne les activités de traitement et à assurer le libre flux des données à caractère personnel entre les États membres* »[1804], précise que « *le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques* »[1805].

L'harmonisation citée par l'ancienne directive s'est traduite dans le nouveau Règlement par la réalisation, la consolidation et la convergence, des notions visant finalement la concorde et l'harmonie, principalement, entre les différents droits et libertés mais aussi entre les différents systèmes juridiques nationaux. À ce titre, en ce qui concerne le traitement des catégories particulières de données, les données sensibles, le Règlement prévoit « *des conditions*

[1802] A. ROUVROY, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des big data », *op. cit.*, p. 407 et 413.
[1803] A. SUPIOT, *La gouvernance par les nombres, op. cit.,* p. 107.
[1804] RGPD, Cons. 3.
[1805] RGPD, Cons. 2.

harmonisées pour le traitement des catégories particulières de données à caractère personnel relatives à la santé, pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est effectué pour certaines fins liées à la santé par des personnes soumises à une obligation légale de secret professionnel »[1806]. De même, en matière de sanctions, « *afin de renforcer et d'harmoniser les sanctions administratives applicables en cas de violation du présent règlement, chaque autorité de contrôle devrait avoir le pouvoir d'imposer des amendes administratives* »[1807], et lorsque le « *règlement n'harmonise pas les sanctions administratives ou, si nécessaire dans d'autres circonstances, […], les États membres devraient mettre en œuvre un système qui prévoit des sanctions effectives, proportionnées et dissuasives* »[1808].

Par ailleurs, le RGPD vise à concilier les droits et les libertés aux fins de trouver un équilibre entre les droits fondamentaux en désaccord, y compris la possibilité de prévoir des exemptions ou des dérogations aux droits et aux obligations prévus par le Règlement pour réaliser la convergence[1809]. Plus généralement, l'Union et les États membres, « *soucieux de renforcer l'unité de leurs économies et d'en assurer le développement harmonieux en réduisant l'écart entre les différentes régions et le retard des moins favorisées* »[1810], estiment que l'évolution de la politique sociale de l'Union, notamment, résultera « *du fonctionnement du marché intérieur*

[1806] RGPD, Cons. 53.
[1807] RGPD, Cons. 150.
[1808] RGPD, Cons. 152.
[1809] RGPD, Cons. 153 « *Le droit des États membres devrait concilier les règles régissant la liberté d'expression et d'information, y compris l'expression journalistique, universitaire, artistique ou littéraire, et le droit à la protection des données à caractère personnel en vertu du présent règlement. Dans le cadre du traitement de données à caractère personnel uniquement à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, il y a lieu de prévoir des dérogations ou des exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, consacré par l'article 11 de la Charte. […]. En conséquence, les États membres devraient adopter des dispositions législatives qui fixent les exemptions et dérogations nécessaires aux fins d'assurer un équilibre entre ces droits fondamentaux. […]* » ; Art. 85 « *Les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, […]. Dans le cadre du traitement réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, les États membres prévoient des exemptions ou des dérogations au chapitre II (principes), au chapitre III (droits de la personne concernée), au chapitre IV (responsable du traitement et sous-traitant), au chapitre V (transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales), au chapitre VI (autorités de contrôle indépendantes), au chapitre VII (coopération et cohérence) et au chapitre IX (situations particulières de traitement) si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information* » ; Art. 90 « *Les États membres peuvent adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôle […] à l'égard des responsables du traitement ou des sous-traitants qui sont soumis, […], à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes,* ***lorsque cela est nécessaire et proportionné pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret.*** *[…]* ».
[1810] Versions consolidées du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne - Journal officiel n° C 326 du 26/10/2012 pp. 0001 – 0390, Préambule TFUE.

qui favorisera l'harmonisation des systèmes sociaux », les procédures de « *rapprochement des dispositions législatives, réglementaires et administratives* » accompagnent finalement ce processus spontané ayant, dans cette perspective, une fonction subsidiaire[1811].

C'est donc le « fonctionnement du marché intérieur », à savoir le « *libre jeu donné aux calculs d'intérêts des opérateurs économiques* », qui doit contribuer à la réalisation de « l'harmonisation des systèmes sociaux » : « *un peu comme le Traité de Gratien, huit siècles plus tôt, le Traité européen vise ainsi à réaliser une « concorde des canons discordants », qui surmonte la diversité des droits nationaux et les impératifs de compétitivité pour aboutir à une « égalisation dans le progrès ». Mais contrairement à Gratien, cette concorde n'est pas conçue comme une œuvre juridique, mais comme un sous-produit du calcul économique que le rapprochement des législations a pour seule fonction d'accompagner et de faciliter* »[1812]. C'est l'harmonie par le calcul destinée à trouver un équilibre, à rapprocher et concilier les législations, et à établir des mesures proportionnelles harmonieuses ainsi qu'une concorde, « *c'est-à-dire un accord parfait transcendant* » les différences des personnes[1813], dans le but de mettre en place une union économique, d'instaurer une union douanière, d'assurer le progrès économique et social, de rapprocher les outils de défense, d'éviter les distorsions de concurrence, ou encore de libérer les flux et la circulation (des données, des capitaux, des marchandises, etc.). De façon plus générale, « *afin de promouvoir un développement harmonieux de l'ensemble de l'Union, celle-ci se développe et poursuit son action tendant au renforcement de sa cohésion économique, sociale et territoriale* »[1814].

Rompant, de ce fait, avec l'approche positiviste du droit, ces législations européennes semblent plus répondre à la doctrine *Law and economics* qui prétend également fonder l'harmonie sociale sur la raison mathématique, et la rationalité numérique, en poursuivant, *de facto* et *in concreto*, une analyse économique du droit qui applique principalement « *the tools of microeconomic theory to the analysis of legal rules and institutions* »[1815]. Cette doctrine, qui se traduit par 'l'analyse économique du droit' (à ne pas confondre avec l'économie politique), tend à appréhender le droit et son application par des outils d'analyse économique et des calculs d'utilité, introduisant le 'code' de la science économique, à savoir « *les concepts de base de la*

[1811] Versions consolidées du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, Art. 151 TFUE.
[1812] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 108.
[1813] A. SUPIOT, *La gouvernance par les nombres, Ibid.,* p. 109.
[1814] Versions consolidées du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, Art. 174 TFUE.
[1815] L. KORNHAUSER, "The Economic Analysis of Law", *In* E. N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy,* Fall 2017 Edition, Metaphysics Research Lab, Stanford University: https://plato.stanford.edu/entries/legal-econanalysis/

théorie économique, certains de ses instruments de calcul et de ses critères d'évaluation »[1816], facilement transposables dans d'autres disciplines de sciences sociales, voire dans l'ensemble de l'ordre juridique et l'univers des normes, ne se réduisant pas aux seuls secteurs de l'industrie et du commerce. Le postulat principal de la doctrine *Law and Economics* est celui de l'existence d'un ordre spontané du marché, dont le bon fonctionnement peut être simplifié ou paralysé par le système juridique en vigueur. Celle-ci peut être de nos jours définie comme « *the application of economic theory (primarily microeconomics and the basic concepts of welfare economics) to examine the formation, structure, processes and economic impact of law and legal institutions* »[1817].

Initiée vers la fin les années 40 par l'Université de Chicago avec l'appui de H. Simons et F. Hayek, cette doctrine a suscité un grand intérêt dans le monde occidental et a connu plusieurs extensions dues, principalement, à G. Becker théorisant le déplacement de la définition de la science économique et donc de l'analyse économique du droit[1818]. Définie auparavant par son objet, « la production et la répartition de la richesse », la science économique se définit désormais par sa méthode, « *laquelle permettrait de dévoiler les ressorts profonds des comportements humains dans tous les domaines de leur existence et d'espérer trouver enfin un système de règles qui rende compte de ces comportements* »[1819]. Ainsi, selon Becker, « *postuler l'hypothèse de fonctions de préférences stables et uniformes se justifie par conséquent de façon explicitement méthodologique : il s'agit de produire des prédictions, infirmables sans ambiguïté, sur le comportement, et d'éviter, chaque fois que cela est possible, les explications particulières fondées sur les changements de goûts, les différences de goûts, l'ignorance et les comportements impulsifs ou névrosés* »[1820].

L'analyse économique du droit emploie donc une méthode qui consister à induire et à tirer de l'observation des comportements, des lois et des normes générales auxquelles sera soumis l'ensemble de l'ordre juridique, ravivant par conséquent la foi dans l'harmonie par le calcul, le pouvoir des nombres, du calcul et des statistiques, y compris le pouvoir de la quantification et des données, et évoquant subtilement le concept du 'règne du code', où ce dernier semble faire

[1816] B. FRYDMAN, « Le calcul rationnel des droits sur le marché de la justice : l'école de l'analyse économique du droit », *In* T. Andreani et M. Rosen, *Structure, Système, Champ et Théorie du Sujet*, L'Harmattan, Paris, 1997 (p. 127-146), p. 127.
[1817] N. MERCURO et S. G. MEDEMA, *Economics and the Law: From Posner to post-modernism*, Princeton University Press, 1997, p. 3.
[1818] G. S. BECKER, *The Economic Approach to Human Behavior*, The University of Chicago Press, Chicago, 1978, 314 p.
[1819] A. SUPIOT, *La gouvernance par les nombres, Ibid.,* p. 188.
[1820] M. BLAUG, *La Méthodologie Économique*, Economica, Paris, 2ème Ed. 1994, p. 228.

la loi dans l'architecture du cyberespace[1821]. Plusieurs concepts, théories, outils et principes, principalement économiques, se sont ainsi développés, comme la théorie des jeux, la rationalité, ou la théorie de l'agence, pour justifier la conception d'un ordre normatif intégralement régi et régulé par le calcul. Posner, magistrat américain et considéré par beaucoup comme le père de la doctrine *Law and Economics*, avançait en ce sens que « *one of the major contributions of economic analysis to law has been simplification, enabling enhanced understanding. Economics is complex and difficult but it is less complicated than legal doctrine and it can serve to unify different areas of law [...]. By cutting away the dense underbrush of legal technicalities, economic analysis can also bring into sharp definition issues of policy that technicalities may conceal* »[1822].

Reprenant et prolongeant les idées du théorème de Coase[1823], la doctrine *Law and Economics* a mis en place la théorie des *property rights*, qui désigne un concept ne se limitant pas à la propriété du bien seule, mais se réfère plutôt à l'ensemble des prérogatives et droits rattachés au bien, un « paquet de droits » attachés aux choses, qui peuvent alors être exclusifs et transférables. Cette théorie tend alors à supprimer la frontière entre droit et produit, où la règle de droit est perçue comme un « produit » et le législateur ou le juge comme des « producteurs de règles » et où tout produit est symétriquement envisagé comme support d'un « paquet de droits ». Par conséquent, suivant cette doctrine, « tout est pensé en termes de droits individuels, et tous ces droits obéissent au modèle du droit de propriété, autrement dit ils sont exclusifs et transférables, et le sujet de droit représente une monade régie par le seul souci de soi, ne connaissant d'autres lois que celles auxquelles elle consent dans ses rapports contractuels avec les autres monades »[1824]. Ce qui mène alors le Professeur Supiot à dire « *une telle représentation participe pleinement de l'imaginaire cybernétique qui associe dans une même représentation du monde le rhizome, les réseaux neuronaux ou les réseaux informatiques. L'ordre juridique est conçu lui aussi comme un ordre réticulaire, sans verticalité et sans*

[1821] *Cf.* p. 363 et s., 402 et s.

[1822] W. M. LANDES et R. A. POSNER, *The Economic Structure of Intellectual Property Law*, The Belknap Press of Harvard University Press, Cambridge, 2003, p 10.

[1823] E. BERTRAND et C. DESTAIS, « Le « théorème de Coase », une réflexion sur les fondements microéconomiques de l'intervention publique », *In Reflets et perspectives de la vie économique*, Ed. De Boeck Supérieur, t. XLI, Vol. N° 2, 2002 (p. 111-124), p. 112 : « *Dans un article resté célèbre* [R. H. Coase (1960) « The problem of social cost »,] *et qui a fait l'objet de nombreux commentaires, parfois divergents, Ronald H. Coase, prix Nobel d'économie 1991, montre sur la base d'exemples tirés de la jurisprudence anglaise et américaine que, dans un monde où les coûts de transaction sont nuls et où les droits de propriété sont clairement définis, le libre jeu de la négociation aboutit à un optimum indépendant de l'attribution initiale des droits. C'est ce qui a par la suite été nommé le « théorème de Coase »* ; voir également, R. H. COASE, « The problem of social cost », *In The journal of Law & Economics*, Vol. III, Octobre 1960 (p. 1-44); Disponible en ligne : http://econ.ucsb.edu/~tedb/Courses/UCSBpf/readings/coase.pdf

[1824] A. SUPIOT, *La gouvernance par les nombres, Ibid.,* p. 200-201.

frontières définies », et précise ainsi que « *dans un tel ordre, il n'y a plus de place pour les principes incalculables car inestimables, sur lesquels reposait le règne de la loi. Toutes les valeurs défendues par ces principes sont converties en valeurs quantifiables* »[1825].

Au regard des jurisprudences européennes modernes, il semble que des intérêts, des droits et des libertés se transforment peu à peu en valeurs quantifiables mises en balance avec d'autres intérêts et valeurs quantifiables. C'est le cas, par exemple, de la dignité humaine qui est « inviolable et doit être respectée et protégée »[1826], la « reconnaissance de la dignité inhérente à tous les membres de la famille humaine […] constituant le fondement de la liberté, de la justice et de la paix dans le monde »[1827], mais qui paraît désormais correspondre à une valeur quantifiable, sous l'égide de l'équivalence et de la proportionnalité, évoquant dans ce cadre la conception de Kant de la dignité : « *dans le règne des fins, tout à un prix ou une dignité. Ce qui a un prix peut être aussi bien remplacé par quelque chose d'autre, à titre d'équivalent ; au contraire, ce qui est supérieur à tout prix, ce qui par suite n'admet pas d'équivalent, c'est ce qui a une dignité* »[1828].

Ainsi, en 2007, la Cour de justice des communautés européennes a jugé que « *l'exercice des droits fondamentaux en cause, à savoir respectivement les libertés d'expression et de réunion ainsi que le respect de la dignité humaine, n'échappe pas au champ d'application des dispositions du traité et […] doit être concilié avec les exigences relatives aux droits protégés par ledit traité* [la libre concurrence, la libre circulation des marchandises et des capitaux et la libre prestation de services] *et conforme au principe de proportionnalité* »[1829]. Dans une autre affaire, elle a en quelque sorte critiqué et réprimé le système juridique allemand pour avoir érigé la dignité humaine en droit fondamental autonome, affirmant que « *l'ordre juridique communautaire tend indéniablement à assurer le respect de la dignité humaine en tant que principe général du droit. Il ne fait donc pas de doute que l'objectif de protéger la dignité*

[1825] A. SUPIOT, *La gouvernance par les nombres, Ibidem,* p. 201 ; *Cf.* p. 558 et s.

[1826] Charte des droits fondamentaux de l'Union Européenne, Art. 1er – Dignité humaine « *La dignité humaine est inviolable. Elle doit être respectée et protégée.* »

[1827] Déclaration universelle des droits de l'homme de 1948, préambule ; l'Art. 1 précise également « *Tous les êtres humains naissent libres et égaux en dignité et en droits. Ils sont doués de raison et de conscience et doivent agir les uns envers les autres dans un esprit de fraternité* ».

[1828] E. KANT, *Fondements de la Métaphysique des mœurs*, (1785), Trad. de V. Delbos (1862-1916), Éd. Les Échos du Maquis, 2013, p. 47, où l'auteur précise « *[…]. La moralité, ainsi que l'humanité, en tant qu'elle est capable de moralité, c'est donc là ce qui seul a de la dignité. L'habileté et l'application dans le travail ont un prix marchand ; l'esprit, la vivacité d'imagination, l'humour, ont un prix de sentiment ; par contre, la fidélité à ses promesses, la bienveillance par principe (non la bienveillance d'instinct), ont une valeur intrinsèque.* » ; disponible en ligne : https://philosophie.cegeptr.qc.ca/wp-content/documents/Fondements-de-la-Métaphysique-des-moeurs.pdf

[1829] CJCE (Grande chambre), International Transport Workers' FederationetFinnish Seamen's Union *c.* Viking Line ABP et OÜ Viking Line Eesti (dit arrêt Viking), Affaire C-438/05 du 11 décembre 2007, §46.

humaine est compatible avec le droit communautaire, sans qu'il importe à cet égard que, en Allemagne, le principe du respect de la dignité humaine bénéficie d'un statut particulier en tant que droit fondamental autonome »[1830]. Le principe de proportionnalité tend dans cette perspective à ramener toute règle, toute norme, à un calcul d'utilité et paraît, *de facto*, pérenniser le raisonnement selon lequel toute règle, toute liberté, a une valeur quantifiable conformément à l'approche de Kant, à l'harmonisation par les calculs, et à la science économique.

Comme il a été vu, le principe de proportionnalité constitue non seulement une valeur européenne de principe, mais compose dorénavant les valeurs numériques européennes applicables en matière de protection des données personnelles[1831]. À l'occasion d'une autre affaire, les juges européens, pour répondre à la question de la « *conciliation nécessaire des exigences de la protection des droits fondamentaux dans la Communauté avec celles découlant d'une liberté fondamentale consacrée par le traité* », et plus particulièrement à la question de la portée respective des libertés d'expression et de réunion, garanties par la CEDH, et de la libre circulation des marchandises, « lorsque les premières sont invoquées en tant que justification d'une restriction à la seconde », ont ainsi adopté le raisonnement selon lequel « *d'une part, la libre circulation des marchandises constitue certes l'un des principes fondamentaux dans le système du traité* » mais peut, sous certaines conditions, faire l'objet de restrictions pour des raisons limitativement énumérées ou au titre des exigences impératives d'intérêt général ; mais que, d'autre part, « *si les droits fondamentaux en cause dans l'affaire au principal sont expressément reconnus par la CEDH et constituent des fondements essentiels d'une société démocratique, il résulte toutefois* [des termes mêmes] *de cette convention que les libertés d'expression et de réunion sont également susceptibles de faire l'objet de certaines limitations justifiées par des objectifs d'intérêt général, pour autant que ces dérogations sont prévues par la loi, inspirées par un ou plusieurs buts légitimes au regard desdites dispositions et nécessaires dans une société démocratique, c'est-à-dire justifiées par un besoin social impérieux et, notamment, proportionnées au but légitime poursuivi* »[1832]. Les juges en concluent que les « *droits à la liberté d'expression et à la liberté de réunion pacifique garantis par la CEDH n'apparaissent pas non plus [...] comme des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société* », et que des restrictions peuvent ainsi être apportées à l'exercice de ces droits pour autant qu'elles ne constituent pas une

[1830] CJCE (1ère chambre), Omega Spielhallen-und Automatenaufstellungs-GmbH *c.* Oberbürgermeisterin der Bundesstadt Bonn (dit arrêt Omega), affaire C-36/02 du 14 octobre 2004, §34.
[1831] *Cf.* p. 297.
[1832] CJCE, Eugen Schmidberger, Internationale Transporte und Planzüge *c.* Republik Österreich (dit arrêt Schmidberger), Affaire C-112/00 du 12 juin 2003, §77-79.

« intervention démesurée »[1833]. Selon la Cour de justice européenne, il convient dans ces conditions de « *mettre en balance les intérêts en présence et de déterminer, eu égard à l'ensemble des circonstances de chaque cas d'espèce, si un juste équilibre a été respecté entre ces intérêts* »[1834].

Des illustrations de ce raisonnement et de la recherche d'un équilibre entre des droits et des libertés fondamentaux conformément au principe de légalité, de nécessité et de proportionnalité se retrouvent fréquemment dans les arrêts de la Cour, caractérisées par la quête de l'harmonie et la conciliation équivalente entre les règles en jeu. *In fine*, c'est une mise en œuvre quasi-générale de la doctrine et du raisonnement *Law and Economics* qui, finalement, « *n'a rien qui puisse surprendre. Depuis ses origines romaines, n'importe quelle idéologie peut user du Droit comme d'une technique, du moins aussi longtemps que cette idéologie respecte l'autonomie de l'ordre juridique. Car une fois franchi ce seuil, une fois brisé le « fétichisme de la forme juridique », on quitte le domaine de la normativité juridique, quand bien même on tenterait d'en sauvegarder les apparences* »[1835].

En effet, pour reprendre la conclusion première de Posner, « *Economics is a great simplifier of law* »[1836].

B. Des stratèges concurrentiels et de bureaucratie

La faculté d'élaborer des modèles économiques personnalisés, ainsi qu'il a été précédemment vu[1837], a révélé le recours à des stratèges économiques, compétitifs, permettant d'asseoir le monopole sur le marché du business-modèle choisi et donc de l'entreprise, ainsi que l'emploi récurrent de la bureaucratie et ses techniques et procédures, afin d'appuyer et de développer le modèle sélectionné et pouvoir surveiller efficacement les internautes, obtenant alors plus d'informations au profit de leurs entreprises et modèles.

La collecte et la captation des données s'opèrent, à l'heure actuelle, autant directement qu'indirectement, les sources étant désormais aussi nombreuses que variées. Les systèmes de fidélisation mis en œuvre par les commerçants et les prestataires de services leur permettent d'établir des profils détaillés et d'acquérir une meilleure compréhension de leurs clients, de réduire les coûts de transaction pour les deux parties, et d'offrir des remises de fidélité et des offres spéciales. Les identifiants de connexion, l'ouverture d'une session et d'autres formes de

[1833] CJCE, Arrêt Schmidberger, *Id.*, §80.
[1834] CJCE, Arrêt Schmidberger, *Ibid.*, §81.
[1835] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 212-213.
[1836] W. M. LANDES et R. A. POSNER, *The Economic Structure of Intellectual Property Law*, *op. cit.*, p. 420.
[1837] *Cf.* p. 142.

renseignements transactionnels de connexion donnent un aperçu du comportement et des besoins des utilisateurs, ce qui permet aux fournisseurs de services d'offrir des services améliorés, adaptés de manière plus spécifique aux besoins des utilisateurs.

D'autres sources de données personnelles observées et surveillées comprennent l'historique de navigation, les consultations de pages web en temps réel ou les téléchargements effectués, permettant le suivi complet des activités en ligne des utilisateurs. Cela peut également inclure les achats et les transactions, l'accès et l'utilisation d'applications particulières, la bureautique et la domotique (*home and office automation*), les réseaux intelligents et la sécurité (comme la télévision en circuit fermé CCTV, les capteurs, etc.). De plus, ces sources et les nombreuses informations collectées peuvent être utilisées pour aider les fournisseurs de services à identifier les menaces potentielles à la sécurité, par exemple en repérant lorsqu'un compte est accédé à partir d'une adresse IP d'une région différente ou à une heure différente de la journée de l'habituelle. Tout ceci vise à contribuer à la mise au point de modèles économiques personnalisés, à l'émergence de nouveaux modèles économiques, mais surtout à rendre le marché si compétitif de sorte que la manifestation d'une situation où certaines entreprises détiennent un monopole sur le marché est inévitable ; le tout fonctionnant sur la base d'une chaîne de valeur et d'un système de hiérarchisation[1838].

Ces nouveaux modèles économiques émergents poursuivent tous une fin commune, celle de mieux comprendre leurs utilisateurs-consommateurs, de les identifier et les connaître intimement pour pouvoir prédire leurs futurs comportements, y compris leurs futurs achats et consommations, qu'il s'agisse d'organisations privées ou publiques. Les données sont également, il convient de le rappeler, agrégées et sauvegardées par de nombreux acteurs de la chaîne de valeur des données, valorisant par conséquent non seulement les données et les personnes, mais aussi les modèles économiques et les organisations, y compris leur rôle et poids sur le marché. Les historiques de navigations, le suivi internet et les enregistrements des 'recherches' (*search*) sont conservés par les fournisseurs de services internet et les fournisseurs de services de recherche web ; les dossiers médicaux sont conservés par des médecins et un large éventail d'organismes des secteurs public et privé, d'assureurs de soins de santé, d'employeurs, et autres ; les dossiers financiers sont conservés par les commerçants et les distributeurs, les banques et les autres institutions financières, les employeurs et les organismes fiscaux, les préfectures et les mairies ; les données de localisation sont stockées par les opérateurs de téléphonie mobile, les fournisseurs d'accès internet, les services publics, les

[1838] *Cf.* p. 135.

opérateurs de transport et autres. Le tout est structuré hiérarchiquement et suit des procédures bureaucratiques, et, quand il est nécessaire ou qu'un intérêt économique ou social l'exige, l'intégralité de ces données est agrégée, corrélée, recoupée ou comparée selon la finalité du moment poursuivie.

En outre, il est utile de noter que les données peuvent faire l'objet de plusieurs cycles d'analyse et de distribution, et que des données supplémentaires sont produites et ajoutées à chaque itération[1839]. Lorsque les informations sont utilisées pour établir un dossier numérique personnel plus raffiné et uniformisé, les entreprises d'analyse de données, nouveau modèle économique, finissent souvent par revendre les dossiers de profils combinés sur le marché représentant, par conséquent, une source importante de données, stimulant la valeur monétaire des données personnelles et des concurrents de taille, à ne pas négliger. Mais il n'est pas toujours nécessaire de recourir aux entreprises d'analyse de données pour obtenir des informations et accroître son modèle économique et son chiffre d'affaire. Les entreprises peuvent désormais effectuer leurs propres traitements et analyses grâce aux données disponibles (directement ou indirectement), en vue d'améliorer le service client et la qualité des produits, d'étudier les questions d'interaction médicamenteuse, d'étudier les habitudes de circulation quotidienne et établir des modèles de circulation quotidienne commune, ou encore d'analyser les données d'achats pour non seulement déterminer le moment de grossesse d'une cliente mais aussi prédire sa date d'accouchement[1840]. Cela valorise et accorde certainement des avantages concurrentiels aux entreprises concernées, néanmoins au prix du respect de la vie privée et du « bien-être » de leurs clientèles.

Rappelons l'exemple de Target qui a réussi à développer un système capable de déterminer le moment de grossesse et la date d'accouchement approximative de leurs clientes, ce qui lui a permis de tirer de nombreux profits[1841]. L'entreprise s'est toutefois retrouvée au milieu d'un scandale en raison de son modèle et de ses techniques de marketing, générant des conséquences sur la vie réelle quotidienne d'une de ses clientes, un père ayant découvert la grossesse de sa fille mineure et les activités intimes de son foyer parce qu'elle avait reçu de l'entreprise en cause des publicités personnalisées, des remises de fidélité sur les produits de grossesse et de nourrisson ainsi que des coupons pour vêtements et berceaux pour bébé par courriel[1842]. Les

[1839] OECD, "Exploring the Economics of Personal Data", *loc. cit.,* p. 13.
[1840] *Cf.* p. 135 et s.
[1841] *Cf.* p. 142.
[1842] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *op cit.,* p. 58, les auteurs nous racontent ainsi que "*One day, an angry man stormed into a Target store in Minnesota to see a manager. "My daughter got this in the mail!" he shouted. "She's still in high school and you're sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?". When the manager called the man a few days later to*

nouveaux modèles, activités et techniques ainsi mis au point augmentent la compétitivité et l'attractivité économique de l'organisation sur le marché, mais peut parallèlement engendrer de nombreuses conséquences dans la vie concrète des personnes, porter atteinte à leur vie privée, leur réputation et leur dignité humaine, et semblent être finalement en contradiction avec leurs objectifs respectifs manifestés qui visent, globalement, le bien-être des individus.

Ce travail d'analyse est souvent effectué par des entreprises dotées d'une infrastructure développée, de solides compétences analytiques et de réseaux de distribution développés, impliquant à la fois des acteurs traditionnels dans la chaîne de valeur, mais surtout de nouveaux modèles économiques et de nouvelles activités émergeants, en réponse aux nouvelles demandes et opportunités manifestées. Sans compter les acteurs traditionnels du traitement de données, parmi lesquels figurent les distributeurs et les prestataires de services exploitant des logiciels de gestion des relations clients (CRM), des systèmes d'intelligence économique et des systèmes de fidélisation, une panoplie de nouveaux acteurs s'est mise en place : comme ceux impliqués dans la publicité en ligne, les études de marché ou le *cloud computing*, les fournisseurs et les courtiers en données, les agrégateurs de données ou les analystes de données spécialisés ; ce dernier acteur, à lui seul, comprend de nombreux autres, tels que les *data analytics, data scientists, behavioural analytics* ou *predictive analytics*. En effet, « *a "tracking industry" has emerged that is driving innovation in advertising* » et de nombreux autres secteurs[1843].

Si ces nouveaux modèles économiques induisant de nouvelles activités et de nouveaux acteurs se développent et progressent dans le cadre d'une dynamique technologique innovante et puissante, leur équilibre concurrentiel reste fragile, et même s'ils captent une partie de la valeur tirée de l'exploitation et du traitement des données, ils demeurent toutefois confrontés à la forte concurrence d'acteurs globaux, aux premiers rangs desquels se trouvent les GAFAM. Ces géants du web occupent des positions stratégiques sur le nouveau marché que représente la chaîne de valeur de données, en exploitant leurs propres atouts inestimables et remarquables tels que les effets de réseau, les capacités d'innovations technologiques, les audiences vastes et prodigieuses, les innombrables ensembles d'inventaires, de dossiers et de données, leur position dominante sur le marché. Il est alors possible et facile pour ces entreprises en question d'exploiter, à leur tour, les nouveaux acteurs intermédiaires, voire de les racheter. Il suffit de penser à Facebook qui a racheté WhatsApp par exemple, ou à Google qui, elle-même détenue

apologise, however, the voice on the other end of the line was conciliatory. "I had a talk with my daughter", he said, "It turns out there's been some activities in my house I haven't been completely aware of. She's due in august. I owe you an apology."

[1843] OECD, "Exploring the Economics of Personal Data", *Id.,* p. 13.

par Alphabet, a racheté YouTube, entre autres. Selon l'Autorité de la concurrence française, « *le développement des positions fortes de Google et Facebook repose avant tout sur l'exploitation de sites et de services populaires pour les internautes tels que Google Search, YouTube, Chrome, Gmail, Maps pour Google ; Instagram, WhatsApp et le réseau social éponyme pour Facebook* »[1844].

Dans le secteur de la publicité en ligne par exemple, Facebook et Google, qui en sont les deux leaders, « *fournissent principalement des services gratuits aux internautes et génèrent l'essentiel de leurs revenus à travers la commercialisation de services publicitaires aux éditeurs et annonceurs, qui sont fondés sur l'exploitation de volumes colossaux d'informations sur les individus, les éditeurs, et les annonceurs. Ces données sont ensuite valorisées et commercialisées par leur intégration à différents services publicitaires, permettant notamment de cibler des segments d'audience, d'adresser les publicités, et de fournir des informations sur le déroulement des campagnes pour améliorer leurs performances* »[1845]. Et leur succès tient au fait qu'ils détiennent de nombreux avantages concurrentiels, leur permettant, *inter alia*, de mettre au point des « *environnements logués* » où les utilisateurs s'identifient pour accéder au service gratuit, constituant à eux seuls des « *sources de nombreuses données sociodémographiques et comportementales* »[1846]. Laissant de côté les condamnations pour manquement à leur obligation de recueillir le consentement des personnes concernées ou pour l'insertion de clauses abusives dans leurs conditions générales d'utilisation, la Commission européenne, gardienne de la concurrence dans l'Union, a ainsi condamné, en 2017, Facebook à une amende de 110 millions d'euros pour avoir fourni des renseignements inexacts ou dénaturés au cours de l'enquête que la Commission a effectuée en 2014, au titre du règlement de l'UE sur les concentrations, concernant l'acquisition de l'application WhatsApp[1847]. Cette décision est censée représenter un sérieux avertissement pour les entreprises susceptibles de recourir aux mêmes types de pratiques. Facebook avait ainsi informé la Commission « *qu'elle ne serait pas*

[1844] Autorité de la Concurrence, Communiqué de Presse du 6 mars 2018 : Enquête sectorielle sur la publicité en ligne : « *L'Autorité de la concurrence rend public son avis dans lequel elle procède au décryptage d'un marché très complexe, marqué par un équilibre concurrentiel fragile. Compte tenu des préoccupations exprimées par les acteurs du secteur, le rapporteur général annonce que ses services vont procéder à un examen préliminaire des éléments rassemblés afin d'estimer s'il y a lieu d'ouvrir une (ou plusieurs) enquête(s) contentieuse(s).* » : http://www.autoritedelaconcurrence.fr/user/standard.php?lang=fr&id_rub=683&id_article=3132

[1845] Autorité de la concurrence, Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, *loc. cit.,* p. 5.

[1846] Autorité de la concurrence, Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, *Id.,* p. 6-7.

[1847] Commission européenne - Communiqué de presse, « Concentrations : la Commission inflige des amendes de 110 millions EUR à Facebook pour avoir fourni des renseignements dénaturés concernant l'acquisition de WhatsApp », Bruxelles, le 18 mai 2017 : http://europa.eu/rapid/press-release_IP-17-1369_fr.htm

en mesure d'établir d'une manière fiable la mise en correspondance automatisée entre les comptes d'utilisateurs de Facebook et ceux de WhatsApp », l'indiquant à la fois dans le formulaire de notification et dans une réponse à une demande de renseignements de la Commission ; or, la Commission a finalement constaté que « *contrairement à ce qu'avait déclaré Facebook [...], la possibilité technique de mettre en correspondance les identités des utilisateurs de Facebook et de WhatsApp existait déjà [...] et que les employés de Facebook étaient au courant de cette possibilité* »[1848].

En revanche, cette stratégie suivie par l'entreprise en cause lui a finalement permis de gagner des avantages concurrentiels, tout en appuyant sa position déjà dominante sur le marché. Il est utile de relever que même la tonalité d'expression de l'Autorité de concurrence, par exemple en rendant ses avis sur la publicité en ligne, s'est véritablement transformée de 2010 à 2018[1849] : elle a, à cet égard, indiqué dans son avis de 2018 que « *les préoccupations* [que l'économie numérique et la régulation des grandes plateformes] *peuvent soulever, et les craintes qu'elles suscitent, ne sont pas tant le fait de leur taille que de la puissance tirée de la masse de données qu'elles collectent et de l'usage qu'elles peuvent en faire grâce à l'utilisation de puissants algorithmes. Le développement de l'intelligence artificielle accentue cette crainte, l'apprentissage profond (machine-learning) permettant d'inférer toujours plus de connaissances du comportement des utilisateurs* », et qu'il faut par ailleurs noter « *qu'une évaluation du poids du secteur est délicate, les différentes sources ne concordant pas toujours entre elles. […]. En outre, les revenus de certains acteurs sont calculés à partir d'estimations, et peuvent présenter des différences avec les revenus réels des entreprises* »[1850].

Le système conçu pour avoir ou pour maintenir une place stratégique et dominante sur le marché s'articule, en lui-même, autour de procédures et stratégies bureaucratiques lui permettant de s'organiser de manière optimale et efficace. S'entendant comme un ensemble particulier de pratiques, la bureaucratie désigne, en général, les grandes organisations publiques

[1848] Commission européenne - Communiqué de presse, « Concentrations : la Commission inflige des amendes de 110 millions EUR à Facebook pour avoir fourni des renseignements dénaturés concernant l'acquisition de WhatsApp », *Id.*

[1849] Autorité de la concurrence, Avis n° 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne, *loc. cit*., et Autorité de la concurrence, Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, *Id.*

[1850] Autorité de la concurrence, Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, *Id.,* p. 14-15, où l'Autorité relève ainsi que « *les difficultés de mesure du marché français de la publicité sur internet sont principalement dues aux multiples critères retenus en termes d'allocation géographique des revenus (adresse de facturation, lieu des clics) et de périmètre des produits. […].* »

et privées dotées de structures hiérarchiques et d'un ensemble de règles, de routines, de méthodes et de procédés complexes et bien élaborés[1851]. Selon le sociologue Weber, l'organisation bureaucratique se compose d'une chaîne de commandement hiérarchique, de bureaux spécialisés pour exécuter des fonctions particulières, et d'un système de règles générales pour gérer l'organisation[1852]. Il affirme, en outre, que « *it does not matter for the character of bureaucracy whether its authority is called "private" or "public"* », la bureaucratie n'étant finalement pas limitée à l'administration gouvernementale ; elle représente aussi une caractéristique de la gestion des affaires[1853]. Ainsi, selon l'auteur, « *bureaucracy, thus understood, is fully developed in political and ecclesiastical communities only in the modern state, and in the private economy only in the most advanced institutions of capitalism* »[1854].

Or, les stratégies et logiques de gestion et de management ont été dernièrement bouleversées par les conceptions de *disruptive technologies* et de *disruptive innovations*[1855]. En effet, en dépit des multiples critiques formulées à l'encontre de ces concepts et du fait qu'ils ont été discrédités par des chercheurs et des professeurs d'université, le concept de « technologies et innovations de disruption » a finalement dominé les débats sur la gestion, depuis sa publication en 1997, dans les secteurs public et privé : « *some fairy tales are too good to stop believing, even after you grow up. Innovation, especially the disruptive kind, has become a religious concept, immune to criticism* »[1856].

Le monde moderne actuel, où tout devient progressivement numérique et où les informations et données sont disponibles en masse, requiert de ce fait une circulation efficace et structurée de l'information pour communiquer, fournir des biens et des services, réglementer, réguler et remplir des fonctions essentielles, de base. À ce titre, Weber indique que la bureaucratie est capable d'atteindre le plus haut degré d'efficacité et de précision et caractérise, en ce sens, formellement le moyen le plus rationnel connu pour exercer une autorité et un contrôle sur les êtres humains[1857]. Les processus bureaucratiques sont très routiniers, luttant et s'efforçant

---

[1851] Voir en ce sens: M. WEBER, *From Max Weber: Essays in Sociology*, H. H. Gerth & C. Wright Mills (trad. & Eds.), New York, Oxford University Press, 1946, p. 196; disponible en ligne: https://archive.org/stream/frommaxweberessa00webe/frommaxweberessa00webe_djvu.txt

[1852] M. WEBER, *Economy and Society: An outline of interpretive sociology*, G. Roth & C. Witticheds (ed.), University of California Press, 1978, p. 956-957; Disponible en ligne: https://archive.org/stream/MaxWeberEconomyAndSociety/MaxWeberEconomyAndSociety_djvu.txt

[1853] M. WEBER, *Economy and Society, Id.*, p. 957.

[1854] M. WEBER, *Economy and Society, Ibid.*, p. 956.

[1855] *Cf.* p. 413-414.

[1856] S. VAIDHYANATHAN, *Anti-social media*, *op. cit.*, p. 206.

[1857] M. WEBER, *Economy and Society, Id.*, p. 223, où l'auteur precise que "*It is superior to any other form in precision, in stability, in the stringency of its discipline, and in its reliability. It thus makes possible a particularly high degree of calculability of results for the heads of the organization and for those acting in*

continuellement pour accroître l'efficacité, visant à normaliser les décisions et à cultiver la spécialisation et l'expertise. Le fonctionnement bureaucratique efficace dépend également d'une quantité considérable de données, notamment celles qui ont trait à des personnes identifiables. En dépit des nombreux avantages que la bureaucratie semble apporter, il faut souligner cependant que, selon Weber, la nature spécifique de la bureaucratie, saluée et accueillie par le capitalisme, « *develops the more perfectly the more the bureaucracy is 'dehumanized,' the more completely it succeeds in eliminating from official business love, hatred, and all purely personal, irrational, and emotional elements which escape calculation. This is the specific nature of bureaucracy and it is appraised as its special virtue* »[1858].

Ainsi, la bureaucratie et ses pratiques peuvent finalement toucher et influencer les personnes qui y sont assujetties, y compris atteindre leur dignité ou leur réputation et affaiblir leurs capacités de critique ou de participation à la société. En outre, les décisions prises au sein des organisations bureaucratiques, publiques comme privées, sont souvent cachées du public, réduisant *ipso facto* la reddition de comptes et l'engagement de la responsabilité. En effet, « *bureaucratic administration always tends to exclude the public, to hide its knowledge and action from criticism as well as it can* »[1859], pouvant alors entraîner des abus ou des négligences en matière de protection des données.

Il faut reconnaître que « *bureaucratic decision-making processes are being exercised ever more frequently over a greater sphere of our lives, and we have little power or say within such a system, which tends to structure our participation along standardized ways that fail to enable us to achieve our goals, wants, and needs* »[1860]. Et l'objectif poursuivi, finalement, ne compte pas vraiment en termes d'impacts réels et palpables dans le quotidien des individus. Le pouvoir n'est pas seulement exercé sous des formes totalitaires, indique le Professeur Solove, et les relations avec les bureaucraties qui sont déséquilibrées en termes de pouvoir peuvent avoir des effets dévastateurs sur les individus, indépendamment des finalités poursuivies : « *Under this view, the problem with databases and the practices currently associated with them is that they disempower people. They make people vulnerable by stripping them of control over their personal information. There is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid*

relation to it. It is finally superior both in intensive efficiency and in the scope of its operations, and is formally capable of application to all kinds of administrative tasks"

[1858] M. WEBER, *From Max Weber: Essays in Sociology, Id.,* p. 216.

[1859] M. WEBER, *Economy and Society, Id.*, p. 992.

[1860] D. SOLOVE, *The Digital Person, op. cit.,* p. 39.

routines, and a way of relating to individuals and their information that often becomes indifferent to their welfare »[1861].

Par ailleurs, la structure de ces modèles économiques et le monopole du marché qu'ils détiennent leur permettent d'émettre des avis, des recommandations et des suggestions, ainsi que d'opérer une traçabilité continue, d'effectuer des corrélations, inductions et prédictions, de développer des algorithmes et des pratiques computationnelles, par le biais de techniques d'apprentissage automatique et de techniques de corrélations devenues de plus en plus élaborées ; le tout ouvrant voie à la chasse au profit des capacités et des applications du Big data manifestée.

Section 2 – La chasse au profit des capacités et applications du Big data

Les innombrables pratiques et techniques offertes par les nouvelles technologies et les logiques et stratégies conséquemment mises en œuvre en font un objet de convoitise, révélant une chasse au profit des capacités et applications du Big data caractérisée par la portée de l'économie des données personnelles (§1) ainsi que par celle de l'économie des sciences de l'homme (§2) ; l'ensemble présentant simultanément une forte valeur ajoutée pour les gouvernements et/ou les entreprises.

§1. La portée de l'économie des données personnelles

La portée de l'économie des données personnelles et son impact profond se traduit, *in concreto*, par les opérations d'avis, de suggestions, de recommandations et de traçabilités (A), dorénavant facilement entreprises, ainsi que par l'emploi continu et massif de la science, de l'innovation, de la prédiction et de la prévention (B).

A. Avis, suggestions, recommandations et traçabilité

La révolution numérique et les avancées technologiques ont multiplié les opportunités de développement d'outils et d'innovations technologiques, dépassant progressivement le seul périmètre d'internet.

Pour ce faire, il s'agit de récolter toujours plus de données et de surveiller les traces et les gisements de données disponibles, en vue d'affiner les modèles et profils et pouvoir alors produire des technologies innovantes individualisées et personnalisées proposant des avis, des

[1861] D. SOLOVE, *The Digital Person*, *Id.,* p. 41.

suggestions, des recommandations, tout en permettant une surveillance et une traçabilité continues de l'internaute afin d'améliorer son quotidien (sa vie ou les services qu'il utilise par exemple), et tout en évitant un gaspillage ou des recommandations générales non effectives, voire même en réduisant les erreurs médicales ou les approximations de la médecine. Les algorithmes, auxquels sont livrés cette masse de données quotidiennement, représenteraient la clé principale permettant de donner une parole différente, objective, aux données qui exprimeraient, à la suite des calculs et des pratiques computationnelles qu'ils opèrent, des facteurs, paramètres ou éléments inconnus par le passé ou impossible à envisager, en raison des technologies manquantes auparavant. C'est par exemple l'objectif principal poursuivi par la politique d'ouverture des données qui cherche à promouvoir le savoir, la transparence, l'efficacité des services publics et administratifs, la recherche ou la vigilance citoyenne[1862].

De façon générale, la révolution et l'innovation technologique résident principalement dans le passage des règles abstraites et normes générales vers des règles précises et un code particulier, une statistique des contextes facilitée par l'accroissement des pouvoirs de calcul, des données, de la quantification, de la statistique, des capacités de récolte et du monopole de la surveillance désormais généralisée. De même, les algorithmes se présentent comme étant plus efficaces et plus objectifs, capables de prédire et de recommander beaucoup mieux qu'un agent humain, permettant de s'adapter aux contextes et aux profils en adaptant leurs codes et leurs méthodes. En effet, dans le cyberespace, « *un algorithme « fonctionne » véritablement lorsqu'il parvient à épouser si étroitement le milieu dans lequel il intervient que les comportements des acteurs se règlent sur ses verdicts et que les principes qu'il met en œuvre nourrissent leurs représentations* »[1863].

Cette révolution numérique induisant des technologies innovantes touche tous les secteurs et tous les espaces privés comme publics, ne se réduisant plus à l'espace de l'internet. À l'heure actuelle, par exemple, il est presque impossible d'échapper à la vidéosurveillance et aux techniques de reconnaissance faciale automatique qui accompagnent souvent ces dispositifs ; techniques qui, en outre, sont aujourd'hui présentes dans de nombreux services, produits, entreprises et commerces. Depuis quelques décennies, des millions de caméras ont été installées dans les foyers, les magasins, les services en ligne, les boîtes de nuit, les téléphones et ordinateurs portables, les parcs et trottoirs, les transports publics et aéroports, les entreprises privées, et ainsi de suite, générant une quantité volumineuse de données conservées et utilisées pour des fins aussi nombreuses qu'hétérogènes : ciblage publicitaire, gestion des réputations

[1862] *Cf.* p. 141-142, et 157-158.
[1863] D. CARDON, *À quoi rêvent les algorithmes*, *op. cit*., p. 62.

(une personne ou une entreprise, ou un produit ou une marque), sécurité du lieu ou sécurité informatique, mesures d'audience en temps réel, offres de produits « sur mesure », recommandations et suggestions personnalisées, identification ou authentification, sélection des clients et ainsi de suite ; l'ensemble contribuant consciemment ou inconsciemment, volontairement ou involontairement, à l'architecture de surveillance de masse et au capitalisme de surveillance susmentionnés[1864].

La vidéosurveillance a donc bel et bien une empreinte dans le quotidien de l'individu, permettant de l'identifier, de le tracer continuellement, de suivre et analyser ses habitudes et comportements, alimentant *de facto* les profils et dossiers numériques constitués sur l'individu en question, utilisables par la suite dans n'importe quel secteur en vue d'émettre un avis ou un jugement sur la personne, une suggestion ou une recommandation guidant finalement ses choix, préférences, comportements et l'évolution de sa personnalité. Aux termes de la CNIL, illustrant parfaitement l'empreinte de la vidéosurveillance : « *Dès que l'on sort de chez soi, on peut être filmé dans le hall de son immeuble, puis dans la rue sur le chemin du bus pour se rendre à son travail. Des caméras peuvent également être présentes dans les transports en commun. À son arrivée sur son lieu de travail, on peut aussi être filmé par les caméras installées par l'employeur. Lors de la pause déjeuner, le magasin où l'on achète sa salade, ou celui où l'on fait ses courses, possède également des caméras pour éviter les vols. Retour au travail pour l'après- midi où une caméra est située dans le hall d'entrée de la société...Le soir, même chemin pour rentrer chez soi, avec des arrêts au distributeur automatique pour retirer de l'argent, sous l'œil d'une caméra, et à la boulangerie pour acheter son pain avec une caméra surveillant la caisse* »[1865].

Il est désormais difficile d'échapper aux caméras de surveillance qui sont souvent associées à des technologies et des services de reconnaissance faciale automatique, ayant atteint une efficacité et une fiabilité redoutable et vendus par des entreprises telles qu'Amazon. Cette dernière a développé un logiciel, Amazon Rekognition, disponible en se connectant sur sa plateforme AWS[1866], qui, selon l'entreprise, « *facilite l'ajout d'une analyse des images et des vidéos à vos applications. Vous fournissez simplement une image ou une vidéo à l'API*

[1864] *Cf.* p. 371 et 380.

[1865] CNIL, Communiqué de Presse du 21 juin 2012 « Vidéosurveillance/vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », p. 1 : https://www.cnil.fr/sites/default/files/typo/document/CNIL-DP_Video.pdf

[1866] Amazon Web Services (AWS), Commencez dès aujourd'hui à créer avec AWS : « *Que vous recherchiez des options de puissance de calcul, de stockage de bases de données, de diffusion de contenu ou d'autres fonctionnalités, AWS dispose des services nécessaires pour vous aider à créer des applications sophistiquées en améliorant la flexibilité, l'évolutivité et la fiabilité* » : https://aws.amazon.com/fr/?nc2=h_lg

Rekognition, et le service peut identifier les objets, les personnes, le texte, les scènes et les activités, ainsi que détecter tout contenu inapproprié. Amazon Rekognition fournit également une reconnaissance et une analyse faciales précises sur vos fichiers image et vidéo. Vous pouvez détecter, analyser et comparer des visages pour une grande variété de cas de vérification d'utilisateurs, de comptage de personnes et d'utilisation pour la sécurité publique »[1867].

Cette API propose ainsi, principalement, la détection de milliers d'objets, scènes et activités spécifiques, la reconnaissance faciale pour identifier une personne, l'analyse faciale pour analyser les attributs du visage, le suivi de trajectoire pour identifier des schémas ou modèles, la détection de contenus appropriés et la fourniture d'étiquettes détaillées permettant de contrôler précisément ce qui est autorisé ou non, la reconnaissance de célébrité, la recherche de personnes ou d'enfants disparus, la détection et la reconnaissance de textes au sein d'images ou à partir d'images[1868]. Rekognition peut être employée, selon l'entreprise, pour la sûreté publique et la sécurité, pour créer des bibliothèques aisément consultables avec des index de recherche précis, pour détecter automatiquement du contenu explicite ou suggestif ou non sécurisé, pour identifier et vérifier l'identité d'une personne ou encore pour analyser les sentiments d'une personne[1869]. À cet égard, l'entreprise indique que « *Amazon Rekognition peut détecter des émotions comme le bonheur, la tristesse ou la surprise sur des images de visages. Rekognition peut analyser des images en direct et envoyer les caractéristiques d'émotions à Redshift pour un rapport périodique sur les tendances pour chaque magasin* »[1870].

[1867] Amazon Web services (AWS), Amazon Rekognition - Ajoutez facilement l'analyse intelligente des images et des vidéos à vos applications : « *Amazon Rekognition est basé sur la même technologie d'apprentissage en profondeur éprouvée, hautement évolutive développée par les scientifiques de la vision par ordinateur d'Amazon pour analyser des milliards d'images et de vidéos par jour, et ne nécessite aucune expertise en apprentissage automatique. Amazon Rekognition est une API simple et facile à utiliser qui permet d'analyser rapidement toute image ou fichier vidéo stocké dans Amazon S3. Amazon Rekognition apprend toujours à partir de nouvelles données et nous ajoutons continuellement de nouvelles étiquettes et des fonctionnalités de reconnaissance faciale au service.* » : https://aws.amazon.com/fr/rekognition/

[1868] Amazon Web services (AWS), Amazon Rekognition - Ajoutez facilement l'analyse intelligente des images et des vidéos à vos applications, *Id.*

[1869] Amazon Web services (AWS), Amazon Rekognition - Ajoutez facilement l'analyse intelligente des images et des vidéos à vos applications, *Ibid.*

[1870] Amazon Web services (AWS), Amazon Rekognition - Ajoutez facilement l'analyse intelligente des images et des vidéos à vos applications, *Ibidem.*

En outre, parmi les clients de ce logiciel, cités par l'entreprise, se trouvent des entreprises du secteur public et privé, comme Motorola Solutions[1871], Wia[1872], Openinfluence[1873], Marinus Analytics[1874] ou Armed[1875], des services publics tels que C-Span[1876], voire des forces de l'ordre tels que le Washington County Sheriff Office[1877], qui en font unanimement la promotion. Des chercheurs et fonctionnaires de l'ACLU[1878] ont manifesté leur inquiétude quant à l'utilisation de ce logiciel, notamment par les autorités publiques, et ont dénoncé sa vente aux services de police et organismes gouvernementaux indiquant, *in fine*, que *« la documentation marketing de Rekognition a tout du petit guide de surveillance dans un régime autoritaire* »[1879].

Plusieurs autres cas d'utilisation des technologies de reconnaissance faciale dans divers autres domaines peuvent être recensés. Ainsi, plusieurs magasins ont désormais recours aux « EyeSee Mannequin » : des mannequins qui semblent bien ordinaires vu de l'extérieur avec leur cadre élancé en polystyrène, la taille et la pose improbable, mais à l'intérieur, ils ne constituent aucunement un simple "mannequin"[1880]. Selon l'entreprise qui les produit, « *thanks to Eye See*

[1871] Amazon Rekognition Customers – Customer use cases "Motorola Solutions": "*Motorola Solutions is a leading global provider of mission-critical communication infrastructure, devices, accessories, software and services.*": https://aws.amazon.com/fr/rekognition/customers/

[1872] Amazon Rekognition Customers – Customer use cases "Wia": "*Wia is where people and things go to talk. Their mission is to make it possible for anyone to connect anything to the Internet, creating the next generation of the physical web*", *Id.*

[1873] Amazon Rekognition Customers – Customer use cases "OpenInfluence": "*Open Influence is a market leader in the influencer marketing space. Their advanced technology solutions and award-winning services allow global brands and agencies to identify relevant influencers based on their campaign objectives, while effectively predicting and monitoring campaign performance.*", *Id.*

[1874] Amazon Rekognition Customers – Customer use cases "Marinus Analytics": "*Marinus Analytics provides law enforcement with tools, founded in artificial intelligence, to turn big data into actionable intelligence. The Marinus flagship software, Traffic Jam, is a suite of tools for use by law enforcement agencies on sex trafficking investigations*", *Ibid.*

[1875] Amazon Rekognition Customers – Customer use cases "Armed Data Fusion System": "*ARMED™ is dedicated to the development and integration of cutting-edge technology to combat acts of political violence, terrorism, organized criminal activities, and insider threats.*", *Ibid.*

[1876] Amazon Rekognition Customers – Customer use cases "C-Span": "*C-SPAN is a public service that provides gavel-to-gavel proceedings of the U.S. House of Representatives and the U.S. Senate, and to other forums where public policy is discussed, debated and decided—all without editing. With 3 network stations and 5 other video feeds, there is a lot of content that must be indexed and made searchable.*", *Ibid.*

[1877] Amazon Rekognition Customers – Customer use cases "Washington County Sheriff Office": "*The Washington County Sheriff Office is the primary first responders for 911 calls from citizens in urban and rural areas, and also provide other services countywide that support city police departments, including crime scene specialists, major crime investigators, and sex offender compliance checks.*", *Ibidem.*

[1878] American Civil Liberties Union (ACLU) is a non-profit organization founded in 1920: *"[…], the ACLU of today continues to fight government abuse and to vigorously defend individual freedoms including speech and religion, a woman's right to choose, the right to due process, citizens' rights to privacy and much more.*": https://www.aclu.org/about/aclu-history

[1879] S. CHINOY, « La reconnaissance faciale, impossible d'y échapper », Courrier International n° 1487, *loc.cit.,* p. 34.

[1880] Par ex., Bloomberg News, « Mannequins collect data on shoppers via facial-recognition software », The Washington Post, publié le 22 novembre 2012 : https://www.washingtonpost.com/business/economy/mannequins-collect-data-on-shoppers-via-facial-

Mannequin by Almax, mannequins have become smart: this product do not only display clothes and encourage the consumer to enter the store, but it also makes it possible to "observe" who is attracted by store windows and reveal important details about customers: age range, gender, ethnicity, dwell time. […]. Thanks to a complex biometrical facial analysis system, […], this special camera installed inside the mannequin's head analyzes the facial features of people passing through the front and provides statistical and contextual information useful to the development of targeted marketing strategies »[1881].

Par ailleurs, dans le cadre de la future mise en place du « porn block » au Royaume-Uni[1882], les sites pornographiques proposeront deux options numériques à leurs utilisateurs pour prouver leurs âges : « *The first involves setting up an encrypted account and uploading your passport, driving license or other ID document. This is a one-time signup – your documents will be digitally stored for future logins. The second option […] is to take a live selfie, using the selfie function on your smartphone or a webcam on your desktop computer. Yoti 'Age Scan' technology will scan your face and determine how old you look. If you pass the facial verification test, you'll be referred back to the porn website* »[1883].

En outre, certains veulent distinguer entre vidéosurveillance et vidéoprotection, cette dernière étant principalement employée dans le cadre de la sécurité et la sûreté nationales, or il est de l'avis du CESE que c'est « *un euphémisme qui a pour fin d'atténuer l'aspect intrusif de ce genre de dispositif […]* »[1884].

De nombreuses autres illustrations de ces technologies permettant d'émettre des avis, suggestions et recommandations peuvent être citées, à l'image des capteurs insérés dans les outils du *quantified self*, dans les montres intelligentes ou dans les *smart cities*, ou encore dans les smartphones entre autres : « *derrière l'omniprésence du vocable smart dans le marketing de l'innovation numérique se cache en réalité cette invasion des capteurs, des instruments d'acquisition de données et des outils d'analyse et d'aide à la décision qui en sont les*

---

recognition-software/2012/11/22/0751b992-3425-11e2-9cfa-e41bac906cc9_story.html?utm_term=.a149cdea7ecd ; et C. Lieber, «Your Favorite Stores Could Be Tracking You With Facial Recognition », Racked, publié le 22 mai 2018: https://www.racked.com/2018/5/22/17380410/facial-recognition-technology-retail

[1881] Almax-italy, EyeSee Mannequin: With Almax, craftsmanship, sustainability and innovation come together to revolutionize the fashion marketing: http://www.almax-italy.com/en-us/page/en_eyesee

[1882] S. GALLAGHER, "Porn Block: New Start Date Announced As 15 July Following Delay - Users will have to prove they are over 18 with a passport or driving licence", HuffPost UK, publié le 17 avril 2019: https://www.huffingtonpost.co.uk/entry/porn-block-new-start-date-announced_uk_5cb6fef0e4b082aab08f084c

[1883] S. GALLAGHER, "Porn Block: You'll Soon Be Able To Verify Your Age With A Selfie - But would you want to?", HuffPost UK, publié le 18 avril 2019: https://www.huffingtonpost.co.uk/entry/porn-block-verify-your-age-with-a-selfie_uk_5cb8330be4b081fd1693593c?guccounter=1

[1884] CESE – E. PERES, *Les données numériques : un enjeu d'éducation et de citoyenneté*, *op. cit.,* p. 45.

compléments obligatoires »[1885]. Les images et vidéos font donc l'objet de reconnaissances, les passants devant les magasins font l'objet d'identifications et d'analyses faciales, les capteurs saisissent les empreintes, la voix, les déplacements et ainsi de suite. Cet ensemble permet, *inter alia*, d'analyser les attributs des visages humains révélant de nombreuses informations, y compris sur les sentiments de la personne analysée, d'opérer une analyse vocale pour en dégager une multitude d'informations, la voix humaine contenant « *des informations pouvant être liées aux caractéristiques physiques, physiologiques, démographiques, médicales, environnementales et autres du locuteur* », explique un scientifique de l'université Carnegie-Mellon, « *les chercheurs découvrent ces micro-signatures et les utilisent pour le profilage* » indique-t-il[1886].

Les individus portent désormais sur eux les outils nécessaires pour une surveillance généralisée et continue facilitant la récolte d'attributs et de traits caractéristiques permettant de les agréger, les traiter et les utiliser au titre de l'amélioration du bien-être de ces mêmes individus. Autrement dit, « *soon we may have access to "always-on" surveillance technologies such as Google Glass that will not only record all of our public and private interactions in both public and private but also share the images and sounds with Google – thus making them available to businesses and governments as well* »[1887].

Toutes ces technologies produisent des données qui font, par la suite, l'objet de plusieurs traitements, multiples analyses et nombreuses utilisations mais ces données produites, sont-elles collectées avec le consentement des utilisateurs - producteurs desdites données ; vu le nombre de traitements qu'il est possible d'opérer simultanément, est-il possible de vérifier la véridicité ou la réalité de la finalité initialement annoncée par le responsable du traitement ; au

---

[1885] CNIL, Cahier IP Innovation & Prospective N° 02 « Le corps, Nouvel Objet Connecté : Du Quantified self à la M-Santé : Les nouveaux territoires de la mise en données du monde », E. Geffray (dir.), p. 17, citant également un extrait de B. Kasanoff et M. Hinshaw, "Smart Customers, Stupid Companies", 2012: " *Today, digital sensors can: monitor your tire pressure and avoid dangerous blowouts; analyze the gait of elderly citizens and warn of falls before they occur; follow the gaze of shoppers and identify which products they examine - but don't buy - in a store; monitor which pages readers of a magazine read or skip; float in the air over a factory and independently monitor the plant's emissions; detect impacts in the helmet of an athlete and make it impossible for them to hide potential serious blows to their brains; reveal when a dishwasher, refrigerator, computer, bridge, or dam is about to fail; trigger a different promotion as a new customer walks by a message board; analyze the duration and quality of your sleep; warn drivers that they are about to fall asleep; prevent intoxicated drivers from operating a motor vehicle; warn a person before he or she has a heart attack; detect wasted energy in both homes and commercial buildings; warn a parent or boss when anger is creeping into their voice, to help prevent them from saying or doing things they will later regret; tell waiting customers how far away the pizza delivery guy is from their house; analyze the movements of employees through a factory to detect wasted time and efforts; trigger product demonstrations or interactive manuals when a customer picks up or examines a product; congratulate an athlete when she swings a tennis racquet properly or achieves an efficient stride while running. What can they do tomorrow?*"

[1886] « Ce que votre voix dit de vous », Extraits de J. McCormick, « What AI Can Tell From Listening to You », The Wall street journal, publié le 1er avril 2019, Courrier International n° 1487, *Id*., p. 34.

[1887] S. VAIDHYANATHAN, *Anti-social media, op. cit.*, p. 71.

regard de l'étendue et de la facilité de circulation des flux de données, le régime de protection en matière de transfert des données, s'applique-t-il ? Il semble que pour améliorer le quotidien des personnes, de nombreuses atteintes à leurs droits et libertés doivent d'abord être entreprises pour accomplir cette amélioration *via* les avis, suggestions et recommandations, le tout possible grâce à une traçabilité et une surveillance continues.

L'exemple de l'identifiant unique, les cartes d'identités électroniques unifiées, Google ID, l'identifiant Facebook, n'en sont que quelques-uns parmi tant d'autres ; l'ensemble développé dans le but d'identifier et d'authentifier de manière certaine et sécurisée les personnes, en leur facilitant la tâche moyennant un seul identifiant visant à centraliser les identités. C'est la vision du projet lancé par Microsoft pour développer une identité Metasystem, « *a new layer of the Internet, an Identity Layer, that would complement the existing network layers to add a new kind of functionality* »[1888].

Ça ne serait pas un outil unique ou une technologie seule, *single-on*, mais plutôt un protocole permettant la mise en place d'un portefeuille virtuel d'informations d'identifications, similaire aux portefeuilles physiques habituels contenant tous les papiers d'identification[1889], mais plus efficace et plus fiable, ne pouvant jamais être "perdu" ou "volé" et facilitant les demandes d'identification et d'authentification. Cette « Identity Layer » est une infrastructure pour internet, porteuse de valeur dans beaucoup de domaines mais ce n'est pas de l'altruisme, « *there is important public value here, but private interest is driving the deployment of this public value* »[1890].

Il apparaît ainsi que cette nouvelle infrastructure contribue à l'architecture de surveillance et de contrôle ainsi qu'au capitalisme de surveillance, notamment compte tenu du fait que « *this*

[1888] L. LESSIG, *Code 2.0, op. cit.,* p. 50.

[1889] L. LESSIG, *Code 2.0, Id.,* p. 50 : *"[...]. You've got a wallet. In it is likely to be a driver's license, some credit cards, a health insurance card, an ID for where you work, and, if you're lucky, some money. Each of these cards can be used to authenticate some fact about you – again, with very different levels of confidence. The driver's license has a picture and a list of physical characteristics. That's enough for a wine store, but not enough for the NSA. The credit card has your signature. Vendors are supposed to use that data to authenticate that the person who signs the bill is the owner of the card. If the vendor becomes suspicious, she might demand that you show an ID as well. Notice the critical features of this "wallet" architecture. First, these credentials are issued by different entities. Second, depending upon their technology, they offer different levels of confidence. Third, I'm free to use these credentials in ways never originally planned or intended by the issuer of the credential. The Department of Motor Vehicles never coordinated with Visa to enable driver's license to be used to authenticate the holder of a credit card. But once the one was prevalent, the other could use it. And fourth, nothing requires that I show all my cards when I can use one. That is, to show my driver's license, I don't also reveal my health insurance card. Or to use my Visa, I don't also have to reveal my American Express card. These same features are at the core of what may prove to be the most important addition to the effective architecture of the Internet since its birth*."

[1890] L. LESSIG, *Code 2.0, Id.,* p. 52, où l'auteur raconte ainsi que « *"Microsoft's strategy is based on web services", Cameron described to me. "Web services are impossible without identity"* »

infrastructure could effectively answer the first question that regulability requires answering : Who did what where ? With an infrastructure enabling cheap identification wherever you are, the frequency of unidentified activity falls dramatically »[1891].

B. Science, innovation, prédiction et prévention

Le potentiel de la production et de l'utilisation croissantes des flux de données représente, au XXI[e] Siècle, une ressource majeure permettant le développement de nouvelles industries, de nouveaux procédés et de nouveaux produits et services, de manière inégalée. Alors que les activités économiques et sociales utilisent depuis longtemps les données, l'ampleur et l'influence des technologies de l'information et de la communication, qui permettent et facilitent l'exploitation économique des données, augmentent, comme il a pu être observé à travers cette étude, à un rythme extraordinaire et incomparable. La diminution constante et graduée des coûts et des frais le long de la chaîne de valeur des données[1892] a été un important vecteur de l'accroissement de la production et de l'utilisation des données, y compris de la migration accélérée des activités socioéconomiques vers internet et le cyberespace grâce à l'adoption étendue, de plus en plus généralisée, des services numériques dans un web de plus en plus participatif et interactif. Par conséquent, « *the resulting phenomenon – commonly referred to as "big data" – signals the shift towards a data-driven economy, in which data enhance economic competitiveness and drive innovation and equitable and sustainable development* »[1893].

À mesure que l'accès aux outils 'intelligents', comme les téléphones portables, les tablettes, les montres intelligentes, et d'autres appareils intelligents et objets connectés, s'amplifie, l'énorme capacité du web à habiliter la « production participative »[1894], le « crowd sourcing », les données sur les consommateurs et les utilisateurs de manière à accroître l'engagement civique ou la participation sociale, et à aider les citoyens et consommateurs dans leurs activités quotidiennes augmente. Dans le même temps, ces nouvelles sources hétérogènes de données,

[1891] L. LESSIG, *Code 2.0, Ibid.,* p. 53.
[1892] *Cf.* p. 135 et 422.
[1893] OECD, "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", OECD Digital Economy Papers, N° 222, OECD Publishing, Paris, 18 juin 2013 (DSTI/ICCP(2012)9/FINAL), p. 7 : http://dx.doi.org/10.1787/5k47zw3fcp43-en
[1894] Commission générale de terminologie et de néologie, Vocabulaire « tous domaines » : Production participative - Équivalent étranger : crowdsourcing : « *Définition : Mode de réalisation d'un projet ou d'un produit faisant appel aux contributions d'un grand nombre de personnes, généralement des internautes. Note : 1. On peut, par exemple, recourir à la production participative pour concevoir un logiciel ou pour élaborer une encyclopédie.*
2. On trouve aussi l'expression « production collaborative », JORF n°0179 du 5 août 2014, p. 12995, texte n° 91 ; disponible en ligne : https://www.legifrance.gouv.fr/affichJO.do?idJO=JORFCONT000029330499

la présence et la manifestation de nouveaux acteurs ayant accès aux données, et la facilité croissante de croisement, de mise en lien, et de transfert des données personnelles remettent, conjointement, en question l'efficacité concrète, pragmatique, des régimes de protection des données et de la vie privée existants.

En effet, l'économie des données paraît aujourd'hui être non seulement une source de croissance mais aussi une source à multiples tendances[1895], et la convergence de ces nombreuses tendances technologiques, computationnelles, sociales ou économiques, couplée avec l'augmentation des moyens et la réduction des frais de collecte, de circulation, de stockage et d'analyse des données induisent la production continue d'une énorme quantité de données pouvant être largement exploitée pour favoriser de nouvelles activités, de nouveaux modèles économiques, de nouveaux procédés, de nouvelles pratiques, mais aussi de nouveaux produits et services, au titre de l'innovation, de la science, de la protection, de la prévention ou encore de la prédiction pour améliorer le quotidien et le bien-être des individus.

De plus, l'augmentation du volume, de la vitesse et de la variété des données utilisées dans l'ensemble de l'économie, mais surtout l'accroissement de leur valorisation sociale et économique, contribuent au virage vers un modèle socioéconomique centré sur les données, l'exploitation des données étant porteuse d'une valeur ajoutée et innovante dans une variété d'opérations touchant de nombreux domaines, tels que la sphère du commerce, de la santé, du sport, des médias, de la politique, de la sécurité, de l'administration publique, du transport, de la recherche et de l'éducation, de la science ; rares sont les domaines échappant à la révolution numérique et au nouveau modèle socioéconomique désormais mis en œuvre.

Dans l'ensemble, la promesse du Big data réside, selon l'OCDE, dans un ou plusieurs des secteurs globaux suivants, découlant de l'exploitation des données, liés à l'innovation : une amélioration de la recherche et du développement (*data-driven Research & Development*) ; le développement de nouveaux produits, biens et services, en utilisant les données soit comme produit (*data products*) ou comme composante majeure d'un produit (*data-intensive products*) ; l'optimisation ou l'automatisation des processus de production ou de livraison (*data-driven processes*) ; l'amélioration du marketing *via* des publicités ciblées et des recommandations personnalisées ou autres types de discriminations liées au marketing (*data-driven marketing*), y compris le design de produits plus expérimental (*data-driven product design*) ; le développement de nouvelles approches d'organisation et de gestion ou l'amélioration

[1895] *Cf.* p. 149 et s.

significative des pratiques existantes (*data-driven organisation and data-driven decision making*)[1896].

Incités par tous ces avantages et par la masse de données disponible, de nouveaux produits et outils numériques ont fait surface envahissant dès lors le quotidien des individus, les surveillant ou les assistant continuellement. En effet, que ce soit pour déterminer un itinéraire, commander un livre, un repas ou un taxi, payer ses impôts ou remplir des formulaires administratifs, prendre un rendez-vous à la mairie ou à la préfecture, ou même pour trouver l'amour et l'âme sœur, ces outils et produits proposent de « *délester les humains de ce qu'il y a de plus mécanique dans leurs activités, assurant qu'ils les libèrent pour des tâches cognitives plus hautes, plus complexes ou plus ambitieuses* »[1897].

En outre, pour que ces outils et produits innovants soient effectivement utilisés quotidiennement, leurs conceptions et leurs designs prennent alors une place fondamentale, recourant à des nouvelles techniques et pratiques pour mettre au point des objets attrayants et marquants. La technique n'est jamais neutre, elle porte une potentialité dissimulée du monde, et correspond plutôt « *à une reconfiguration des possibles, naissant de la rencontre entre un travail de création d'un objet et sa prise en main par les individus. La conception des outils n'est donc pas un processus anodin, inerte du point de vue des utilisateurs ou même de la société. Les outils nous façonnent autant que nous les façonnons. L'avènement du numérique change surtout l'échelle à laquelle ce façonnage est susceptible de s'opérer* »[1898].

Il est vrai qu'à l'heure actuelle, les produits, outils et services peuvent être distribués et diffusés avec une rapidité extrême et ont tous la capacité de s'adapter, avec finesse, discrétion et efficacité, à leurs utilisateurs respectifs, disposant ainsi « *de toutes les caractéristiques pour pouvoir transformer la société en profondeur* »[1899]. Pour pouvoir assurer une telle diffusion, l'organisation en question doit alors générer des conceptions, des designs, ingénieux et des

---

[1896] OECD, "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", *Id.*, p. 14; où, dans le cadre du Data-driven Science and research, l'OCDE indique: "*Measurement has always been fundamental to science. The advent of new instruments and methods of data-intensive exploration has prompted some to suggest the arrival of "data-intensive scientific discovery", which builds on the traditional uses of empirical description, theoretical models and simulation of complex phenomena (BIAC, 2011). This could have major implications for how discovery occurs in all scientific fields. Some have challenged the usefulness of models in an age of massive datasets, arguing that with large enough data sets, machines can detect complex patterns and relationships that are invisible to researchers. The data deluge, it is argued, makes the scientific method obsolete, because correlations are enough (Anderson, 2008; Bollier, 2010)."* (Box 1)

[1897] D. CARDON, *À quoi rêvent les algorithmes*, *Id*., p. 101.

[1898] CNIL, Cahiers IP Innovation & Prospective N° 06 « La forme des choix : Données personnelles, design et frictions désirables », janvier 2019, p. 6-7 ; Disponible en ligne : https://www.cnil.fr/sites/default/files/atoms/files/cnil_cahiers_ip6.pdf

[1899] CNIL, Cahiers IP Innovation & Prospective N° 06 « La forme des choix : Données personnelles, design et frictions désirables », *Id.*, p. 7.

marques fortes dans l'esprit des personnes (d'où le développement de la réputation des individus ou de leurs marques, de celle des entreprises ou de leurs marques, produits et services, etc.[1900]), participant par conséquent à l'architecture esthétique du monde. Et « *cette esthétique, dont l'individu n'a que très peu conscience, est éminemment réfléchie. Un conditionnement via le design préfigure tout ce que l'individu manipule ou visualise dans l'univers numérique* », et les géants du web l'ont très bien compris[1901]. Ces derniers se livrent conséquemment à une compétition acharnée visant à attirer l'attention des utilisateurs[1902], à personnaliser leurs expériences et à leur faire des recommandations et suggestions personnalisées, « *à infléchir le plus subtilement et le plus substantiellement leurs conduites, des loisirs au politique* »[1903].

Par ailleurs, la révolution numérique et les opportunités d'innovation qui l'accompagnent touchent également le secteur de la sécurité, que ce soit la sécurité du réseau, l'identification et l'authentification sécurisée, la sécurité des transports ou la vigilance des lieux, au nom de la protection, de la prévention ou de la prédiction. À cet égard, de nombreuses stratégies d'identification et d'authentification ont été déployées, au nom de la sécurité, pour récupérer plus de données. Cela s'est manifesté à travers la surveillance de plus en plus accrue du trafic frontalier, des espaces publics, et de la circulation du flux sur les réseaux de communication au titre de la vigilance, nécessaire pour assurer la protection des lieux et des personnes ; de même, au regard de l'ampleur (et parfois de la sensibilité) des informations échangées sur l'ensemble du réseau numérique, la demande de sécurité fondée sur l'authentification contre les virus, les logiciels espions ou les spams, est devenue une puissante force motrice du développement de la fonctionnalité des systèmes de confiance et des produits de sécurité dans les secteurs public et privé[1904].

En outre, la récolte des données au nom de la vigilance et de la protection peut même s'opérer d'une manière stratégiquement directe, soit moyennant les affiches signalant des messages tels que « soyez vigilants, si vous voyez quelque chose de suspect signalez-le à un agent », beaucoup de personnes transmettant volontairement pas mal d'informations, soit *via* une technique plus indirecte cherchant à inculquer des croyances et des habitudes appropriées sur la gestion des informations personnelles : « *the emerging regimes of pervasively distributed*

[1900] *Cf.* p. 120 et s.
[1901] CNIL, Cahiers IP Innovation & Prospective N° 06 « La forme des choix : Données personnelles, design et frictions désirables », *Id.*, Édito, I. Falque-Pierrotin, p. 1.
[1902] *Cf.* p. 575.
[1903] CNIL, Cahiers IP Innovation & Prospective N° 06 « La forme des choix : Données personnelles, design et frictions désirables », *Ibid.*, Édito, I. Falque-Pierrotin, p. 1.
[1904] J. E. COHEN, *Configuring the Networked Self, op. cit.,* p. 167-169.

security and authentication depend on the ready availability of large quantities of personal information. It is important therefore, that individuals continue to provide those regimes with the information that they require. Nurturing the optimal blend of vigilance and compliance requires educating members of the public to understand their own disclosures as essential to the purchase of both security and convenience »[1905].

Dès lors, il semble qu'au nom de l'innovation, du développement, de la science, de la protection, de la prévention ou de la prédiction, les individus laissent des traces et cèdent continuellement des données pour leurs propres bien et intérêt. Or, au nom de ces mêmes objectifs, de nombreuses atteintes à plusieurs droits et libertés fondamentales sont finalement observées, la plupart étant inconnues du public, comme de nombreux cas, susmentionnés dans cette étude, le montrent. Il suffit de penser à l'affaire de Cambridge Analytica[1906] impliquant Facebook qui collecte une large variété de données concernant ses utilisateurs, provenant de multiples sources (directes ou indirectes) et comprenant un peu plus de 98 sortes et catégories différentes comme l'appartenance ethnique, la religion, l'appartenance politique, la valeur du patrimoine, la valeur de la résidence, la situation familiale, le nombre d'enfants, le nombre d'emprunts contractés, la date d'un achat effectué, et ainsi de suite[1907]. En théorie, Facebook récolte et analyse l'ensemble de ces données pour améliorer ses services et mieux cibler les publicités et les recommandations ; en pratique, les faits et évènements ont révélé autre chose, une autre finalité, à savoir la vente de leurs données, et de leurs profils et dossiers uniformisés, pour son propre gain.

En vue d'accomplir ces divers objectifs, l'entreprise recourt à des algorithmes computationnels puissants ainsi qu'à des pratiques telles que la psychométrie, précédemment vue, pour analyser, ficher, catégoriser, divulguer des tendances communes, stimuler, inculquer, infléchir le comportement, et ainsi de suite. La plupart des gens pensent que les données sont neutres, ne reflétant pas de biais intrinsèques ; c'est le cas du "fil d'actualité" de Facebook, par exemple, au regard duquel les gens pensent que Facebook n'intervient pas dans ce qui s'affiche, « *alors que c'est exactement ce que fait son algorithme propriétaire* »[1908]. C'est donc finalement une personne ou un groupe de personnes, ayant conçu l'algorithme en question, qui accomplissent la tâche en l'abordant avec « *tous les biais et les a priori culturels qui font de nous ce que nous*

[1905] J. E. COHEN, *Configuring the Networked Self, Id.,* p. 170, et l'auteur indique "*[…]. The inevitable and often spectacular failures of systems put in place to ensure commercial security tend to be understood as demonstrating the need for still more disclosure so that more tightly controlled authentication can succeed."*

[1906] *Cf.* p. 375 et 385-389.

[1907] S. HALPERN, « Tous fichés, Tous manipulés », *In* Books – L'actualité à la lumière des livres, Hors-série N° 14, *Internet : pièges et maléfices*, Ed. Books, Coll. Books Le Magazine, décembre 2018-Janvier 2019, p. 47.

[1908] S. HALPERN, « Tous fichés, Tous manipulés », *Id.*, p. 48.

sommes. [...]. Ce n'est pas de la science, c'est de la présomption. Et c'est gravé dans l'algorithme »[1909].

De même, en ce qui concerne les publicités qui surgissent sur les sites fréquentés, sur les navigateurs et moteurs de recherche, ou encore sur les pages Facebook, les individus pensent qu'elles sont là parce qu'une entreprise cherche à leur vendre un service ou un produit en fonction d'une page web visitée, d'une recherche effectuée, d'un click opéré ou d'un mail envoyé, ce qui constitue en réalité une des raisons, puisqu'elles sont aussi là « parce que nous habitons dans tel quartier, fréquentons tel type de personne ou que nous avons été repérés par des voies obscures grâce à une représentation pointilliste de notre vie. Et nous n'imaginons certainement pas que nous voyons ces pubs parce qu'un algorithme a établi que nous sommes un loser, une proie facile ou que nous appartenons à tel ou tel groupe ethnique »[1910].

Toute trace, tout gisement, toute information fait l'objet d'une récolte et d'une convoitise en vue de poursuivre des objectifs liés à l'innovation, à la prévention, à la protection, instaurant par là même une dynamique consumériste poussant l'individu à divulguer toujours plus d'informations, sans réellement discerner le niveau ou l'ampleur des menaces que cela pourrait engendrer. Et ces dynamiques et infrastructures ne s'arrêtent pas au monde de Facebook ou des GAFAM, il suffit de penser à la montre Fitbit qui capte et récolte une grande quantité d'informations sur ses utilisateurs tout en s'adaptant à leurs besoins, mise en place au nom de l'innovation, de la science, et de l'amélioration de la santé[1911]. En effet, « *les infrastructures des big data cherchent à guider sans contraindre, à orienter sans obliger. Elles constituent un exemple typique de ce que Cass Sunstein appelle les nudges, ces outils du « paternalisme libertaire » qui, par défaut, suppléent les choix des individus en les persuadant qu'ils agissent au mieux de leurs intérêts* »[1912].

Ainsi, comme le souligne le Professeur Cardon, une économie des sciences de l'homme se met en œuvre, porteuse d'une multitude de capacités et d'applications : « *Dans un article qui a fait grand bruit, Chris Anderson, un des gourous de la Silicon Valley, a annoncé la « fin de la théorie ». Les calculateurs des big data, explique-t-il, peuvent désormais chercher des corrélations sans se préoccuper d'avoir un modèle qui leur donne une explication. Les données massives et les mathématiques permettraient de faire l'économie des sciences de l'homme* »[1913].

[1909] S. HALPERN, « Tous fichés, Tous manipulés », *Ibid.*, p. 48.
[1910] S. HALPERN, « Tous fichés, Tous manipulés », *Ibidem*, p. 49.
[1911] *Cf.* p. 408 et s.
[1912] D. CARDON, *À quoi rêvent les algorithmes*, *Id*., p. 101.
[1913] D. CARDON, *À quoi rêvent les algorithmes*, *Ibid*., p. 51.

§2. La portée de l'économie des sciences de l'homme

L'économie des sciences de l'hommes élaborée dans l'environnement numérique actuel s'exprime, principalement, par l'essor du pouvoir des méthodes d'apprentissage automatique (A), mais aussi par celui du pouvoir des corrélations automatiques inférées (B).

A. Le pouvoir des méthodes d'apprentissage automatique

À mesure que les données prolifèrent et se démultiplient dans les organisations, il s'est avéré de plus en plus nécessaire de comprendre leurs implications et incidences moyennant la production de connaissances. La production de connaissances par une veille stratégique[1914], et des renseignements stratégiques, opérationnels et analytiques, est disponible depuis bien longtemps, exigeant cependant l'aide d'analystes spécialisés et formés. Le nombre d'analystes limitait alors les connaissances dont les décideurs d'une organisation avaient besoin, et sans accès facile à des données statistiques et analytiques, ces spécialistes se fiaient souvent à leurs expériences et intuitions. Pire encore, la complexité et les frais des technologies antérieurement disponibles rendaient difficiles la recherche et l'analyse des données requises pour produire des connaissances et informations. Au cours des dernières décennies, de nombreuses technologies ont été mises en œuvre afin de démocratiser la production d'informations et de connaissances, y compris des programmes et paquets statistiques interactifs, des tableaux et feuilles de calcul, des outils d'analyse visuelle faciles à manipuler et ainsi de suite, qui, finalement, se sont avérés insuffisants à l'ère du Big data et des avancées technologiques effectuées depuis. L'augmentation rapide de la quantité et du volume des données et de la puissance des algorithmes de traitement a souligné la nécessité d'opérer de nouvelles interventions en vue d'obtenir des niveaux de connaissance et d'information encore inexplorés.

Les méthodes et les technologies antérieures n'étant capables de générer que des analyses descriptives et des statistiques sur le passé, ne convenaient de ce fait plus aux nouvelles avancées technologiques et aux nouveaux modèles socioéconomiques qui souhaitaient, de plus

---

[1914] H. LESCA, *Veille stratégique : concepts et démarche de mise en place dans l'entreprise,* Guides pour la pratique de l'information scientifique et technique, Ministère de l'Éducation Nationale, de la Recherche et de la Technologie, 1997 (27 p.), p. 1 : « *La veille stratégique est le processus collectif continu par lequel un groupe d'individus traquent, de façon volontariste, et utilisent des informations à caractère anticipatif concernant les changements susceptibles de se produire dans l'environnement extérieur de l'entreprise, dans le but de créer des opportunités d'affaires et de réduire des risques et l'incertitude en général. Parmi ces informations figurent des signes d'alerte précoce […]. Finalement, l'objectif de la veille stratégique est de permettre d'agir très vite et au bon moment. Les anglo-saxons utilisent les expressions Environmental Scanning et Competitive Intelligence pour désigner des concepts très voisins.*
Rappelons que, dans le modèle de la prise de décision de H. Simon (Prix Nobel), la veille stratégique se situe dans la phase dite « intelligence de l'environnement de l'entreprise ». » ; Disponible en ligne : http://www.veille-strategique.org/docs/plaquette-20418.pdf

en plus, l'élaboration de modèles de prédiction et de prévision générant des informations sur ce qui pourrait arriver dans le futur à leur entreprise, leur produit, leur rentabilité, leur capital, leur investissement, etc., mais aussi des normes, pratiques, et statistiques prescriptives stimulant les résultats commerciaux et la gestion de leur organisation. Ces objectifs et souhaits sont dorénavant largement atteignables grâce au développement de l'analyse prédictive, des algorithmes puissants et sophistiqués mais surtout grâce à l'automatisation et les techniques d'apprentissage automatique. Technique statistique et computationnelle particulière, « *l'apprentissage automatique, « machine learning », a bouleversé la manière dont les calculs pénètrent nos sociétés* »[1915].

En effet, les développements et progrès technologiques ont permis de mettre en place des algorithmes exécutant automatiquement des tâches répétitives qui impliquent des traitements de données et des calculs complexes, qui autrement, effectuées par des individus, seraient trop longues et coûteuses. Les derniers progrès en matière d'apprentissage automatique ont, cependant, « *porté les algorithmes à un niveau supérieur permettant aux ordinateurs de résoudre des problèmes complexes, de faire des prévisions et de prendre des décisions de manière plus efficiente que les êtres humains, […]* »[1916].

Le concept d' « algorithme » est fort ancien, précédant la création des ordinateurs, se référant à « une série de règles à appliquer pour accomplir une tâche particulière, une séquence logique permettant d'obtenir un certain résultat à partir d'un intrant donné, ou encore une capacité de donner aux informations reçues une forme nouvelle afin de pouvoir être utilisées en vue des stades ultérieurs du fonctionnement du système »[1917]. Dans cette perspective, il semble alors que « *la volonté d'étendre à la société toute entière ce que l'on imagine être une organisation scientifique du travail* », qui a été le lot du capitalisme, n'a pas disparu de nos jours, mais a simplement changé de forme : « *son modèle n'est plus celui des lois de la physique classique, mais celui des algorithmes de l'informatique. L'organisation du travail* [est désormais conçue] *comme un système programmable faisant communiquer entre elles des unités capables de rétroagir aux signaux qu'elles reçoivent en fonction de cette programmation. La révolution numérique va ainsi de pair avec celle qui se donne à voir en matière juridique, où l'idéal d'une gouvernance par les nombres tend à supplanter celui du gouvernement par les lois* »[1918].

[1915] D. CARDON, *À quoi rêvent les algorithmes*, *Id.*, p. 33.

[1916] OCDE, « Algorithmes et ententes - Note d'information du Secrétariat », juin 2017 (DAF/COMP(2017)4), p. 7 ; Disponible en ligne : https://one.oecd.org/document/DAF/COMP(2017)4/fr/pdf

[1917] OCDE, « Algorithmes et ententes - Note d'information du Secrétariat », *Id.,* p. 6-7, et A. SUPIOT, *La gouvernance par les nombres, op. cit.,* p. 215-216.

[1918] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 216 ; et, *Cf.* p. 498 et s.

À l'heure actuelle, il est évident, comme il a été précédemment vu, que les algorithmes envahissent le quotidien des personnes, sur les réseaux sociaux, les téléphones et ordinateurs portables, les rues, transports et bâtiments, pour déterminer l'éligibilité à un travail, à un crédit ou à une assurance, ou même pour répartir les futurs bacheliers dans les universités tel que c'est le cas avec Parcoursup ; et l'ensemble de ces algorithmes employés ont été améliorés grâce à l'apprentissage automatique. Souvent associée au domaine de l'intelligence artificielle, la technique d'apprentissage automatique fournit, selon A. Samuel, « aux ordinateurs/machines la capacité d'apprendre sans être explicitement programmés »[1919].

De nos jours, trois grandes catégories de modes d'apprentissage peuvent être relevées : *l'apprentissage supervisé*, dans lequel l'algorithme se sert d'un échantillon de données étiquetées pour apprendre une règle générale de réaffectation des intrants en extrants ; *l'apprentissage non supervisé*, où l'algorithme doit identifier lui-même la structure dissimulée et les motifs permettant de regrouper les données non étiquetées ; et, *l'apprentissage par renforcement* grâce auquel l'algorithme peut exécuter une tâche dans un environnement dynamique, comme la participation à un jeu[1920] ou la conduite d'un véhicule, et apprendre par essai et erreur[1921]. Existe enfin une sous-catégorie de l'apprentissage automatique, l'apprentissage profond (*deep learning*) qui permet à un ordinateur de construire des concepts ou représentations complexes à partir de concepts ou représentations plus simples et parvient à modéliser des abstractions puissantes à partir de données ; « *specifically, it is a type of machine*

[1919] A. L. SAMUEL, "Some Studies in Machine Learning Using the Game of Checkers", *In* IBM Journal, Vol. 3, N° 3, July 1959 (p. 535-554), p. 548 : l'auteur se base sur les techniques d'apprentissage par mémorisation et par généralisation (*rote learning* et *learning by generalization*) pour tester l'efficacité et la réussite de son système, et en conclut que « *one can say with some certainty that it is now possible to devise learning schemes which will greatly outperform an average person and that such learning schemes may eventually be economically feasible as applied to real-life problems* » :
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.368.2254&rep=rep1&type=pdf

[1920] Pour illustration : « *Libratus est un programme d'apprentissage automatique conçu […] pour jouer une version complexe du poker, le ramponneau sans limites (ou no limit Texas hold'em). Afin de maîtriser la stratégie du poker, l'algorithme sur lequel repose Libratus s'appuie sur une méthode d'apprentissage par renforcement […]. Libratus a été testé en janvier 2017 dans un tournoi où il a joué en tout 120 000 mains de poker contre les premiers joueurs mondiaux. Tout au long de ce tournoi, la machine jouait contre des adversaires humains pendant la journée puis, mettant à profit les nouvelles données recueillies, améliorait sa stratégie pendant la nuit en corrigeant les faiblesses détectées par les autres joueurs. La machine a obtenu un succès sans précèdent, l'emportant avec un total de 1.776.250 USD en jetons contre tous les autres joueurs, qui étaient dans le rouge à la fin du tournoi. […]. En tant que jeu dynamique présentant des imperfections informationnelles et des millions de combinaisons de cartes possibles, le poker reflète partiellement la complexité et l'incertitude des problèmes du monde réel. La capacité de Libratus à procéder à des raisonnements complexes dans des situations aléatoires, à interpréter les informations reçues mais susceptibles de l'induire intentionnellement en erreur et à anticiper les conséquences de ses actes sur les décisions des autres joueurs suggère en particulier que l'IA pourra être utilisée dans le contexte d'interactions « humaines » plus complexes, ainsi que dans des processus décisionnels.* » : OCDE, « Algorithmes et ententes - Note d'information du Secrétariat », *Id.,* p. 9 (Encadré 1).

[1921] OCDE, « Algorithmes et ententes - Note d'information du Secrétariat », *Ibid.,* p. 7-8.

learning, a technique that enables computer systems to improve with experience and data. […]. Deep learning is a particular kind of machine learning that achieves great power and flexibility by representing the world as a nested hierarchy of concepts, with each concept defined in relation to simpler concepts, and more abstract representations computed in terms of less abstract ones »[1922]. Ainsi, l'apprentissage profond permet aux machines d'apprendre avec une plus grande rapidité et une plus grande exactitude que l'apprentissage automatique conventionnel qui, néanmoins, demeure pertinent et efficace. En revanche, il est utile de noter que « *malgré les progrès obtenus récemment en ce domaine et l'énorme capacité potentielle de l'apprentissage profond à résoudre les problèmes les plus complexes, en l'absence d'extraction de caractéristiques, il est impossible de savoir quels critères ou quelles informations ont été utilisés par l'algorithme pour convertir les intrants en extrants. Autrement dit, quelle que soit la qualité des résultats obtenus, les algorithmes d'apprentissage profond ne permettent pas aux programmeurs de connaître les modalités du processus de décision ayant conduit à ces résultats* »[1923].

L'analyse prédictive, moyennant ces méthodes d'apprentissage automatique, peut, à l'époque de la société de l'information, être entreprise en grande partie de manière automatisée, ne nécessitant plus vraiment d'intervention humaine. En effet, bon nombre de tâches clés, requises pour l'apprentissage automatique, y compris la préparation des données, l'ingénierie des caractéristiques, l'ingénierie des fonctions, ou la transformation des variables, peuvent être effectuées par les machines et outils informatiques. Ces techniques prédictives ont, par exemple, été ajoutées à la plupart des algorithmes mesurant la popularité, la notoriété ou l'e-réputation[1924], ou à ceux effectuant les suggestions et recommandations personnalisées[1925]. L'algorithme apprend ainsi en comparant un profil à d'autres ayant accompli la même action ou ayant adopté le même comportement, pour déterminer, de façon probabiliste, l'action ou le comportement futur du profil analysé. Il s'agit donc « *de calculer le profil de l'utilisateur à partir des traces de ses activités, en développant des techniques d'enregistrement qui collent au plus près de ses gestes* »[1926], l'ambition ultime de cette technique d'apprentissage étant de personnaliser les calculs à partir des données et traces des individus en vue de « *les inciter à*

[1922] I. GOODFELLOW, Y. BENGIO et A. COURVILLE, *Deep learning*, MIT Press, 2016, p. 8; disponible en ligne: http://www.deeplearningbook.org ou http://www.deeplearningbook.org/contents/intro.html
[1923] OCDE, « Algorithmes et ententes - Note d'information du Secrétariat », *Ibid.,* p. 10.
[1924] *Cf.* p. 120 et s.
[1925] *Cf.* p. 430.
[1926] D. CARDON, *À quoi rêvent les algorithmes*, *op. cit*., p. 34.

agir dans telle direction plutôt que dans telle autre »[1927]. Dans cette perspective, le pouvoir de prédiction des machines, moyennant les techniques d'apprentissage automatique, qu'elles soient conventionnelles ou profondes, mis en œuvre dans les différents secteurs d'activités assoit la pérennisation du capitalisme de surveillance[1928].

En ce sens, grâce à ces techniques et méthodes, les techniques de reconnaissances faciale et vocale ont également fait de grands progrès à l'aide du *deep learning* ; Google a pu perfectionner Google Translate, son logiciel de traduction ; de même pour la structure de Facebook, dans laquelle « *its chief form of governance is machine learning* »[1929], laissant le tout s'autogérer et s'autocontrôler en dépit des conséquences que ceci pourrait entraîner. En outre, il est utile de noter que, pour apprendre, les machines ont besoin d'une vaste quantité de données, qui étaient rares et insuffisantes à l'origine des développements des machines « intelligentes ». À l'ère du Big data où l'énorme fait la norme, ce problème est résolu et le progrès des algorithmes, logiciels, ou outils intelligents, se fait progressivement sentir ; cela dit, « *machine learning is only as effective as the "training data" that go into it* »[1930].

Par ailleurs, l'Union européenne manifeste un intérêt pour ces nouvelles techniques et tendances et a, en ce sens, adopté en 2018 une stratégie sur l'Intelligence Artificielle « *pour favoriser le développement et l'utilisation de l'IA en Europe* »[1931]. Une coopération plus étroite et plus efficace entre les États membres, la Norvège, la Suisse et la Commission européenne est ainsi envisagée dans des domaines d'action essentiels, tels que l'accroissement des « investissements par l'intermédiaire de partenariats » du secteur public et privé, la création des « espaces européens des données » afin de « rendre davantage de données disponibles » et « permettre un partage des données transfrontières fluide », ou cultiver les talents en favorisant le talent, les compétences et l'apprentissage tout au long de la vie »[1932]. Selon la Commission, l'intelligence artificielle est une réalité présente désormais partout dans nos quotidiens, rendant la vie des individus plus facile en les aidant à organiser leurs journées, ou en les transportant et les conduisant moyennant un véhicule automatique, ou en leur suggérant des chansons ou des restaurants qui leur plairont, et, « *beyond making our lives easier, AI is helping us to solve some*

[1927] D. CARDON, *À quoi rêvent les algorithmes*, *Id*., p. 33.
[1928] *Cf.* p. 371 et 380.
[1929] S. VAIDHYANATHAN, *Anti-social media*, *op. cit.*, p. 88.
[1930] S. VAIDHYANATHAN, *Anti-social media*, *Id*, p. 75.
[1931] Commission européenne, Communiqué de Presse « Intelligence artificielle », Bruxelles, 7 décembre 2018 : https://ec.europa.eu/commission/news/artificial-intelligence-2018-dec-07_fr
[1932] Commission européenne, Communiqué de Presse « Intelligence artificielle », *Id.*

of the world's biggest challenges: from treating chronic diseases or reducing fatality rates in traffic accidents to fighting climate change or anticipating cybersecurity threats »[1933].

L'Union souhaite ainsi exploiter, en premier lieu, le potentiel de l'intelligence artificielle pour des secteurs principalement d'intérêts publics, comme la santé, les transports, la sécurité ou l'énergie, et a, par conséquent, prévu de consacrer « *au moins 20 milliards d'euros d'investissements publics et privés à la recherche et l'innovation dans le domaine de l'IA d'ici à la fin de 2020 et plus de 20 milliards d'euros par an d'investissements publics et privés au cours de la décennie suivante* »[1934]. La coopération entre les États membres permettrait alors, entre autres, de capitaliser sur le marché unique numérique européen, ou de tirer profit d'une masse de données industrielles, de recherche et du secteur public, qui peuvent être déverrouillées pour alimenter les systèmes d'IA. À cet égard, il est prévu que, « *in parallel to this Communication, the Commission is taking action to make data sharing easier and to open up more data – the raw material for AI – for re-use* »[1935].

En parallèle, fut établie à Montréal la Déclaration pour un développement responsable de l'intelligence artificielle par une équipe scientifique pluridisciplinaire et interuniversitaire qui affirme que, « *pour la première fois dans l'histoire de l'humanité, il est possible de créer des systèmes autonomes capables d'accomplir des tâches complexes que l'on croyait réservées à l'intelligence naturelle : traiter de grandes quantités d'informations, calculer et prédire, apprendre et adapter ses réponses aux situations changeantes, et reconnaître et classer des objets. En raison de la nature immatérielle de ces tâches qu'ils réalisent, et par analogie avec l'intelligence humaine, on désigne ces systèmes très divers par le terme général d'intelligence artificielle* », qui certes « constitue un progrès scientifique et technologique majeur » mais « présente cependant des défis éthiques et des risques sociaux majeurs »[1936]. En conséquence, la déclaration prévoit des principes tels que le principe de bien-être, de respect de l'autonomie,

---

[1933] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Artificial Intelligence for Europe", Bruxelles, 25 avril 2018, COM(2018) 237 final, p. 2, et la Commission définit l'intelligence artificielle comme suit "*Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications). We are using AI on a daily basis, e.g. to translate languages, generate subtitles in videos or to block email spam.*": https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

[1934] Commission européenne, Communiqué de Presse « Intelligence artificielle », *Ibid.*

[1935] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Artificial Intelligence for Europe", *Id.*, p. 3.

[1936] Déclaration de Montréal – IA Responsable, une initiative de l'Université de Montréal : https://www.declarationmontreal-iaresponsable.com/la-declaration

de protection de l'intimité et de la vie privée, ou d'inclusion de la diversité, qui reposent « *sur l'idée commune que les êtres humains cherchent à s'épanouir comme êtres sociaux doués de sensations, d'émotions et de pensées, et qu'ils s'efforcent de réaliser leurs potentialités en exerçant librement leurs capacités affectives, morales et intellectuelles* »[1937].

Essentiellement, les ordinateurs et les machines exécutent des algorithmes informatiques dont l'apprentissage automatique est une catégorie particulière leur permettant, *de facto*, d'apprendre et de s'auto-modifier pour s'améliorer. Par conséquent, indique Schneier, cryptologue, spécialiste en sécurité informatique et professeur adjoint à la Harvard Kennedy School[1938], il est impossible pour les individus de comprendre ce que ces algorithmes font ou comment ils obtiennent leurs résultats, mais, dans l'ensemble, les individus ne s'en plaignent pas et semblent en être ravis, préférant le système de diagnostic d'apprentissage automatique le plus précis au technicien humain, bien qu'il ne puisse se justifier ou s'expliquer ou être tenu pour responsable : « *for this reason, machine-learning systems are becoming more pervasive in many areas of society. For the same reasons, we're allowing algorithms to become more autonomous* [… and] *to have physical agency. This is what I was thinking about when I described the Internet+ as an Internet that can affect the world in a direct physical manner. When you look around, computers with physical agency are everywhere, from embedded medical devices to cars to nuclear power plants* »[1939].

Les risques et conséquences que le développement et l'évolution de ces algorithmes d'apprentissage automatique, de plus en plus autonomes, peuvent entraîner sont considérables, mais sont déjà omniprésents selon Schneier, sans avoir besoin d'attendre l'avènement de la robotique ou d'intelligences artificielles plus modernes et sophistiquées, la crainte vis-à-vis de celles-ci devant être considérée plutôt comme un miroir de nos propres sociétés que comme un présage de l'avenir ; « *AI and intelligent robotics are the culmination of several precursor technologies, like machine-learning algorithms, automation, and autonomy. The security risks from those precursor technologies are already with us, and they're increasing as the*

[1937] Déclaration de Montréal – IA Responsable, *Id.*

[1938] "*Schneier is a fellow at the Berkman Klein Center for Internet & Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an Advisory Board Member of the Electronic Privacy Information Center and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.*": About Bruce Schneier – Blog: https://www.schneier.com/blog/about/, et B. Schneier, Adjunct Lecturer in Public Policy, Harvard Kennedy School – John F. Kennedy School of Government: https://www.hks.harvard.edu/faculty/bruce-schneier

[1939] B. SCHNEIER, *Click here to kill everybody, op. cit.,* p. 83, où l'auteur donne un exemple: "*DeepPatient is a machine-learning system that has surprising success at predicting schizophrenia, diabetes, and some cancers – in many cases performing better than expert humans. But although the system works, no one knows how, even after analyzing the machine-learning algorithm and its results*."

technologies become more powerful and more prevalent. So, while I am worried about intelligent and even driverless cars, most of the risks are already prevalent in Internet-connected drivered cars. And while I am worried about robot soldiers, most of the risks are already prevalent in autonomous weapons systems »[1940].

Or, l'OCDE de son côté avance, en conclusion, que « malgré les risques évidents que les algorithmes posent […], il s'agit d'un domaine encore extrêmement complexe et incertain où aussi bien l'absence d'intervention qu'une règlementation excessive pourrait avoir un coût élevé pour la société, compte tenu en particulier des avantages potentiels que l'on peut attendre des algorithmes »[1941], vision similaire à celle manifestée par l'Union européenne.

B. Le pouvoir des corrélations automatiques inférées

Une autre secousse est venue modifier les méthodes statistiques et de calcul conventionnelles, à savoir l'abandon progressif de la recherche séculaire et pérenne du lien de causalité, introduisant ainsi le passage de la causalité à la corrélation qui ne requiert plus une hypothèse ou une théorie particulière pour fournir une justification. Cela signale, selon certains auteurs, la fin de la théorie et de la méthode scientifique qui cherchait toujours un modèle théorique en tentant de le falsifier ou de le démontrer, et la mise à jour de la célèbre citation de G. Box, qui stipulait dans les années 70-80, « *essentially, all models are wrong, but some are useful* »[1942] devenue, avec le directeur de recherche de Google en 2008, « *all models are wrong, and increasingly you can succeed without them* »[1943]. Aujourd'hui, le pouvoir des données disponibles en masse et celui du calcul et des nombres semblent être suffisants pour justifier une analyse de corrélations exempte de théorie, hypothèse ou modèle, « *this is a world where massive amounts of data and applied mathematics replace every other tool that might be brought to bear. Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is*

[1940] B. SCHNEIER, *Click here to kill everybody, Id.,* p. 86-87.
[1941] OCDE, « Algorithmes et ententes - Note d'information du Secrétariat », *Ibid.,* p. 62.
[1942] G. E. P. BOX, "Science and Statistics", *In* Journal of the American Statistical Association, Vol. 71, N° 356, Décembre 1976 (p. 791-799), p. 792: Disponible en ligne: http://www-sop.inria.fr/members/Ian.Jermyn/philosophy/writings/Boxonmaths.pdf ; G. E. P. BOX et N. R. DRAPER, *Empirical Model Building and Response Surfaces*, John Wiley & Sons, New York, 1987, p. 74 et p. 424.
[1943] P. NORVIG, "Practice Makes Perfect: How Billions of Examples Lead to Better Models", 2008 O'Reilly Emerging Technology Conference, March 2008: https://conferences.oreilly.com/et2008/public/schedule/detail/1778; Cité par C. ANDERSON, "The end of theory: The Data deluge makes the scientific method obsolete", Wired, publié le 23 juin 2008: https://www.wired.com/2008/06/pb-theory/

they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves »[1944].

L'analyse de données existe depuis des millénaires, les humains ayant toujours tenté d'analyser les informations et les données se trouvant à leur disposition pour diverses raisons, comme la gestion, le suivi, les statistiques ou l'étude des risques, alors même qu'à l'ère analogique, la collecte et l'analyse de telles données étaient extrêmement coûteuses et chronophages. De façon générale, la méthode scientifique repose sur des hypothèses vérifiables émettant une théorie ou un modèle qui pourra ensuite être testé, et les expériences confirment ou infirment les modèles théoriques émis. Les scientifiques étaient alors formés pour reconnaître que la corrélation n'est pas une causalité, qu'aucune conclusion ne doit être tirée simplement sur la base d'une corrélation entre deux éléments, qui pourrait s'avérer être une simple coïncidence, et qu'il faut plutôt comprendre les mécanismes sous-jacents qui les relient. Une fois le modèle théorique établi, il était alors possible de relier les ensembles et séries de données recueillies, puisqu'en l'absence de modèles, les données ne représentaient que du bruit. Or, face à la masse de données grandement disponible de nos jours, « *this approach to science — hypothesize, model, test — is becoming obsolete* »[1945].

En effet, avant l'avènement de l'ère numérique, l'analyse se limitait habituellement à tester un petit nombre d'hypothèses définies par les scientifiques et chercheurs bien avant la collecte des données ; en revanche, dans le monde du Big data, la parole est d'abord aux données[1946], « *when we let the data speak, we can make connections that we never thought existed. Hence, some hedge funds parse Twitter to predict the performance of the stock market. Amazon and Netflix base their product recommendations on a myriad of user interactions on their sites. Twitter, LinkedIn, and Facebook all map user's "social graph" of relationships to learn their preferences* »[1947]. De ce fait, contrairement à l'ère analogique, l'ère du tout numérique permet d'abandonner l'obsession de causalité pour s'orienter vers la découverte de schémas, modèles (*patterns*) et corrélations dans les données, offrant des informations et des connaissances innovantes et inestimables. Les géants du web ont évolué dans ce monde, et se sont développés et améliorés en fonction du passage progressif du kilooctet au mégaoctet au téraoctet, arrivant

[1944] C. ANDERSON, "The end of theory: The Data deluge makes the scientific method obsolete", *Id.*
[1945] C. ANDERSON, "The end of theory: The Data deluge makes the scientific method obsolete", *Ibid.*; cité également par, M. GRAHAM, "Big data and the end of theory?", The Guardian, publié le 9 mars 2012: https://www.theguardian.com/news/datablog/2012/mar/09/big-data-theory
[1946] *Cf.* p. 135 et s.
[1947] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *op. cit.,* p. 14.

au pétaoctet et au monde du Cloud ayant la capacité d'enregistrer et de stocker un volume massif de données[1948].

Or, à l'échelle des pétaoctets, l'information n'est pas une simple question de taxonomie, de classification et d'ordre tridimensionnel et quadridimensionnel, mais plutôt de statistiques dimensionnelles agnostiques, exigeant, par conséquent, une approche totalement différente où les données sont analysées en totalité sans recherche de lien de causalité et sans distinguer des séries de données, puisque « *every single data set is likely to have some intrinsic, hidden, not yet unearthed value, and the race is on to discover and capture all of it* »[1949]. Dès lors, c'est le délaissement des règles abstraites pour des statistiques de contextes, facilité par le pouvoir des données, du calcul, de la quantification et de l'arithmétique mais aussi par les techniques d'apprentissage automatique et par l'automatisation progressivement généralisée ; les capacités technologiques désormais disponibles permettant de tester plusieurs milliers d'hypothèses en même temps, tout en ayant les moyens de prendre en compte plusieurs théories dans la prédiction et surtout « *de changer les pondérations affectées aux différentes hypothèses pour chaque profil et chaque contexte d'utilisation* »[1950].

L'analyse de corrélation s'est, néanmoins, avérée depuis longtemps être utile, bien avant l'arrivée du Big data. Le concept a été initié par Sir Galton, cousin de Darwin, en 1888, apparu au moment où il a reconnu un fil commun entre trois problèmes scientifiques différents qu'il étudiait, après avoir remarqué une relation entre la taille des hommes et la longueur de l'avant-bras[1951]. Les mathématiques sous-jacentes de son analyse de corrélation sont relativement simples et robustes, ce qui constitue l'une de ses caractéristiques essentielles contribuant à en faire l'une des mesures statistiques les plus utilisées[1952]. En revanche, avant l'époque du Big data et de la société de l'information, l'utilité de cette méthode était assez limitée et les scientifiques et statisticiens suivaient, finalement, une approche conduite par des essais et erreurs fondés sur des hypothèses pour entreprendre leurs analyses de corrélation et en dégager des connaissances, du savoir. Mais à l'heure actuelle, les données sont disponibles en masse,

---

[1948] *Cf.* p. 112.

[1949] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Id.,* p. 15.

[1950] D. CARDON, *À quoi rêvent les algorithmes*, *op. cit*., p. 61, et l'auteur précise alors « *[…]. Les méthodes non paramétriques ont ceci d'agnostique qu'elles ne figent pas la contribution de leurs variables, mais les révisent constamment en fonction des actions de l'utilisateur*. »

[1951] F. GALTON, "Co-relations and their measurement, chiefly from anthropometric data", *In* Proceedings of the Royal Society, Vol. 45, December 13, 1888, p. 135-145: http://galton.org/essays/1880-1889/galton-1888-co-relations-rsoc.pdf

[1952] F. GALTON, "Co-relations and their measurement, chiefly from anthropometric data", *Id.*; et, F. GALTON, "Kinship and Correlation", *In* North American Review, Vol. 150, 1890, p. 419-431: http://galton.org/essays/1890-1899/galton-1890-nareview-kinship-and-correlation.html

les techniques et les pratiques computationnelles, de quantification ou de datafication constituent un pouvoir inédit permettant d'élaborer des analyses computationnelles de corrélation sophistiquées, sans avoir besoin de variables ou d'hypothèses ou de règles abstraites de sorte que, au lieu de suivre une approche « *hypothesis-driven* », il est dorénavant possible d'adopter une approche « *data-driven* »[1953].

Les prédictions entreprises à l'ère du Big data dans de nombreux secteurs aussi divers que variés sont, en majorité, fondées sur cette analyse de corrélation. Comme il a pu être observé dans le cadre de cette étude, les cotes de solvabilité peuvent être utilisées pour prédire les comportements des personnes concernées ; les historiques de navigation et les recherches effectuées peuvent être utilisées pour prédire des schémas ou des comportements ; de même, les historiques de crédits peuvent être utilisés pour prédire le niveau de revenu des personnes concernées ; les historiques d'achats peuvent être utilisés pour prédire les grossesses, et ainsi de suite. Le recours aux corrélations, tout comme le recours aux techniques d'apprentissage automatique, ne fait que s'étendre dans le monde numérique du XXI[e] Siècle, affectant tous les secteurs et domaines, et perfectionnant les analyses de prédiction, nécessaire au capitalisme de surveillance. Il ne s'agit même plus de déterminer une théorie unifiée des comportements, les avancées technologiques permettant désormais d'établir des micro-théories concernant chaque dossier numérique et évaluant les conduites probables. C'est une manière inversée de fabriquer le social qui « *témoigne du renversement de la causalité opérée par le calcul statistique pour faire face à l'individualisation de nos sociétés et à l'indétermination de plus en plus grande des déterminants de nos actions. Il est en effet frappant de constater que les logiques actuelles des calculateurs cherchent à redonner des cadres à la société, mais en quelque sorte, à l'envers et par le bas, en partant des comportements individuels pour en inférer ensuite les attributs qui les rendent statistiquement probables* »[1954].

Lors de chaque cas de surveillance révélé, qu'elle ait été effectuée par une entreprise ou un gouvernement, l'attention est, en général, centrée sur la collecte de données, entreprise de manière intrusive et sans le consentement des personnes concernées, mais l'attention est

---

[1953] V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data*, *Id.,* p. 55, les auteurs expliquent ainsi "*No longer do we necessarily require a valid substantive hypothesis about a phenomenon to begin to understand our world. Thus, we don't have to develop a notion about what terms people search for when and where the flu spreads. We don't need to have an inkling of how airlines price their tickets. We don't need to care about the culinary tastes of Walmart shoppers. Instead we can subject big data to correlation analysis and let it tell us what search queries are the best proxies for the flu, whether an airfare is likely to soar, or what anxious families want to nibble on during a storm*."

[1954] D. CARDON, *À quoi rêvent les algorithmes*, *Id*., p. 53-54.

rarement portée sur la corrélation des données opérée, la mise en lien des identités parmi différents ensembles de données en vue de tirer des inférences des données combinées. En effet, de nos jours, le système qui collecte les numéros de plaque d'immatriculation des caméras se trouve être également équipé d'un logiciel de reconnaissance faciale automatique ou d'un algorithme conçu pour l'identification des véhicules automatiques, établissant dès lors beaucoup plus qu'une simple base de données de saisie de plaques d'immatriculations. De même, les drones, disponibles de plus en plus à des prix résiduels, ne font pas simplement de la captation d'images ou de vidéos, mais sont équipés d'un algorithme de reconnaissance faciale permettant au système d'identifier les personnes automatiquement, en analysant les vastes bases de données de photos étiquetées, taguées, qui proviennent des permis de conduire, de Facebook, de Twitter, d'Instagram, des magazines et journaux ou encore des annuaires de lycées.

De plus, ces systèmes ont les capacités de corréler les identifications faites avec une multitude d'autres bases de données, et de sauvegarder l'ensemble de ces données sans limitation de temps. Chacun de ces systèmes opère sa propre surveillance et ses propres corrélations en fonction de ses objectifs, et « *ubiquitous surveillance is the result of multiple streams of mass surveillance tied together* »[1955], ce qui s'avère être le cas aujourd'hui avec la confusion, de plus en plus accentuée, entre les gouvernements et les entreprises évoquant l'avènement de l'État-entreprise[1956]. Les corrélations s'effectuent dorénavant de plus en plus facilement et de plus en plus automatiquement ne se réduisant plus au cyberespace, compte tenu du fait que des entreprises, telles que Facebook, peuvent désormais corréler les comportements en ligne de ses utilisateurs avec leurs actions hors ligne, moyennant le recours aux *data brokers* qui effectuent également des corrélations de données, afin de compléter et de perfectionner leurs profils et dossiers numériques uniformisés et en tirer par là même des avantages et profits : « *once you can correlate different data sets, there is a lot you can do with them* »[1957].

Ainsi, confrontés au pouvoir des corrélations et aux inférences et prédictions qu'il induit, il s'avère actuellement quasi-impossible pour un individu de préserver son intimité et sa vie privée, ou de garder son anonymat s'il le souhaite, y compris pour des hackers, des agents spéciaux formés ou des spécialistes en matière de sécurité informatique. Selon Schneier, une

---

[1955] B. SCHNEIER, *Data and Goliath*, *op. cit.,* p. 48.

[1956] *Cf.* p. 355 et 371.

[1957] B. SCHNEIER, *Data and Goliath*, *Id,* p. 49, et l'auteur fournit une illustration: "*Imagine building up a picture of someone's health without ever looking at his patient records. Credit card records and supermarket affinity cards reveal what food and alcohol he buys, which restaurants he eats at, whether he has a gym membership, and what nonprescription items he buys at a pharmacy. His phone reveals how often he goes to that gym, and his activity tracker reveals his activity level when he's there. Data from websites reveal what medical terms he's searched on. This is how a company like ExactData can sell lists of people who date online, people who gamble, and people who suffer from anxiety, incontinence, or erectile dysfunction."*

organisation qui a les capacités de corréler les différents flux de surveillance, a souvent les moyens d'identifier des personnes essayant de se cacher et de garder leur anonymat[1958], et souligne, par conséquent, que « *maintaining internet anonymity against a ubiquitous surveillor is nearly impossible.[…]. The same is true for large sets of anonymous data. We might naïvely think that there are so many of us that it's easy to hide in the sea of data. Or that most of our data is anonymous. That's not true. Most techniques for anonymizing data don't work, and the data can be de-anonymized with surprisingly little information* »[1959].

De la sorte, plus aucune recherche ou base de données rendues anonymes n'est à l'abri d'être comparée à n'importe quelle autre, et, par le biais d'une analyse de corrélation, aboutir à une identification quasi certaine des personnes concernées, ce qui est contre-intuitif indique Schneier, « *but it takes less data to uniquely identify us that we think* »[1960]. Les individus, même les plus typiques, sont absolument distincts, ayant chacun des caractéristiques, des habitudes et des comportements individuels, uniques, propre à leur Soi et à leur identité, et il est de nos jours facilement possible de les identifier *via* leurs habitudes de lecture, de trajet, d'achat en ligne et hors ligne ou de navigation moyennant les corrélations, pour ensuite induire ou prédire. C'est la raison pour laquelle « *regulation based on the concept of "personally identifying information" doesn't work. PII is usually defined as a name, unique account number, and so on, and special rules apply to it. But PII is also the amount of data; the more information someone has about you, even anonymous information, the easier it is for her to identify you* »[1961].

Il n'est donc pas étonnant que les géants du web puissent facilement, à l'aide de leurs propres ressources et bases de données volumineuses, recourir à ces techniques de corrélations et dé-anonymiser une série de données initialement anonymisées, pour en tirer des informations et des connaissances, faire des prédictions et des inductions ainsi que guider les comportements et les actions, le tout en étant conforme à la loi : « *Now Google and like-minded companies are*

[1958] B. SCHNEIER, *Data and Goliath*, *Id,* p. 50-51, pour illustration indique l'auteur « *A member of the hacker group Anonymous called "w0rmer", wanted for hacking US law enforcement websites, used an anonymous Twitter account, but linked to a photo of a woman's breasts taken with an iPhone. The photo's embedded GPS coordinates pointed to a house in Australia. Another website that referenced w0rmer also mentioned the name Higinio Ochoa. The police got hold of Ochoa's Facebook page, which included the information that he had an Australian girlfriend. Photos of the girlfriend marched the original photo that started all this, and police arrested w0rmer aka Ochoa.* »

[1959] B. SCHNEIER, *Data and Goliath*, *Ibid,* p. 51.

[1960] B. SCHNEIER, *Data and Goliath*, *Ibid.,* p. 52.

[1961] B. SCHNEIER, *Data and Goliath*, *Ibidem,* p. 53.

sifting through the most measured age in history, treating this massive corpus as a laboratory of the human condition. They are the children of the Petabyte Age »[1962].

Les risques et conséquences que les analyses de corrélation et de prédiction peuvent engendrer sont multiples et majeurs, sans compter les atteintes systématiques aux droits à la protection des données personnelles et au respect de la vie privée qu'elles entraînent, comme il a été vu, pouvant facilement stigmatiser une personne, la discriminer ou la classer en « individu dangereux » ou en « personne suspecte »[1963], par exemple : « *already law enforcement agencies make use of predictive analytic tools to identify suspects and direct investigations. It's a short step from there to the world of Big Brother and thoughtcrime* »[1964].

Face aux pouvoirs de l'analyse de corrélation et de l'analyse de prédiction, les individus sont finalement appréhendés comme des fragments de données, appartenant à un large flux de données qu'il s'agit de traiter, représenter, calculer et modéliser, de sorte qu' « *on ne se trouve plus devant le couple masse-individu. Les individus sont devenus des dividuels. Le dividuel, c'est l'individu divisé, fragmenté en plusieurs morceaux de données. Ces morceaux sont autant de données qui naviguent dans l'océan du cyberespace. L'individu ne s'appartient plus qu'imparfaitement. Il est donc en parti nié* »[1965].

Il semble ainsi que c'est la concrétisation et la pérennisation de la gouvernance par les nombres et les données et du capitalisme de surveillance qui ont, indéniablement, des influences et des impacts majeurs sur la vie des individus, leur liberté de se constituer et de développer leur identité propre et unique. En effet, « *dans la mesure où elle vise la programmation de l'agir humain, la gouvernance par les nombres peut d'autant moins demeurer sans effet sur l'état des personnes qu'elle affecte nécessairement leur statut et leur identité. Au lieu de réduire l'être humain à un rôle mécanique d'obéissance à des règles, comme le faisait l'État administratif ou l'entreprise fordiste, elle exploite sa capacité – soulignée par Norbert Wiener – de donner aux*

[1962] C. ANDERSON, "The end of theory: The Data deluge makes the scientific method obsolete", *Id.*

[1963] *Cf.* p. 463 et s.

[1964] B. SCHNEIER, *Data and Goliath*, *Id.,* p. 116.

[1965] A. BASDEVANT et J.-P. MIGNARD, *L'empire des données, op. cit.,* p. 253-254, et les auteurs citent en note de bas de page les propos de Gilles Deleuze : « *Le langage numérique du contrôle est fait de chiffres, qui marquent l'accès à l'information, ou le rejet. On ne se trouve plus devant le couple masse-individu. Les individus sont devenus des « dividuels », et les masses, des échantillons, des données, des marchés ou des « banques ». C'est peut-être l'argent qui exprime le mieux la distinction des deux sociétés, puisque la discipline s'est toujours rapportée à des monnaies moulées qui renfermaient de l'or comme nombre étalon, tandis que le contrôle renvoie à des échanges flottants, modulations qui font intervenir comme chiffre un pourcentage de différentes monnaies échantillons.* », G. Deleuze, « Post-scriptum sur les sociétés de contrôle », dans *Pourparlers (1972-1990)*, Minuit, 1990.

informations qu'il reçoit « une forme nouvelle afin de pouvoir être utilisée en vue des stades ultérieurs du fonctionnement » du système auquel il appartient »[1966].

En fin de compte, il apparaît ainsi que « *l'ancien Big Brother était préoccupé par l'inclusion – l'intégration, mettre les gens en rang et les y maintenir. Ce qui intéresse le nouveau Big Brother, c'est l'exclusion – c'est chercher les gens qui ne conviennent pas au lieu où ils sont ; les bannir de ce lieu et les déporter "là où est leur place" ; ou, mieux encore, ne jamais les autoriser, pour commencer, à se rapprocher de ce lieu. Le nouveau Big Brother fournit aux officiers de l'immigration les listes de gens qu'ils ne devraient pas laisser entrer, et aux banquiers la liste de ceux qu'ils ne devraient pas admettre dans la compagnie de ceux qui sont dignes de crédit. Il donne aux gardes des instructions concernant ceux qu'ils devraient arrêter devant les grilles et ne pas laisser pénétrer dans la communauté de l'autre côté des grilles. Il insuffle aux surveillants du voisinage l'idée d'épier et de chasser les prétendus rôdeurs ou ceux qui ont des intentions louches – étrangers qui ne sont pas à leur place. Il offre aux propriétaires des circuits de télévision fermés, pour empêcher les indésirables de s'approcher. Il est le saint patron de tous les videurs, que ce soit au service d'une boîte de nuit ou d'un ministre d'État, ministre de l'Intérieur* »[1967].

[1966] A. SUPIOT, *La gouvernance par les nombres, op. cit.,* p. 216 ; et, *Cf.* p. 557 et s.
[1967] Z. BAUMAN, *Vies perdues : La modernité et ses exclus*, Paris, Payot, 2006, p. 242-243.

TITRE II – UNE RÉALITÉ SOCIOJURIDIQUE

« *Les individus […] auront le même point de départ, la même civilisation, la même langue, la même religion, les mêmes habitudes, les mêmes mœurs, et à travers lesquels la pensée circulera sous la même forme et se peindra des mêmes couleurs. Tout le reste est douteux, mais ceci est certain* »[1968].

Les enjeux de l'identité numérique soulèvent, dans un second temps, le problème de l'influence technologique et scientifique sur la politique publique et la société dans son ensemble, concrétisant une réalité sociojuridique complémentaire à la réalité économico-sécuritaire et en découlant, affectant les identités sujets du traitement de données personnelles tel qu'envisagé à l'ère de la numérisation de la société.

À ce degré, il est question des défis et des risques observés et analysés, de manière pragmatique, suivant l'approche de la sociologie juridique, qui traite « des phénomènes plus ou moins teintés de droit, dont le droit peut être cause, effet ou occasion, y compris des phénomènes de violation, d'ineffectivité, ou de déviance »[1969], en vue d'appréhender, scientifiquement et juridiquement, les enjeux qui entourent, *in concreto*, les phénomènes sociaux survenus, notamment à travers les opérations de traitement, et, en prolongement, les individus et leurs identités, dans un milieu social donné.

C'est donc une « *[…] science qui se propose de comprendre par interprétation l'activité sociale, et par là d'expliquer causalement son déroulement et ses effets* »[1970], et dont le domaine porte sur le fait social qui « *[…] se reconnaît au pouvoir de coercition externe qu'il exerce ou est susceptible d'exercer sur les individus ; et la présence de ce pouvoir se reconnaît à son tour soit à l'existence de quelque sanction déterminée, soit à la résistance que le fait oppose à toute entreprise individuelle qui tend à lui faire violence* »[1971]. Ce qui caractérise ainsi le fait social que constitue dorénavant le traitement des identités numériques en réponse à l'interprétation et à l'analyse résultant du traitement de l'activité sociale, pour la plupart numérisée, donc du traitement des données à caractère personnel, l'expression du soi connecté.

À l'heure actuelle, les capacités de traitements et d'analyses de données aussi variables que nombreuses permettent aux entités privées comme publiques de modifier et d'adapter leurs

[1968] A. DE TOCQUEVILLE, *De la démocratie en Amérique*, t. I, Ed. GF Flammarion, Paris, 1981, p. 313.
[1969] J. CARBONNIER, *Sociologie juridique*, 2ème éd., Paris, PUF, Coll. Quadrige, 2004, 415 p.
[1970] M. WEBER, *Économie et société*, t. I (1922), Ed. Librairie Plon, 1971, p. 23.
[1971] É. DURKHEIM, *Les règles de la méthode sociologique*, 2ème Ed. (1937), PUF, Coll. Bibliothèque de philosophie contemporaine, 1973, p. 11.

politiques et leurs gestions en recourant, de manière principale, aux pratiques et dispositifs technologiques et scientifiques développés suivant leurs besoins et leurs objectifs du moment respectivement poursuivis. *De facto*, cet ensemble affecte la mise en œuvre de la politique publique à poursuivre, des normes pénales et répressives à prévoir, des architectures et cultures sociales à adopter, et, *in extremis*, du quotidien sociojuridique dans lequel tout individu vit et évolue.

Dans ce contexte, un changement de politique criminelle, entendue dans son approche interdisciplinaire tenant compte de son pan socioculturel, a été adopté. En effet, comme il a pu être constaté « *[…] la politique criminelle s'est détachée, tant du droit pénal que de la criminologie et de la sociologie criminelle, et a pris une signification autonome* »[1972]. D'emblée, la nécessité de ne pas la réduire au seul droit pénal fut soulignée afin « *[…] d'y voir « la réaction, organisée et délibérée, de la collectivité contre les activités délictueuses, déviantes ou antisociales », en s'attachant à faire ressortir son double caractère de « science d'observation » et d' « art », ou de « stratégie méthodique de la réaction anticriminelle ». […]. Certes le droit pénal reste très présent, comme le noyau le plus dur ou le lieu de la plus haute tension, également de la plus grande visibilité ; mais les pratiques pénales ne sont pas seules dans le champ de la politique criminelle, où elles se trouvent comme enveloppées par d'autres pratiques de contrôle social : non pénales (sanctions administratives par exemple), non répressives (prévention, réparation, médiation par exemple), et parfois même non étatiques (pratiques répressives des milices privées, actions protestataires de type Amnesty International, ou mesures disciplinaires, le terme évoquant certains types de régulation professionnelle)* »[1973]. Les pratiques pénales ne poursuivent plus, à l'heure de la révolution numérique, l'objectif premier de punir eu égard les avancées technologiques qui permettent d'effectuer des opérations de traitement visant une prévention ou une prédiction en amont et *a priori*, accordant en conséquence de nombreux pouvoirs et discrétions aux autorités étatiques, alors même qu' « *il serait trop naïf, pour ne pas dire coupablement naïf, que le droit pénal du XXI^e siècle prétende ignorer que, chaque fois qu'il légitime l'exercice du pouvoir punitif, il légitime un domaine du pouvoir qui va être mis en œuvre par des agences qui, durant plus d'un siècle, ont démontré, de façon accablante, leur capacité à commettre les plus grands massacres de toute l'histoire de l'humanité. Il est temps de se réveiller face à une horrible réalité, puisqu'il n'y a*

[1972] M. DELMAS-MARTY, *Les grands systèmes de politique criminelle*, PUF, Coll. Thémis, 1992, p. 13.
[1973] M. DELMAS-MARTY, *Les grands systèmes de politique criminelle*, *Id.*, p. 13-14.

plus de prétextes pour l'éluder. L'horreur ne peut pas paralyser la science juridique, mais doit lui donner de l'impulsion »[1974].

Par ailleurs, les questions de sécurité, de défense, de sûreté, voire de l'amélioration de la société et de l'être humain, impliquent à la fois les autorités publiques et privées, mais aussi les individus composant la société, le Président de la République française ayant bien souligné que ces questions caractérisent des « enjeux » devant mobiliser la société dans son ensemble, et, « au-delà, toutes les ressources vives de la communauté nationale »[1975].

Dans ce cadre, et en observant les diverses applications et impacts du monde social, juridique, et technologique, le traitement des données personnelles, tel qu'entrepris à l'heure actuelle, semble ainsi viser le traitement des identités numériques et, *a fortiori*, des individus dans leur environnement social ; traitements accompagnés de garanties très insuffisantes, puisque ne serait-ce qu'en ce qui concerne « *[…] les informations « de haute politique » — sûreté de l'État, défense, sécurité publique* — [elles] *ne seront pas accessibles et personne ne saura jamais, à moins d'un concours de circonstances extraordinaire, si l'information inscrite sur sa fiche correspond à la réalité ou est erronée* »[1976].

Les paradigmes sociaux, et par conséquent les phénomènes juridiques, paraissent dès lors inversés, porteurs d'ambiguïtés et de confusions, générant des situations équivoques également porteuses d'éventuelles ingérences et atteintes aux droits et libertés des individus, notamment à leur construction et à leur autonomie personnelle.

Quels sont alors les enjeux entourant l'identité numérique appréhendée de manière pragmatique dans le monde social et juridique du XXI^{e} Siècle ? Ceux-ci ont-ils suscité, *in concreto*, des changements dans la réalité sociojuridique des êtres humains, telle qu'elle est vécue et perçue ? Il ressort, à travers ces derniers développements, que le traitement des données personnelles mute et passe à l'échelle du traitement des identités numériques et des individus caractérisant ces identités, compte tenu, d'une part, du changement de politique criminelle adopté (Chap. I), et, d'autre part, du changement de paradigme socioculturel manifesté ; l'ensemble affectant, *in fine*, les individus et leurs réalité et environnement sociojuridiques.

[1974] E. R. ZAFFARONI, « Dans un État de droit il n'y a que des délinquants », RSC 2009, p. 43.
[1975] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République Emmanuel Macron », DICoD - Bureau des Éditions, Octobre 2017, p. 5-7.
[1976] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit*., p. 5787.

Chapitre I. Le traitement des identités numériques : Un changement de politique criminelle

> « *The Master said, "Yu, shall I teach you what knowledge is? When you know a thing, to hold that you know it; and when you do not know a thing, to allow that you do not know it; this is knowledge."* »[1977]

Le développement des outils et procédés technologiques et scientifiques a permis d'envisager et de mettre en place une nouvelle politique criminelle orientée vers plus de prévention et de répression, compte tenu des capacités informatiques et des opérations de traitement de données mises au point facilitant le traitement et la gestion des identités numériques et, par extension, les individus concernés. Pourtant, « *cela fait aujourd'hui plus de trente ans que de nombreux experts en criminologie et en société prônent davantage de prévention que de répression en matière de criminalité. Or, malgré le manque d'efficacité du système répressif dans son ensemble, un seul constat s'impose : il n'y a eu guère d'évolution* »[1978].

La politique criminelle, qui constitue à la fois les réponses pénales et non pénales aux phénomènes criminels et antisociaux en vue d'assurer l'ordre social, est « *[…] pendant longtemps restée synonyme de théorie et pratique du système pénal […]* »[1979] ; le droit pénal, théoriquement, « *ayant renoncé à la divinité, au moins dans la conception occidentale, […], s'attacherait désormais à faire respecter l'humanité* »[1980]. Toutefois, non réduite au seul droit pénal, la politique criminelle comprend plutôt « *l'ensemble des procédés par lesquels le corps social organise les réponses au phénomène criminel et apparaît donc comme « théorie et pratique des différentes formes du contrôle social »* »[1981].

En pratique, la mise en œuvre de la nouvelle politique publique recourt à des normes pénales et sociales pouvant être qualifiées de « sécuritaires », « *[…] en ce sens qu'elles fondent leur légitimité sur la dangerosité et non sur la culpabilité, […]* », donc axée principalement sur la prévention, « *[…] leur efficacité sur la mesure de sûreté et non sur la punition […]* »[1982], des mesures, pour la plupart, restrictives de liberté. Centré principalement sur les objets et

---

[1977] Confucius, *The Analects*, written in ca 500 B.C., Book 2, Chap. 17 ; Disponible en ligne: http://classics.mit.edu/Confucius/analects.1.1.html

[1978] J. KROPP et S. BRUNEAU (recension), Irvin Waller, Lutter contre la délinquance - Comment le tout répressif tue la Sécurité, (L'Harmattan, Paris, France, 2009, 224 p.), Notes bibliographiques, RSC 2011, p. 278.

[1979] M. DELMAS-MARTY, *Les grands systèmes de politique criminelle*, *op. cit*, p. 13.

[1980] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », RSC, 1994, p. 477.

[1981] M. DELMAS-MARTY, *Les grands systèmes de politique criminelle*, *Id.*, p. 13.

[1982] M. DELMAS-MARTY, Les politiques sécuritaires à la lumière de la doctrine pénale du XIX[e] au XXI[e] siècle, RSC 2010, p. 5.

dispositifs numériques développés et en développement, le but de la dernière politique criminelle poursuivie est non seulement d'instaurer une défense sociale permettant la prévention, notamment celle du risque, mais aussi permettant « *[…] d'améliorer la résilience des administrations de l'État en favorisant l'émergence en leur sein d'une culture de la cybersécurité, en affectant les moyens nécessaires à la protection de leurs systèmes d'information et en garantissant, en cas de crise, la fluidité des relations entre les différents acteurs de la prévention et la protection […] mais aussi de la judiciarisation* »[1983].

Quelle est donc la nouvelle politique publique mise en place eu égard à la facilité, l'utilité et l'efficacité des opérations de traitement de données et de l'accès à l'information ? et plus particulièrement, quel est l'impact du changement de la politique criminelle adoptée sur le traitement et la gestion de l'information ainsi que sur la société et les individus ?

S'observe alors, à travers les développements suivants, la mise en œuvre d'une politique criminelle préventive (Section 1) d'un côté, et liberticide (Section 2), de l'autre, caractérisant *ipso facto* le sentiment de traitement en masse des identités numériques avéré.

Section 1 – La mise en œuvre d'une politique criminelle préventive

Afin de maintenir l'ordre social à l'ère de la révolution numérique et de la croissance des risques, une nouvelle politique criminelle s'est mise en place, souvent réclamée par les citoyens inquiets et incertains. De nature fortement préventive, cette politique criminelle se caractérise, principalement, par un droit pénal fondé sur la dangerosité et le risque (§1), ainsi que par une défense sociale centrée sur la peur et la prévention du risque (§2), visant ainsi à assurer plus de sécurité et de sûreté aux citoyens.

§1. Un droit pénal fondé sur la dangerosité et le risque

Un droit pénal institué sur la conception de la dangerosité et du risque se conçoit alors pour répondre au sentiment d'insécurité croissant, ressenti et manifesté, cherchant continuellement à repérer l'individu dangereux (A) en vue de prévenir et de prédire la dangerosité et le risque tout en réaménageant les mesures de sûreté (B).

[1983] Rapport d'information n° 299 de MM. O. CADIC et R. MAZUIR, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, « Cyberattaque contre « ARIANE » : une expérience qui doit nous servir », (2018-2019) – déposé au Sénat le 6 février 2019 ; disponible en ligne : https://www.senat.fr/notice-rapport/2018/r18-299-notice.html

A. L'individu dangereux

En 1978, lors d'une conférence, M. Foucault aborde la question de l'évolution de la notion d' « individu dangereux » dans le champ légal ainsi que dans le champ de la psychiatrie, conduisant cette dernière à pénétrer progressivement le champ pénal[1984]. En propos liminaires, Foucault cite un procès ayant eu lieu à la Cour d'assise de Paris, donc un fait judiciaire, relatant le silence de l'inculpé et l'étonnement de la Cour, du procureur et des jurés confrontés à un accusé totalement muet. Ce qui est frappant dans ce cas précis, selon le Professeur, c'est que l'appareil judiciaire, destiné à établir des faits délictueux, à en déterminer l'auteur, et à sanctionner ses actes en appliquant les peines prévues par la loi, ne semblait pas de lui-même apporter toutes les réponses voulues à l'occasion de cette affaire, alors même que le corps judicaire de la fin du XVIII[e] début du XIX[e] Siècle ne pouvait « *rêver de situation plus limpide* »[1985].

Ce cas particulier lui fait prendre conscience qu'un simple aveu n'aurait également pas suffi à la machine pénale qui requiert désormais, semble-t-il, « *un matériau supplémentaire* », une confession, un examen de conscience, une mise en lumière de ce qu'on est, une explication de soi, afin que tout le monde comprenne pourquoi l'acte réprimé a été commis et jugé en fonction. De ce fait, il y a non seulement une attente de responsabilité de l'auteur en raison des faits commis mais aussi, indique Foucault, une exigence de rationalité de l'acte commis et une attente de punition. Pour fonctionner, la machine pénale paraît alors nécessiter, en plus d'une loi, d'une infraction et d'un auteur responsable des faits, un « *autre type de discours : celui que l'accusé tient sur lui-même, ou celui qu'il permet, par ses confessions, souvenirs, confidences etc., qu'on tienne sur lui* » afin que les magistrats, les jurés, les avocats mais aussi le Ministère public, puissent « *réellement jouer leur rôle* »[1986].

Plusieurs affaires de l'époque, telle que l'affaire Patrick Henry plaidée par M[e] Badinter, semblaient sous-tendre que cet élément de compréhension, le fait de connaître la personne qu'on juge, de comprendre ses actes, devenait indispensable à la scène judiciaire, à l'acte de juger et de punir. C'est ce qui a préparé le terrain pour l'intervention de la psychiatrie dans le

[1984] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », Communication au symposium de Toronto «Law and Psychiatry», Clarke Institute of Psychiatry, 24-26 octobre 1977, *In* Journal of Law and Psychiatry, Vol. I, 1978, p. 1-18 (« About the Concept of the «Dangerous Individual» in 19th Century Legal Psychiatry »), disponible en ligne: http://1libertaire.free.fr/MFoucault340.html ; et, M. FOUCAULT, *Dits et écrits,* t. III (1976-1979), *op. cit.*, texte n°220.

[1985] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Id.*

[1986] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Id.*

milieu pénal, les experts pouvant apporter des réponses à cette quête de rationalité, de compréhension, et aider le juge à déterminer si l'inculpé est accessible à une sanction pénale, s'il peut être tenu pour responsable et puni. L'auteur s'intéresse ainsi à des cas criminels graves particuliers ayant sollicité le recours à un expert en psychiatrie pour combler cette attente de rationalité de la société, dont les juges, avocats, jurés et ministres sont les porte-paroles, alors que, selon lui, il y a bien plus de crimes sans raison que de crimes avec raison, la démence, la fureur ou la folie constituant autant de causes insondables de crimes.

Tous ces cas, ayant principalement la même forme, ont ouvert la voie au XIX[e] Siècle à la psychiatrie du crime, qui s'est inaugurée par une « pathologie du monstrueux » découlant de ces crimes « contre nature » et « sans raison » : « *Au moment où se fonde la nouvelle psychiatrie et où on applique, à peu près partout en Europe et en Amérique, les principes de la réforme pénale, le grand assassinat monstrueux, sans raison ni préliminaire, l'irruption soudaine de la contre-nature dans la nature est donc la forme singulière et paradoxale sous laquelle se présente la folie criminelle ou le crime pathologique. […]. Ce que la psychiatrie du XIX[e] siècle a inventé, c'est cette entité absolument fictive d'un crime folie, d'un crime qui est tout entier folie, d'une folie qui n'est rien d'autre que crime* »[1987].

C'est l'avènement du concept de « monomanie homicide » et de l'entêtement des psychiatres à prendre place dans les mécanismes pénaux et à revendiquer leur droit d'intervention ; le crime étant devenu pour eux un enjeu important, « une modalité de pouvoir à garantir et à justifier »[1988]. Néanmoins, l'importance grandissante de la psychiatrie au XIX[e] Siècle ne se manifestait pas uniquement par son application d'une « nouvelle rationalité médicale aux désordres de l'esprit ou de la conduite », mais aussi par son fonctionnement en tant que « forme d'hygiène publique ». En effet, le « corps social » apparaissait de plus en plus comme une « réalité biologique et un domaine d'intervention médicale », le médecin devant alors être le « technicien du corps social et la médecine, une hygiène publique »[1989]. Et la psychiatrie, au

---

[1987] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Ibid.,* et l'auteur précise « *[…]. Je dis paradoxale, puisque ce qu'on essaie de saisir, c'est un type d'aliénation qui ne se manifesterait que dans le moment et sous les formes du crime, une aliénation qui n'aurait pour tout symptôme que le crime lui-même, et qui pourrait disparaître celui-ci une fois commis. Et inversement, il s'agit de repérer des crimes qui ont pour raison, pour auteur, pour «responsable juridique», en quelque sorte, ce qui, dans le sujet, est hors de sa responsabilité ; à savoir la folie qui se cache en lui et qu'il ne peut même pas maîtriser, car bien souvent il n'en est pas conscient*. »

[1988] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Ibid.*

[1989] M. FOUCAULT, *Il faut défendre la société*, Cours au collège de France 1975-1976, Coll. Hautes Études, EHESS, Gallimard – Seuil, 1997, Cours du 17 mars 1976 - p. 217, où l'auteur affirme « *Ce sont ces phénomènes-là* [notamment la maladie et l'épidémie] *qu'on commence à prendre en compte à la fin du XVIII[e] siècle et qui amènent la mise en place d'une médecine qui va avoir, maintenant, la fonction majeure de l'hygiène publique, avec des organismes de coordination des soins médicaux, de centralisation de l'information, de*

milieu de tous ces changements, a réussi à gagner en autonomie et en prestige en s'inscrivant « *dans le cadre d'une médecine conçue comme réaction aux dangers inhérents du corps social* »[1990].

Il semble alors que la psychiatrie et la médecine mentale ont pénétré la pénalité d'en bas, du côté des mécanismes de punition et de la signification qui leur était donnée permettant de justifier les sanctions infligées et de répondre aux attentes de rationalité ; le milieu de la presse qui construisait aussi ces affaires criminelles, à dimension intelligible, a amplifié encore plus ce phénomène. En effet, au tournant des XVIII[e] et XIX[e] Siècles, « *punir était devenu, parmi toutes les techniques nouvelles de contrôle et de transformation des individus, un ensemble de procédés concertés pour modifier les infracteurs : l'exemple terrorisant des supplices ou l'exclusion par le bannissement ne pouvaient plus suffire dans une société où l'exercice du pouvoir impliquait une technologie raisonnée des individus* », la punition portant, en conséquence, sur le criminel en soi plutôt que sur le crime commis, « *c'est-à-dire sur ce qui le rend criminel, ses motifs, ses mobiles, sa volonté profonde, ses tendances, ses instincts* »[1991]. À cet égard, Foucault précise « *dans les anciens systèmes, l'éclat du châtiment devait répondre à l'énormité du crime ; désormais, on cherche à adapter les modalités de la punition à la nature du criminel* », ce qui convenait à la machine pénale dans la mesure où la psychiatrie a finalement contribué *via* la monomanie à « l'intégration de l'acte dans la conduite globale de l'individu »[1992].

Par ailleurs, de ce défi d'irrationalité que le crime adresse à la société, une nouvelle doctrine pénale a vu le jour, focalisée principalement sur le thème de l'individu dangereux, et dénotant un virage important dans la pensée pénale où « *de plus en plus la pratique puis la théorie pénale aura tendance au XIX[e] puis au XX[e] siècle à faire de l'individu dangereux la cible principale de l'intervention punitive* » et où, de son côté, de plus en plus « *la psychiatrie du XIX[e] aura*

---

normalisation du savoir, et qui prend aussi l'allure de campagne d'apprentissage de l'hygiène et de médicalisation de la population. [...] »

[1990] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Ibid.,* et à cet égard l'auteur indique que « *[...]. Les aliénistes de l'époque ont pu discuter à l'infini sur l'origine organique ou psychique des maladies mentales, ils ont pu proposer des thérapeutiques physiques ou psychologiques : à travers leurs divergences, ils avaient tous conscience de traiter un «danger» social soit parce que la folie leur apparaissait liée à des conditions malsaines d'existence (surpopulation, promiscuité, vie urbaine, alcoolisme, débauche), soit encore parce qu'on la percevait comme source de dangers (pour soi-même, pour les autres, pour l'entourage, pour la descendance aussi par l'intermédiaire de l'hérédité). La psychiatrie du XIX[e] siècle, au moins autant qu'une médecine de l'âme individuelle, a été une médecine du corps collectif.* »

[1991] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Ibid.*

[1992] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Ibidem.*

tendance à rechercher les stigmates pathologiques qui peuvent marquer les individus dangereux […] »[1993].

C'est la naissance de l'anthropologie de l'homme criminel qui a surgit avec l'école italienne, comprenant Lombroso, Ferri et Garofalo, et la théorie de la défense sociale mise en œuvre, d'abord, par l'école belge avec notamment Prins. Selon l'école italienne, la seule volonté d'imputer un acte à un individu suivant un code réprimant ledit acte est insuffisante, il faudrait au contraire saisir l'acte à sa source, sa biographie avec ses caractéristiques individuelles ; cette source de la criminalité désignant donc l'individu. Lombroso a ainsi, en faisant appel à Darwin entre autres, tenté de fonder l'atavisme de certaines formes de criminalité[1994], le menant vers sa réflexion selon laquelle les criminels constituent « *une véritable race à part avec des stigmates précis, biologiques ou psychologiques, qui en constitueraient la marque indélébile* »[1995]. Quant à Ferri, fervent critique des postulats de l'école classique, surtout de Beccaria[1996], les réfute en

---

[1993] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX^e^ siècle », *Ibidem.*

[1994] C. Lombroso, *L'Anthropologie criminelle et ses récents progrès*, Coll. Félix Alcan, Bibliothèque de philosophie contemporaine, 1890, Préface, p. 7 et *sq.,* où l'auteur indique que « *Le plus étrange, c'est que bien des gens, tout en admettant l'atavisme des criminels, trouvent que justement pour cela, il n'est pas possible d'admettre son influence pathologique. M. Manouvrier, au contraire, tout en acceptant l'influence pathologique (ce qui explique l'asymétrie du visage, l'enchevêtrement des dents des criminels), y puise un prétexte pour nier l'atavisme. Mais est-ce que ce n'est pas le cas de bien des maladies mentales (la microcéphalie, par exemple), de montrer réunis, tout à fait enchevêtrés et presque fondus ensemble, la pathologie et l'atavisme ? […].* » (p.7-8)

[1995] M. DELMAS-MARTY, « Les politiques sécuritaires à la lumière de la doctrine pénale du XIX^e^ au XXI^e^ siècle », Introduction, RSC 2010, p. 5.

[1996] E. FERRI, *La sociologie criminelle* – Introduction, Trad. de l'Italien par Léon Terrien, Coll. Félix Alcan, Paris, 2^ème^ Ed., 1914 (1^ère^ éd. 1893), l'auteur avance ainsi « *On peut dire qu'Adam Smith fut pour l'économie politique ce que fut César Beccaria pour le droit criminel. Ils ont inauguré deux grands et glorieux courants scientifiques qui se ressemblaient par un noble esprit de réaction contre l'empirisme du moyen âge, et qui tous deux élevaient la bannière de l'individualisme, l'un en prêchant la libre concurrence, l'autre en défendant les droits de l'humanité contre la tyrannie de l'État dans le domaine de la justice criminelle. […]. Adam Smith et son école emploient la méthode a priori et étudient les phénomènes économiques – consommation, production, distribution des richesses – comme des êtres abstraits égaux à eux-mêmes en tout temps et en tous lieux ; ils formulent des lois qu'ils déclarent universelles, absolues, immuables. Ils partent d'un grand principe : l'homme cherche toujours le bien-être, et ils en tirent, par voie de déduction logique, les dernières conséquences, les lois générales. Mais depuis un certain nombre d'années, en Allemagne d'abord, puis ailleurs, il s'est produit dans la science économique un mouvement hétérodoxe qui a donné naissance à l'école réaliste, ou historique, ou positive, de l'économie politique ; […]. Et maintenant cette nouvelle évolution s'est répandue partout, […], et a trouvé son expression complète dans les doctrines socialistes dont Marx avait déjà, antérieurement, tracé les lignes avec une méthode positive rigoureuse et puissante. Or, qui ne voit que cette direction positive de la science économique, où l'on proclame la nécessité d'observer les faits économiques non plus d'une façon abstraite, mais tels qu'ils se produisent en réalité, dans telles et telles conditions de temps et de lieu, pour en déduire des lois historiques valables pour tel pays, pour telle période de temps, et non pour d'autres pays et d'autres époques – direction qui conduit par une logique inexorable au socialisme positif et scientifique, qui est le transformisme économique,– qui ne voit, dis-je, que cette direction est tout à fait analogue à celle que l'école positive préconise et qu'elle a déjà commencé à appliquer dans les sciences criminelles et pénales ?*
Et qui ne voit alors que, en rapprochant le fait de la tendance nouvelle de la criminologie des faits analogues qui se produisent dans l'art et dans la science, on obtient une preuve nouvelle et singulièrement éloquente de son opportunité historique et de son utilité pratique ? D'autre part tout cela ne fait que confirmer une fois de plus une idée désormais solidement établie dans l'histoire de l'humanité ; savoir qu'aucun phénomène n'est

soutenant que « *l'anthropologie montre, par les faits, que le délinquant n'est pas un homme normal, qu'au contraire, par des anormalités organiques et psychiques, héréditaires et acquises, il constitue une classe spéciale, une variété de l'espèce humaine ; la statistique prouve que l'apparition, l'augmentation, la diminution et la disparition des délits dépendent de raisons autres que les peines inscrites dans les codes et appliquées par les magistrats ; la psychologie positive a démontré que le prétendu libre arbitre était une pure illusion subjective* »[1997]. Dès lors, la question psychiatrique, avec ses possibilités d'analyse de l'instinct et de l'affectivité et d'analyse causale de toutes les conduites, quel que soit le degré de leur criminalité, s'est étendue à tout le champ des infractions, ne se limitant plus au seul crime grave, irrationnel, qui pouvait alors « *se maintenir en termes de danger, et donc de protection à assurer* »[1998]. La défense de la société imposait, par conséquent, une distinction entre « homme normal » et « homme criminel », ces derniers constituant un danger, un risque pour le corps social.

À cet égard, l'approche de Garofalo consistait, en quelque sorte, à graduer la dialectique entre la « capacité criminelle » de l'individu et son « adaptabilité sociale » ; *in fine*, une approche fondée sur une logique d'appréciation individuelle, biographique, sociale, comportementale de celui qui a commis l'acte[1999]. La notion de capacité individuelle, que l'auteur nomme « témébilité » (*temibilità*), se réfère à la perversité constante et agissante et à la quantité de mal qu'on peut attendre d'un individu en fonction de l'analyse portée sur lui. Il s'agit donc, autrement dit, de déterminer la capacité criminelle de l'individu, sa redoutabilité, sa dangerosité, qui exigerait par conséquent, de manière dynamique, d'évaluer sa capacité de s'éloigner du danger en fonction de sa perversité et de son degré de sociabilité. À ce niveau, c'est la recherche de la possibilité ou de la capacité d'adaptation pour chaque individu, à savoir les conditions dans lesquelles il est possible de présumer qu'il cessera d'être un individu

---

miraculeux ni arbitraire, mais que tout ce qui arrive devait arriver, parce qu'un fait n'est jamais que l'effet naturel de causes déterminantes. De sorte que, si, dans la science criminelle, s'est manifesté de notre temps et s'élargit sans cesse davantage ce mouvement progressif, ce serait une étrange aberration de voir en cela une velléité personnelle de tel ou tel individu, au lieu d'y reconnaître la manifestation nécessaire et inévitable d'une certaine condition historique de la science comme reflet de la vie sociale. » ; Disponible en ligne : http://classiques.uqac.ca/classiques/ferri_enrico/sociologie_criminelle/socio_criminelle_intro.html

[1997] E. FERRI, *La sociologie criminelle* – Introduction, *Id.*, « *Parmi les bases fondamentales du droit criminel et pénal tel qu'on le comprenait jusqu'à présent, sont les trois postulats que voici : 1° Le criminel est pourvu des mêmes idées, des mêmes sentiments que tout autre homme ; 2° Le principal effet des peines est d'arrêter l'augmentation et le débordement des délits ; 3° L'homme est doué du libre arbitre ou liberté morale et, par là même, moralement coupable et légalement responsable de ses délits. Il suffit au contraire de sortir du cercle scolastique des études juridiques et des affirmations a priori pour trouver, en opposition avec les assertions précédentes, ces conclusions des sciences expérimentales : […]. »*

[1998] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Id.*

[1999] R. GAROFALO, *La criminologie –Étude sur la nature du crime et la théorie de la pénalité*, Félix Alcan, 2[ème] Ed., 1890 ; Disponible en ligne : https://gallica.bnf.fr/ark:/12148/bpt6k76988k.texteImage & http://classiques.uqac.ca/classiques/garofalo_raffaele/criminologie/criminologie.html

dangereux. Avec l'école de l'anthropologie criminelle surgit un changement radical dans la mission pénale, qui va dorénavant être chargée de lutter contre la criminalité en tant que phénomène social dont le socle est la lutte contre l'individu dangereux, générant également une série de déplacements « *du crime vers le criminel, de l'acte effectivement commis vers le danger virtuellement inclus dans l'individu, de la punition modulée du coupable à la protection absolue des autres* »[2000]. Cette école prônait, ainsi, une « dépénalisation du crime » par l'élaboration d'un appareil et de pratiques autres que ce qui était prévu par les codes juridiques.

Cela a également induit une influence sur le système juridique de la responsabilité, initiée, en particulier, par la mutation du droit de la responsabilité civile et la naissance du droit de la responsabilité sans faute. Selon Foucault, « *d'une manière qui peut sembler étrange au premier regard, c'est le droit civil qui a rendu possible dans le droit pénal l'articulation du code et de la science* »[2001]. En effet, la transformation manifestée dans le droit civil tournait principalement autour des notions d'accident, de risque et de responsabilité, due notamment à l'avènement du salariat, des techniques industrielles, du machinisme ou des indemnités par assurances, et donc des accidents du travail et leur rattachement à des fautes de niveaux différents ; une transformation alors vers un droit fondé sur un système de probabilité et de risque où la sanction aurait pour fonction de protéger et de prévenir contre les risques « inévitables », précise Foucault.

Pour ce faire, il était donc question de mettre en place un droit de la responsabilité sans faute, effort des civilistes occidentaux, et surtout allemands « *poussés qu'ils étaient par les exigences de la société bismarckienne – société non seulement de discipline mais de sécurité* »[2002]. À ce titre, le régime de sécurité sociale français actuel présente, selon l'École nationale supérieure de Sécurité sociale, plus de similitudes avec le modèle bismarckien qu'avec le modèle beveridgien[2003]. La mutation de la responsabilité civile désormais dépénalisée, n'établissant plus de faute mais une estimation du risque créé, a été finalement un modèle pour la responsabilité pénale, qui pouvait rattacher l'acte commis au risque de criminalité que constitue la personnalité propre de l'individu. Dans cette perspective, la sanction aura pour rôle principal

[2000] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX^e siècle », *Ibid.*
[2001] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX^e siècle », *Ibid.*
[2002] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX^e siècle », *Ibidem.*
[2003] G. NEZOSI, « Comment la France se situe-t-elle entre le modèle bismarckien et le modèle beveridgien ? », Vie-publique, publié le 29 février 2016 : https://www.vie-publique.fr/decouverte-institutions/finances-publiques/approfondissements/comment-france-situe-t-elle-entre-modele-bismarckien-modele-beveridgien.html

« *de diminuer dans toute la mesure du possible -soit par l'élimination, soit par l'exclusion, soit par restrictions diverses, soit encore par des mesures thérapeutiques - le risque de criminalité représenté par l'individu en question* »[2004].

C'est la doctrine de la défense sociale telle qu'exposée par A. Prins au début du XX[e] Siècle, qui aurait initialement introduit le terme d' « être dangereux » ou de « terribilité », centrée autour de la notion capitale de risque et induisant des législations et des mesures de sécurité centrées sur la notion d' « individu dangereux », destinées à le mettre hors d'état de nuire. Il suffit d'observer l'ensemble de plus en plus gigantesque « *des mesures législatives, des décrets, des règlements, des circulaires qui permettent d'implanter des mécanismes de sécurité* » nécessitant toute une série de techniques différentes, comme les techniques de surveillance par exemple, afin d'assurer cette sécurité[2005]. Ainsi, pour nous protéger efficacement contre les individus dangereux, « *la loi pénale doit sans cesse tracer cette frontière entre « nous » et « eux ». Au fil de ses réécritures, elle sépare inlassablement les délinquants et les honnêtes gens, les bonnes et les mauvaises victimes* »[2006].

La rationalité est, dès lors, laissée de côté au profit de la pulsion criminelle d'une personne pour la juger et se prononcer sur sa capacité d'adaptabilité en vue d'infliger une sanction plus modérée, faisant écho au débat entourant la mise en place de la loi de 2008 relative à la rétention de sûreté[2007]. Le droit pénal a ainsi « *étendu, organisé, codifié le soupçon et le repérage des individus dangereux, de la figure rare et monstrueuse du monomane à celle, fréquente, quotidienne, du dégénéré, du pervers, du déséquilibré constitutionnel, de l'immature, etc.* »[2008].

Dans ce contexte, un individu est jugé pour ce qu'il est, ou ce qu'on suppose qu'il est, indépendamment de l'acte qu'il a commis, et la sanction, au-delà de la peine, peut être accompagnée d'une mesure de sécurité, une mesure de sûreté imposée en raison de son état dangereux. À travers ces mesures de sûreté désormais nécessaires à l'ordre pénal, transparaît la dangerosité qui est profondément ancrée dans le droit pénal contemporain.

La nouvelle doctrine pénale induisant des bouleversements dans le champ pénal a eu, *in fine*, une portée considérable sur le droit pénal, sur la conception du crime et de la peine, mais surtout, sur la société et les individus la composant. Un glissement s'est opéré depuis l'école classique

---

[2004] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Id.*

[2005] M. FOUCAULT, *Sécurité, Territoire, Population*, Cours au collège de France 1977-1978, Coll. Hautes Études, EHESS, Gallimard – Seuil, 2004, Leçon du 11 janvier 1978 - p. 9.

[2006] D. SALAS, *La volonté de punir, op. cit.*, p. 186.

[2007] Loi n° 2008-174 du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental.

[2008] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX[e] siècle », *Ibid.*

passant du criminel, sujet de l'acte, à l'individu dangereux, sujet virtuel de l'acte, caractérisant la volonté de saisir pénalement la virtualité criminelle qui va être l'objet principal des nouvelles politiques criminelles. C'est donc un réalisme punitif par opposition à un angélisme punitif qui se manifeste, marquant le passage de « *l'homme pécheur* » susceptible de pardon, longtemps au centre de la réforme pénitentiaire, à « *l'homme symptôme* » susceptible de traitement par les sciences humaines, caractérisant *ipso facto* la place centrale qu'occupe désormais l'individu[2009].
Ce nouveau réalisme punitif se justifie encore plus dans la mesure où il tend à saisir la demande de toute une société inquiète de la source du danger et se sentant menacée, permettant au politique de se légitimer par son réalisme puisqu'il va saisir à la source la menace, sans se borner à appliquer mécaniquement les dispositions du Code pénal à un fait commis.
Cette nouvelle doctrine de défense sociale porteuse du réalisme punitif autorise, par conséquent, le politique à organiser la réaction sociale en fonction du danger potentiel qui menace la société, le danger ne se référant plus « à l'imputabilité mais à une causalité menaçante »[2010]. Les politiques criminelles modernes vont, dès lors, s'orienter vers la recherche d'un savoir capable de mesurer l'indice de danger d'un individu donné *a priori*, en amont, et non plus après que l'acte ait été commis, afin de prendre toutes les précautions et préventions nécessaires à la protection de la société ; « *bref, l'évaluation des risques entre dans la rationalité pénale* »[2011].
Et qui dit évaluation des risques suggère leur nécessaire anticipation, impliquant par là même une traçabilité, en vue de prévenir ou de désigner un responsable potentiel. Or, avec les dernières avancées technologiques et les pratiques et techniques dorénavant disponibles, même la rationalité pénale se déplace en ce sens que « *le contrôle de la traçabilité occulte l'appel à la responsabilité. Procureurs et policiers trouvent leurs nouvelles normes de référence dans les performances prédictives.* [… Et] *la gestion prévisionnelle des aléas efface le souci d'imputation individuelle. Ce qui compte est d'établir des « profils » à risques et de surveiller les groupes d'individus qui y correspondent* »[2012].

[2009] D. SALAS, *La volonté de punir, Id.*, p. 189.
[2010] D. SALAS, *La volonté de punir, Ibid.*, p. 190.
[2011] D. SALAS, *La volonté de punir, Ibid.*, p. 191.
[2012] D. SALAS, *La volonté de punir, Ibidem*, p. 194-195.

B. Dangerosité, risque et sûreté

Le concept d'individu dangereux permettant à la politique criminelle de chercher un savoir capable de mesurer l'indice de danger d'un individu ou celui d'un comportement donné, à travers les études de personnalités, de traits caractéristiques ou de statistiques, a amorcé l'avènement d'un droit pénal de la précaution et de la prévention ayant de plus en plus recours aux techniques de profilage ou d'enquête de personnalité. La doctrine de défense sociale s'affirme alors plus fortement, s'appuyant sur le réalisme de la défense de la société, se sentant continuellement menacée et en danger, qui implique un nouveau postulat, à savoir l'homme peut être mauvais et dangereux par nature, entraînant par conséquent la nécessité de le mettre hors d'état de nuire au reste de la société. « *Nous voilà donc entrés dans le présent* », prévient Giudicelli-Delage, « *un présent où les codes et les lois n'hésiteraient plus, désormais, à faire place à une pénalité qui donne à la société des droits sur les individus à raison de ce qu'ils sont, et non plus à partir de ce qu'ils ont fait, [...]. Un présent qui serait l'émergence et la recomposition d'une nouvelle, d'une autre pénalité, se construisant autour des notions de dangerosité et de risque, plus que de culpabilité* »[2013].

La teneur de la pénalité, depuis sa conception néoclassique alliant justice et utilité, peut se résumer par l'ancienne formule célèbre « *pas plus qu'il n'est juste, pas plus qu'il n'est utile* »[2014]. La légitimité de la peine repose ainsi sur ces deux principes de juste et d'utile qui servaient, en les combinant, de limite et de balance pour la mission pénale, « *combinaison indispensable, rappelait Garraud, car, isolés l'un de l'autre, le juste et l'utile conduiraient à des conséquences également dangereuses* »[2015]. Le droit pénal doit échapper, d'une part, aux excès de la justice absolue et, d'autre part, à ceux de la défense sociale, pour adopter plutôt une combinaison de l'utilité sociale et de la justice morale. Dans ce contexte, cela doit *de facto* mener vers un droit pénal qui excluerait toute possibilité de sanction en dehors de toute imputabilité, la peine, « *figure du sacré à l'origine* », étant issue « *d'une anthropologie de l'équivalence : le mal infligé doit supprimer le mal subi* »[2016] (une peine n'étant, en effet, juste que si l'acte est reprochable), mais aussi, toute possibilité de distinction entre culpabilité et dangerosité, le droit

[2013] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », RSC 2010, p. 69.
[2014] J.-L.-E. ORTOLAN, *Éléments de droit pénal : Pénalité – Juridictions – Procédure*, t. I, Librairie de Henri Plon, 3ème éd., 1863, p. 92 ; Disponible en ligne : https://gallica.bnf.fr/ark:/12148/bpt6k6147667z/f6.image.texteImage ; R. Merle, A. Vitu, *Traité de droit criminel : problèmes généraux de la science criminelle, droit pénal général*, t. I, Paris, Ed. Cujas, 7ème éd., 1997, p. 112 et *sq*.
[2015] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Id.*, p. 69.
[2016] D. SALAS, *La volonté de punir, Id.*, p. 187.

pénal et la peine combinant simultanément une fonction rétributive et préventive. Les discours politiques récents, destinés à apaiser les victimes et, en même temps, à rassurer l'opinion publique, semblent progressivement rompre l'alliance nécessaire en affichant l'utile sans le juste, tendant à la suppression du lien entre culpabilité et dangerosité et entre peine et imputabilité, aboutissant ainsi « *à vider la responsabilité pénale de toute signification, prise qu'elle serait entre une "dangerosité sans culpabilité" et une "culpabilité sans imputabilité"* »[2017].

La dangerosité apparaît de plus en plus comme une notion autonome, détachée de l'infraction pénale, sans compter qu'elle légitime l'accès à des mesures de sûreté nécessitant plusieurs pratiques et technologies pour les assurer, telles que des mesures de surveillance, de soins, d'interdiction, de fichage, de traçabilité ; l'exemple de la mise sous surveillance électronique mobile[2018] en présente une illustration significative parmi tant d'autres. Ces différentes mesures semblent alors concrétiser et pérenniser la séparation des notions de dangerosité et culpabilité et celles de culpabilité et imputabilité, ces mesures pouvant être prononcées à l'égard d'un individu désigné dangereux alors qu'il a purgé sa peine, ou encore à l'égard d'une personne à risque ou en manque de discernement sans pour autant lui imputer l'acte commis. À ce titre, la Cour de cassation a eu l'occasion de rendre un arrêt jugeant que les mesures de sûreté constituent, en réalité, des peines ou des modalités d'application de la peine sur la base du « principe de la légalité des peines », ce qui permet de constater que le droit français, implicitement certes, permet dorénavant une sanction sans imputabilité[2019].

C'est un mouvement graduel de 'désindividualisation judicaire de la peine' qui s'observe à travers, *inter alia*, une radicalisation et une généralisation des mesures de surveillance, une collecte massive et un « maillage de plus en plus étroit » des fichiers de bases de données personnelles qui, finalement, indique Giudicelli-Delage, permettent « *une traçabilité individuelle, au nom de la dangerosité et du risque* »[2020]. Déjà, Foucault prévenait de « *ce qu'il*

[2017] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Id.*, p. 70.
[2018] Loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales ; Vie-publique, « La loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales », publié le 14 décembre 2005 : « *Cette loi vise à renforcer la répression contre la récidive et institue de nouvelles mesures de suivi des condamnés "dangereux". Elle élargit les catégories de délits permettant de parler de récidive et limite le nombre de sursis avec mise à l'épreuve. [...]. Certains criminels pourront être placés sous surveillance électronique mobile à la demande du juge de l'application des peines. [...]. Ce dispositif pourra aussi être utilisé dans le cadre nouveau de la "surveillance judiciaire" [...].* » : https://www.vie-publique.fr/actualite/panorama/texte-vote/loi-du-12-decembre-2005-relative-au-traitement-recidive-infractions-penales.html
[2019] Cour de cass., Ch. Crim., arrêt du 21 janvier 2009, pourvoi n° 08-83492 : https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000020181010 ; et, P.-J. Delage, « Vérité et ambiguïté autour de l'imputabilité morale - À propos de Crim. 21 janvier 2009 », RSC, 2009, p. 69.
[2020] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Id.*, p. 70.

y aurait de redoutable à autoriser le droit à intervenir sur les individus en raison de ce qu'ils sont [...] »[2021].

Or, au sein des dispositions au cœur du droit pénal moderne, que ce soit en France ou à l'étranger, la dangerosité semble pragmatiquement, de manière explicite ou implicite, constituer le noyau de ces dispositifs légaux, impliquant l'avènement d'un « droit pénal de la dangerosité » et d'un « droit pénal de l'ennemi », centrés autour de l'évaluation de la dangerosité et du risque ainsi que sur le développement croissant des mesures de sûreté. En effet, depuis quelques années, de nouvelles mesures, prises particulièrement au nom de la lutte contre la récidive, telle que la loi de 2005 susmentionnée permettant la mise sous surveillance électronique mobile, ou encore la loi de 2008 sur la rétention de sûreté autonomisant la dangerosité par rapport à la culpabilité et séparant la mesure de sûreté de la peine, permettant ainsi de maintenir un individu en détention de manière renouvelable sur le seul critère de sa dangerosité[2022] et alors même qu'un « *placement en détention provisoire est un marqueur fort de suspicion* »[2023], ressemblent étrangement « à un retour de la défense sociale dans sa forme la plus radicale », indique la Professeure Delmas-Marty : « *bien qu'elles soient présentées comme à l'avant-garde du progrès, soutenues par une industrie de la surveillance en pleine expansion, et réactualisées par le développement des nouvelles technologies (interconnexion des banques de données et corrélation avec les identifiants biologiques), ces mesures semblent renouer avec la doctrine de l'école positiviste* »[2024].

En outre, au sein des mécanismes juridiques étrangers, une prise en compte de la dangerosité s'est accentuée depuis le début du XX^{e} Siècle, que ce soit en Angleterre avec l'emprisonnement à durée indéterminée des délinquants récidivistes quand ces derniers présentaient un danger significatif, ou en Italie avec l'insertion des mesures de sûreté dans leurs codes, ou encore en Allemagne qui, en 1933, instaure un internement de sûreté des criminels dangereux ; mesure de détention-sûreté, introduite dans l'arsenal législatif allemand après l'arrivée au pouvoir des nazis et maintenue par les Alliés en 1945, « *son origine nazie n'a semble-t-il gêné ni les Alliés - il y aurait beaucoup à dire sur l'indifférence, pour ne pas dire l'adhésion à certaines pratiques eugénistes - ni la Cour constitutionnelle fédérale allemande* »[2025]. Ces différentes législations

[2021] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX^{e} siècle », *op. cit.*
[2022] Loi du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, *loc. cit.*
[2023] R. PARIZOT, « Présomption d'innocence *versus* marqueurs de culpabilité : quel équilibre ? », RSC 2019, p. 127.
[2024] M. DELMAS-MARTY, « Les politiques sécuritaires à la lumière de la doctrine pénale du XIX^{e} au XXI^{e} siècle », Introduction, *loc. cit.*, p. 5.
[2025] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Id.*, p. 72.

demeuraient toutefois endormies, notamment dans la période de l'après-guerre et le « climat humaniste » ambiant de l'époque, leur application n'étant que résiduelle[2026].

Mais avec le mouvement de la défense sociale, des réaménagements de ces législations, quoique sous une forme assouplie, se sont manifestés à travers, par exemple, la promulgation d'une loi sur les alcooliques dangereux[2027] ou d'une disposition autorisant la détention « *d'une personne susceptible de propager une maladie contagieuse, d'un aliéné, d'un alcoolique, d'un toxicomane, ou d'un vagabond* »[2028]. En revanche, à partir des années 80-90, un réaménagement plus profond de ces lois anciennes a été entrepris, réactivant des mesures visant la dangerosité tout en produisant, notamment, une distinction entre « délinquants dangereux et délinquants à contrôler », suivi, à l'aube du XXI[e] Siècle, d'une accélération qui s'amplifie tendant vers un durcissement des mesures antérieures, de sorte que « *cela fait donc maintenant plus de vingt ans que, de réactivations en accélérations, se dessinent ces nouveaux droits pénaux de la dangerosité* »[2029]. En effet, précise Giudicelli-Delage, « *il est vrai que l'heure de ces dernières lois n'était pas bien choisie, si l'on considère que l'essor, la réactivation, l'accélération ne se sont produits qu'à des périodes de crises économiques plus ou moins fortes, c'est-à-dire dans des périodes où les populations sont plus facilement accessibles à un discours de peur et d'exclusion* »[2030].

Pourtant, alors même que des mesures de sûreté plus dures et plus fermes se mettaient en place, les statistiques dans certains des États concernés montraient une baisse, ou du moins une stagnation, de la criminalité, sans compter que ces mesures étaient souvent promulguées à l'occasion d'un fait divers ayant eu lieu dans le pays concerné. Quant à l'accélération, elle s'est surtout manifestée après les attentats du 11 septembre ayant marqué la société mondialement et ayant généré un renouveau de peur et de danger. Les pays occidentaux commençaient graduellement à distinguer peines et mesures de sûreté, comme a pu le faire durant ces dernières

[2026] M. DELMAS-MARTY, « Les politiques sécuritaires à la lumière de la doctrine pénale du XIX[e] au XXI[e] siècle », Introduction, *Id.*, p. 6.
[2027] Loi n° 54-439 du 15 avril 1954 sur le traitement des alcooliques dangereux pour autrui.
[2028] Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950, Art. 5, al. 1, point e).
[2029] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Id.*, p. 73.
[2030] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Ibid.*, p. 73.

années la Cour de cassation[2031] ou la Cour constitutionnelle allemande[2032], chaque système juridique les qualifiant ou les nommant différemment mais, foncièrement, elles sont toutes semblables permettant d'écarter l'applicabilité des principes du droit pénal, tel que celui de la non rétroactivité des lois pénales et des peines par exemple. Cette distinction n'est finalement ni claire ni incontestable, « *non seulement parce que toute peine comporte un objectif de prévention et parce que toute mesure de sûreté prononcée par le juge pénal est ressentie par celui qui la subit comme une rétribution/punition, mais encore parce que le droit comparé montre que les mêmes mesures peuvent indifféremment, selon les pays, être qualifiées de peine ou de mesure de sûreté* »[2033].

Par ailleurs, la dissociation entre culpabilité et dangerosité conduit à ce que le principe de proportionnalité ne soit applicable que pour la peine, qui peut être courte, mais pas pour les mesures de sûreté, qui peuvent être longues, et dont le contrôle porte sur l'existence présumée, et non particulièrement sur la gravité, de la dangerosité. En ce sens, la CEDH a eu l'occasion d'affirmer en 2009 que « quant à la gravité de la détention de sûreté – qui n'est pas un critère décisif en soi – la Cour observe qu'il s'agit d'une mesure qui, depuis l'amendement de la loi intervenu en 1998, ne connaît plus de limite de durée. En outre, l'octroi d'un sursis avec mise à l'épreuve est subordonné au constat d'un tribunal selon lequel il ne subsiste pas de risque que le détenu commette de nouvelles infractions (graves), condition qui peut être difficile à remplir (comme le constate le Commissaire aux droits de l'homme selon lequel il est « impossible de prévoir avec certitude si une personne récidivera »). Force est donc de constater que cette mesure paraît être l'une des plus graves de celles prévues par le Code pénal allemand »[2034]. Et la Cour note à cet égard que « *le requérant a eu beaucoup plus à pâtir de la prolongation de sa*

[2031] Cour de cass., Ch. Crim., du 28 mars 2018, Pourvoi n° 17-86.938, qui affirme par exemple : « *Attendu que, si la décision du Conseil constitutionnel du 21 février 2008 interdit qu'une personne soit placée sous le régime de la rétention de sûreté à raison de faits commis avant l'entrée en vigueur de la loi qui a institué cette mesure et a été promulguée le 25 février 2008, il résulte de la même décision que les dispositions de cette loi relatives à la surveillance de sûreté s'appliquent aux faits commis avant son entrée en vigueur ; qu'il s'en déduit que la rétention de sûreté peut être appliquée, conformément aux articles 723-37 et 706-53-19 du code de procédure pénale, à une personne, même condamnée avant l'entrée en vigueur de cette loi, qui méconnaît, après l'entrée en vigueur de cette loi, les obligations qui lui sont imposées dans le cadre de la surveillance de sûreté* ; »

[2032] BVerfG, 5 février 2004, 2 BvR 2029/01, BVerfGE 109, 133 : NJW, 2004, p. 911 et s., note J. Kinzig ; KritV, 2004, p. 137, note T. Mushoff ; RSC, 2004, p. 689, comm. T. Weigend et D. Capitant : Cette distinction, fondamentale en droit allemand, a été validée par la Cour : la détention-sûreté ne visant pas la culpabilité mais le danger que représente le détenu, elle n'est donc pas une peine au sens du droit allemand et dès lors les principes du droit des peines - en l'espèce était en question la non-rétroactivité - ne lui sont pas applicables. Décision condamnée par la CEDH dans l'affaire M. *c*. Allemagne, requête n° 19359/04, du 17 décembre 2009 ; mais revirement de jurisprudence avec l'affaire Ilnseher *c.* Allemagne, Grande chambre, Requêtes no. 10211/12 et 27505/14, du 4 décembre 2018.

[2033] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Id.*, p. 74.

[2034] CEDH, Affaire M. *c.* Allemagne, Requête n° 19359/04, du 17 décembre 2009, point 132.

détention de sûreté – dont la durée est à ce jour plus de trois fois supérieure à celle de la peine d'emprisonnement – que de la peine d'emprisonnement proprement dite », et en conclut que la détention de sûreté doit être qualifiée de peine « *après être allée au-delà des apparences et avoir procédé à sa propre analyse* »[2035].

Cependant, les règles pénales se trouvent perturbées non seulement par l'effet de la distinction entre peine et mesure de sûreté, mais aussi par l'élaboration d'une « présomption d'innocuité », qui, « *transposée des produits aux êtres humains, est pourtant un non-sens* »[2036], ou par la mise en place d'une « présomption de dangerosité » qui impose à la personne en cause de démontrer son absence de dangerosité, à l'image de celle instaurée au Canada en 2008 ; voire, par le développement d'une « justice actuarielle », comme aux États-Unis, qui se base sur des statistiques, essentiellement étrangères au cas et à la personnalité du suspect, afin de déterminer la peine[2037]. Ainsi, comme a pu le constater Tocqueville, « *en Europe, le criminel est un infortuné qui combat pour dérober sa tête aux agents du pouvoir ; la population assiste en quelque sorte à sa lutte. En Amérique, c'est un ennemi du genre humain et il a contre lui l'humanité toute entière* »[2038].

C'est ainsi que la dangerosité travaille et ronge le droit pénal de l'intérieur, celui-ci ressemblant de plus en plus à un droit pénal de la dangerosité au sein duquel existe une multitude de pratiques de sécurité et de maintien de l'ordre ainsi que des mesures de sûretés, parmi lesquels se trouvent des mesures visant des individus en raison d'actes commis, mais aussi en raison d'actes qu'ils seraient susceptibles de commettre au regard de certaines de leurs particularités, de leurs habitudes et comportements, ou en raison de leur appartenance à des groupes qualifiés de terroristes, ou encore à une communauté qualifiée comme étant à risque[2039]. Mises à part les divergences qui peuvent être recensées dans les différents pays appliquant un droit pénal de la dangerosité, certains points communs peuvent être soulevés, concrétisant les formes de dangerosité et d'individu dangereux observées : les individus qualifiés d'incorrigibles ou de dangereux se voient adresser des mesures de rétribution, de prévention voire d'élimination ; s'ils sont considérés incontrôlables et/ou imprévisibles, les mêmes mesures leurs sont adressées, mais dans ce cas, c'est sur le fondement de la prédiction d'un événement ou d'une pulsion criminelle, ou même d'une action ou inaction de sa part. Par conséquent, des mesures de

[2035] CEDH, Affaire M. *c.* Allemagne, du 17 décembre 2009, *Id.,* points 132 et 133.
[2036] M. DELMAS-MARTY, « Les politiques sécuritaires à la lumière de la doctrine pénale du XIX^e^ au XXI^e^ siècle », Introduction, *Id.*, p. 6.
[2037] B. HARCOURT, « Une généalogie de la rationalité actuarielle aux États-Unis aux XIX^e^ et XX^e^ siècles », RSC 2010, p. 31.
[2038] A. DE TOCQUEVILLE, *De la démocratie en Amérique*, t. I, *op. cit.*, p. 164.
[2039] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Ibid.*, p. 74.

neutralisation par le biais d'une surveillance constante et d'une traçabilité continue sont prévues, eu égard au fait qu' « *un sujet à risques est défini par une batterie de réponses à un questionnaire, une accumulation de renseignements et de traces soigneusement stockées. À aucun moment, sa responsabilité n'est réintroduite sauf, s'il y a lieu, au moment d'un jugement. Ni libre, ni déterminée, sa déviance est inscrite en lui à son insu* »[2040].

De même, les figures de la dangerosité, ne se réduisant pas au criminel dangereux, peuvent être cernées ou classées de manière apophatique : parmi les individus classifiés comme étant non-dangereux, certains peuvent engendrer des risques considérables, comme des risques économiques, écologiques, financiers, ou environnementaux. Il apparaît alors que ce n'est pas le risque en soi qui est dorénavant pris en compte de manière objective, mais bel et bien le risque que font courir certaines personnes pour ce qu'elles sont, ou pour ce que les sociétés présument qu'elles sont. Comme a pu le constater Foucault, « *en mettant de plus en plus en avant non seulement le criminel comme sujet de l'acte, mais aussi l'individu dangereux comme virtualité d'actes, est-ce qu'on ne donne pas à la société des droits sur l'individu à partir de ce qu'il est ? Non plus certes à partir de ce qu'il est par statut (comme c'était le cas dans les sociétés d'Ancien Régime), mais de ce qu'il est par nature, selon sa constitution, selon ses traits caractériels ou ses variables pathologiques. Une justice qui tend à s'exercer sur ce qu'on est : voilà qui est exorbitant [...]* »[2041].

En outre, à la fin des années 90, le Professeur Jakobs, en se fondant *inter alia* sur l'exemple des mesures de détention-sûreté allemandes, amorçait l'application d'une doctrine du droit pénal de l'ennemi dans son essai, suscitant une vive réaction et un débat international qui niaient non seulement la validité de la doctrine, mais aussi l'existence même d'un droit pénal de l'ennemi. Pourtant, sa position était de dire qu'il existait déjà un droit pénal de l'ennemi, il ne faisait que le constater de manière neutre et réaliste, alors même que les grands attentats terroristes n'avaient pas encore eu lieu ; cette doctrine visant ainsi tous les dangereux de manière générale. L'analyse de la doctrine de Jakobs montre, de manière schématique, que la dangerosité est appliquée à celui qualifié d' « ennemi » mais la culpabilité est réservée au citoyen, que toute contrainte (garde à vue ou écoute téléphonique, par exemple) est une forme de dépersonnalisation, que « *sauvegarder l'État de droit suppose aussi d'employer des moyens contraires à l'État de droit – justifié par une exigence de réalisme, le droit pénal de l'ennemi le serait encore du fait même que ce sont les individus eux-mêmes qui se sont exclus du jeu en*

[2040] D. SALAS, *La volonté de punir, op. cit.*, p. 193-194.
[2041] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX^e siècle », *Id.*

raison de leurs actes et comportements », mais aussi, que des catégories juridiques peuvent être brouillées dans la mesure où le droit pénal de la dangerosité ne s'affiche pas comme un droit d'exception, et rend possible une « *contamination de l'ordinaire par l'exceptionnel* »[2042].

Dès lors, avec les dernières accélérations observées, *primo*, une dépersonnalisation extrême pourrait conduire vers une déshumanisation, non seulement celle qui repose sur l'emploi de la torture ou de traitements inhumains et dégradants, mais aussi celle qui vise à ramener un individu à une seule caractéristique, sa dangerosité et le risque qu'il représente, voire celle qui consiste à prédire la dangerosité d'un individu en raison de son appartenance à un groupe ou à une communauté particulière, en raison de ses habitudes et comportements, ou encore en fonction des statistiques générées, chosifiant la singularité de l'individu et niant, *de facto*, « l'irréductible » singularité de l'individu, « l'irréductible humain »[2043]. Or, « *réduire un être humain à sa seule dangerosité reviendrait à lui refuser toutes autres caractéristiques que l'on accepterait de reconnaître dans les « autres » membres de la communauté humaine - les « non-dangereux » - et, par ce mouvement réducteur, à refuser d'admettre son égale dignité* »[2044].

Et, *secundo*, les accélérations observées sous-tendent, en plus d'une remise en question de l'État de droit, que l'ennemi devient le « bouc émissaire » de la société, indique Zaffaroni, « *le plus grand scandale que met en exergue aujourd'hui la prétention de théoriser un droit pénal de l'ennemi est qu'elle révèle que le droit pénal l'a toujours théorisé, parce qu'il a abaissé ses drapeaux et qu'il a, ainsi, manqué à sa mission de renforcement de l'État de droit. De là naissent ses multiples équivoques, son refuge dans la scientificité aseptisée, les contradictions politiques de plusieurs de ses auteurs, dont le conditionnement en tant que sujets connaissants les a empêchés de percevoir les traces de composantes de l'État absolu qu'ils incorporaient à leur discours et le fait qu'ils minaient l'État de droit. Le XXI^e^ siècle exige du droit pénal qu'il prenne conscience que l'ennemi n'est pas autre que le bouc émissaire de René Girard, celui que l'on sacrifie dans le massacre pour canaliser toute la violence diffuse de la société et, par conséquent, que tout discours à propos de l'ennemi est un acte préparatoire d'un meurtre, aussi bien que, en dernière analyse, une technique de « neutralisation de valeurs » au sens de Sykes et de Matza, préparatoire de la commission de crimes contre l'humanité* »[2045].

Par ailleurs, un autre enjeu s'annonce, relatif à l'incapacité du système juridique et politique à répondre aux objectifs affichés, tels que l'éradication du crime ou encore la suppression du

[2042] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *Ibid.*, p. 76.
[2043] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », RSC 2010, p. 107 ; et, *Cf.* p. 630.
[2044] P.-J. DELAGE, « La dangerosité comme éclipse de l'imputabilité et de la dignité », RSC 2007, p. 799.
[2045] E. R. ZAFFARONI, « Dans un État de droit il n'y a que des délinquants », RSC 2009, p. 57.

risque même de la commission d'un crime. Se rallie à cette incapacité, le discours politique qui prône et alimente la culture de la peur, que le choc terroriste des attentats de New-York, de Madrid, de Londres, de Belgique ou de France a permis de nourrir. En effet, la « *dangerosité, passant du déterminisme au probabilisme (du criminel né au criminel potentiel, de l'ennemi héréditaire à l'ennemi planétaire) s'inscrit désormais dans le modèle évolutif d'une « société du risque », appelée, au nom du principe de précaution, à anticiper sur des dangers de plus en plus imprévisible* »[2046].

Cependant, d'une part, cela déforme la réalité, compte tenu de la sélection en amont des cibles ; et d'autre part, la transformation de la défense et du contrôle social se concrétise, reposant toujours plus sur la sécurité et la prévention au prix des libertés individuelles. Comme le souligne la Professeure Delmas-Marty, « *face à la globalisation des risques, une vigilance internationale s'est en effet progressivement imposée, au nom du principe dit « de précaution »* [… qui] *se caractérise davantage par l'idée d'anticipation [...]* »[2047].

§2. Une défense sociale centrée sur la peur et la prévention du risque

La défense sociale adoptée, centrée sur la peur des individus et la prévention du risque, semble constituer une réponse face à la mondialisation, la globalisation et le besoin de sécurité en découlant (A), entraînant une illusion de sécurité mais aussi de liberté (B), deux notions aspirant continuellement à être en équilibre.

A. Mondialisation, globalisation et besoin de sécurité

Un nouveau monde voit le jour, un monde où l'État et ses frontières territoriales passent au second plan, marqué par les mouvements de mondialisation et de globalisation qui évoquent la fin des frontières, une liberté et une fluidité de circulation, et une vision extraterritoriale permanente. Plus la mondialisation, qui « *est tout autant un facteur de division que d'unification* »[2048], s'intensifie plus elle bouleverse les repères et les références sociales, nationales, locales des individus, et plus elle éveille un instinct de repli sur soi, d'exclusion, d'angoisse, d'incertitude, de peur face à l'inconnu. *De facto*, plus les flux de la mondialisation s'intensifient, plus le besoin de sécurité s'élargit afin de combler l'incertitude croissante

[2046] M. DELMAS-MARTY, « Les politiques sécuritaires à la lumière de la doctrine pénale du XIX^e^ au XXI^e^ siècle », Introduction, *Id.*, p. 6.
[2047] M. DELMAS-MARTY, *Les forces imaginantes du droit (III) – La refondation des pouvoirs*, Ed. du Seuil, Coll. La couleur des idées, 2007, p. 202.
[2048] Z. BAUMAN, *Le coût humain de la mondialisation, op. cit.*, p. 8.

ressentie par les sociétés à travers ces flux de mobilité de plus en plus incontrôlables. En effet, avec les processus de mondialisation, la « *mobilité accède au premier rang des valeurs désirables, et la liberté de circulation, qui a toujours été un avantage rare et inégalement réparti, devient rapidement le principal facteur de stratification de l'âge moderne et postmoderne* », caractérisant ainsi une mondialisation de la condition humaine « *actuellement soumise à des transformations aux multiples facettes qui sont bien résumées par l'expression "compression spatio-temporelle"* »[2049].

Bauman qualifie la mondialisation de « liquide », qui s'opposerait donc à une mondialisation « solide » que l'État peut facilement encadrer, les flux intenses modernes et postmodernes qui ont pu être observés incarnant bien l'idée de liquidité, de fluidité, de notre époque. Ne serait-ce qu'au sein de l'Union européenne, la liberté de circulation mise en place banalise les frontières et permet une circulation plus fluide des personnes, des marchandises, des biens, des services ou des données ; de même, les accords et traités internationaux banalisent les frontières étatiques pour une liberté de circulation plus fluide des flux, comme le *Privacy Shield*[2050], le CETA/AECG[2051], le NAFTA/ALENA[2052] ou l'ACEUM[2053] pour ne citer que quelques exemples. Cela instigue la vision d'une mondialisation qui peut s'avérer, en raison de son caractère liquide, dense et incontrôlable, source pour les individus de menace, de danger ou d'insécurité, qu'ils soient de nature physique, économique, ou environnementale, puisque remplis d'incertitudes et d'angoisses. Dans cette perspective, une atmosphère d'insécurité permanente s'installe et engendre une peur de l'autre, de sa déviance, aboutissant à une quête permanente de protection et de sécurité de la part des individus, qui vont se retourner alors vers les capacités politiques et étatiques.

Caractéristiques de la modernité et de la société liquides, les incertitudes se trouvent être à l'origine de l'accroissement des « peurs sociales et obsessions sécuritaires »[2054] chez les personnes privées de repères et de références et partageant des liens sociaux fragmentés,

---

[2049] Z. BAUMAN, *Le coût humain de la mondialisation, Id.*, p. 8-9.

[2050] Privacy Shield EU-US, ou Bouclier de protection des données UE-US du 1er août 2016 ; Invalidé par l'arrêt « Schrems II » de la CJUE le 16 juillet 2020, *loc. cit.* : https://www.privacyshield.gov/welcome ; https://www.cnil.fr/fr/le-privacy-shield ; https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-suites-de-larret-de-la-cjue

[2051] Accord économique et commercial global (AECG), ou Comprehensive Economic and Trade Agreement (CETA) signé le 30 octobre 2016 : http://ec.europa.eu/trade/policy/in-focus/ceta/index_fr.htm

[2052] Accord de libre-échange Nord-américain (ALENA) ou North American Free Trade Agreement (NAFTA), du 1er janvier 1994 : https://www.nafta-sec-alena.org/Accueil/Textes-de-laccord/Accord-de-libre-échange-nord-américain

[2053] Accord Canada-États-Unis-Mexique (ACEUM), signé le 30 novembre 2018 : https://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/index.aspx?lang=fra

[2054] Z. BAUMAN, *Le présent liquide : Peurs sociales et obsessions sécuritaires*, Ed. du Seuil, Paris, 2007.

temporaires. Ainsi, confrontées à la multitude de dangers que présente une telle société, les incertitudes individuelles nourrissent un sentiment d'insécurité et de danger de plus en plus croissant, cultivant la peur, en ce sens que « *le sentiment d'insécurité ou son équivalent conjugue partout deux composantes : une peur vécue à la première personne associée dans l'esprit des gens au risque d'être volé ou agressé personnellement, et une préoccupation pour la sécurité qui traduit une inquiétude diffuse concernant le crime et ses causes supposées sans qu'on appréhende nécessairement d'être victime. La peur vécue repose sur l'anticipation d'une atteinte – de la menace à l'agression physique en passant par le vol* »[2055].

Il semble alors que l'appréhension ou l'incertitude ressentie et vécue, ne présentant aucun lien direct avec un danger particulier subi, dépend directement de la constitution et de la sensibilité individuelles, subjectives, variables en fonction des événements. La peur, et donc la conscience des menaces qui guettent, est tout à la fois subjective et circonstancielle générant *ipso facto* une obsession et une demande de sécurité conditionnées par les appréhensions et les incertitudes ressenties, par les peurs et les insécurités vécues, ainsi qu'une société, « *otage de ses peurs*, [qui] *ne peut construire qu'un lien social pauvre et négatif* »[2056].

La mondialisation est porteuse de plusieurs effets, selon Bauman, compte tenu notamment de la « polarisation des valeurs se jouant sur plusieurs plans » redonnant du « *lustre aux anciennes distinctions : riche et pauvre, nomade et sédentaire, "normal" et anormal ou "celui qui enfreint la loi"* »[2057]. Dès lors, elle entraîne une compression de l'espace et du temps ayant des effets sur « *la structuration des sociétés et des communautés, des plus grandes aux plus petites* » ; elle a un impact sur la planification urbaine et la gestion de l'espace induisant des « *tendances contemporaines qui visent à fragmenter et à construire pour exclure* » ; elle influence également la souveraineté politique sujette au « *règne de la mondialisation de l'économie, de la finance et de l'information* » ; elle engendre des conséquences culturelles et, plus particulièrement, une « *division de l'expérience humaine* » et une opposition dans la nouvelle hiérarchie constituée, menant à une « *profonde crise existentielle, faite d'incertitude d'angoisse et de peur* » ; mais elle suscite aussi une tendance à « *criminaliser des cas qui ne sont pas à la hauteur des normes idéales* »[2058].

Dans ce contexte, existe alors une tendance à réduire la question de l'incertitude existentielle, conséquence du processus de mondialisation, à un simple problème de « maintien de l'ordre »,

[2055] H. LAGRANGE, *Demandes de sécurité : France, Europe, États-Unis,* Ed. du Seuil et La République des Idées, Paris, 2003, p. 54.
[2056] D. SALAS, *La volonté de punir, op. cit.,* p. 21.
[2057] Z. BAUMAN, *Le coût humain de la mondialisation, Id.*, p. 10.
[2058] Z. BAUMAN, *Le coût humain de la mondialisation, Ibid.*, p. 11-12.

permettant ainsi de s'apercevoir que « *les préoccupations concernant la « sécurité », que l'on réduit le plus souvent au souci de la protection du corps et des biens, sont au contraire « surdéterminées » : elles reçoivent tout le poids des angoisses engendrées par un des aspects fondamentaux de l'existence actuelle – l'incertitude* »[2059]. Par conséquent, la demande de sécurité dépend largement des faits et évènements et de la peur que ceux-là inspirent, la sécurité caractérisant *in fine* une édification, une articulation intersubjective.

La société « liquide » ainsi remplie d'incertitude existentielle se retourne, dès lors, vers l'État et la capacité politique pour répondre à ses demandes et assurer sa sécurité, capacité qui, cependant, sous les effets de la mondialisation, subit une séparation progressive entre le pouvoir, « *l'efficacité d'action dont jouissait auparavant l'État moderne* », et la politique, « *la faculté d'imposer à l'action une orientation et un objectif* »[2060]. Ce qui creuse un véritable fossé « *entre la globalité du pouvoir et le caractère local de la politique* »[2061], les grandes puissances émergentes, notamment celles du marché, se situant à une échelle qui échappe aux individus, provoquant une alliance inédite entre État et marché, et aboutissant à l'aube du monde numérique, à l'État-entreprise[2062].

Ainsi, le processus de mondialisation implique la remise en question du modèle occidental, antérieurement adopté et fortement promulgué, par « d'autres façons de penser l'institution de la société », se démarquant alors, dans cette logique, de la notion « acritique » de globalisation qui exprime plutôt « un mot d'ordre », et dont le projet est « *celui d'un Marché total, peuplé de particules contractantes n'ayant entre elles de relations que fondées sur le calcul d'intérêt* »[2063]. Et, précise Supiot, « *ce calcul, sous l'égide duquel on contracte, tend ainsi à occuper la place jadis dévolue à la Loi comme référence normative* »[2064], provoquant un environnement (social) où tout devient une question de calcul d'intérêt, y compris les réponses aux demandes de sécurité des populations.

Par ce biais, indique Bauman qui rejoint dans cette affirmation Garland, auteur de la « culture du contrôle »[2065], une société de contrôle généralisée et mondialisée voit le jour, au sein de laquelle les individus sont continuellement sujets à des contrôles technologiques croissants. La

[2059] Z. BAUMAN, *Le coût humain de la mondialisation, Ibid.*, p. 13.
[2060] Z. BAUMAN, *Le présent liquide, Id.*, p. 8.
[2061] Z. BAUMAN, *Le présent liquide*, *Ibid.*, p. 75.
[2062] *Cf.* p. 371-374.
[2063] A. SUPIOT, *La gouvernance par les nombres, op. cit.,* p. 14-15.
[2064] A. SUPIOT, *La gouvernance par les nombres, Id.,* p. 15.
[2065] D. GARLAND, *The culture of control: Crime and social order in contemporary society*, Oxford University Press, 2001 (308p.).

multiplication des contrôles renverse le rapport entre l'acte et la sanction, puisqu'il ne s'agit plus de répondre à un acte commis, mais plutôt de le prédire et le prévenir, de l'anticiper, *via* un contrôle croissant et constant sur les auteurs potentiels pouvant être qualifiés de dangereux ou à risque. Ici, les illustrations ne manquent point, comme la mise en place des contrôles automatiques dans les aéroports ou les gares routières, le développement des passeports biométriques, de la géolocalisation, ou encore des techniques de profilage et de traçabilité ; le tout mis en œuvre dans le but d'entreprendre une intervention préventive et d'identifier les auteurs potentiels dangereux ou présentant des risques et des menaces, moyennant ces techniques et pratiques permettant de les cibler comme tels, pouvant alors induire différents abus, comme l'avait précisé Foucault à travers son étude sur l'individu dangereux. Dans cette perspective, la figure même du délinquant se transforme, étant donné que ce n'est plus l'acte répréhensible qui va être saisi, mais son profil, voire sa posture menaçante ou n'importe quel signe le désignant comme menaçant.

Désormais, par le biais d'un signe ou d'une attitude particulière, il est donc possible de qualifier une personne de terroriste potentiel ou d'individu dangereux pour la société, et si le logiciel de profilage, par exemple, cible la personne concernée comme telle, alors elle sera, de fait, considérée comme terroriste ou dangereuse. En effet, la réalité scientifique prend le dessus dans un monde de contrôle généralisé où tout est pris en compte, la démarche, la posture, la parole, la voix, les traits de visage et ainsi de suite, aboutissant à une identification numérique de la potentialité ou de la pulsion criminelle par le biais d'éléments corporels. Dans le monde numérique, les techniques de recherche d'indices permettent de déceler la présence du barbare, du vagabond, de l'ennemi, les machines développées étant capables de produire des 'identités suspectes' à travers des catégories préalablement déterminées ; c'est indubitablement la « société du tout traçable » touchant les hommes, les animaux ou encore les objets, qui « devient un cauchemar »[2066].

À ce titre, Bauman insiste sur ce phénomène nouveau de la société liquide combinant contrôle social, mutations technologiques, précarisation, ségrégation, ou encore individualisme radical, dans laquelle la vie, de façon globale, est assujettie au temps et à la consommation, et où les êtres humains sont chosifiés au nom du progrès, de l'innovation, voire de l'efficacité[2067]. Dans cette modernité liquide induisant une société « liquéfiée », une démultiplication des angoisses et des incertitudes se manifeste, cultivant un registre de la peur et une forte volonté de se protéger par nécessité. C'est la crainte de l'invasion par l'autre qui menace, ou de la déviance

[2066] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *Id*., p. 107.
[2067] Z. BAUMAN, *La vie liquide*, Ed. de Rouergue-Chambon, Coll. Les Incorrects, 2006, p. 57 et *sq*.

d'un autre, générant la demande de protection et de sécurité adressée au gouvernement et à la justice pour tenter de calmer les incertitudes et réduire l'imprévisibilité des dangers. Cela dit, précise Delmas-Marty, « *l'imprévisibilité des dangers a sans doute augmenté avec les incertitudes accrues dans le domaine économique et social, mais aussi avec les interactions croissantes liées aux nouvelles technologies. Or, l'imprévisibilité des dangers contribue à nourrir la peur. Peur des risques globaux (risques environnementaux comme le changement climatique, ou sanitaires comme les épidémies). Mais aussi la peur de l'autre, quand il apparaît comme une menace : délinquant (auteur de meurtres, d'attentats sexuels, de violences volontaires), ancien délinquant (récidiviste ayant exécuté peine), délinquant potentiel, ou personne seulement potentiellement dangereuse (malades mentaux, étrangers en situation irrégulière, mineurs « à risques »). Et la peur tend à brouiller les frontières entre les réponses aux risques (droit civil ou droit de l'environnement) et les réponses aux menaces (droit pénal)* »[2068].

La peur, indique Bauman, est une force en soi se reproduisant et se suffisant à elle-même, « *dès qu'elle descend sur le monde des humains, la peur acquiert son énergie propre, sa propre logique de croissance : elle n'exige que très peu d'attention et presque aucun investissement supplémentaire pour grandir et se répandre, irrésistiblement* », sans compter qu'elle engendre un cercle vicieux, sans fin, à l'image du serpent qui se mord la queue, dans la mesure où « *nos craintes nous poussent à prendre des mesures défensives qui, à leur tour, confèrent un caractère immédiat et tangible à notre peur* »[2069]. Par conséquent, « *dans une telle société, les sentiments d'insécurité existentielle et les peurs diffuses sont inévitablement endémiques* », détachés de toute rationalité ou de tout réalisme[2070]. La peur peut donc être facilement exploitée pour en tirer de nombreux profits aussi divers que variés, ce que Bauman qualifie de « capital-peur », capital que toute société actuelle comporte de manière variable, selon les États.

En ce sens, les préoccupations sécuritaires de l'opinion publique et du corps social sont recueillies et instrumentalisées en vue d'accomplir une multitude de stratégies et de finalités puisque, « *comme l'argent liquide, prêt pour n'importe quel investissement, le capital-peur est susceptible de produire n'importe quel type de profit, commercial ou politique. Et il est aujourd'hui très exploité. C'est donc la sécurité personnelle qui est devenue l'un des principaux arguments de vente – sinon le principal – dans toutes sortes de stratégies marketing. Le « respect de l'ordre », de plus en plus réduit à la promesse de sécurité personnelle (ou, plus*

[2068] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *Ibid*., p. 107.
[2069] Z. BAUMAN, *Le présent liquide*, *Id.*, p. 18.
[2070] Z. BAUMAN, *Le présent liquide*, *Ibid.*, p. 78.

précisément, corporelle), est devenu l'un des principaux arguments de vente, sinon le principal, dans les programmes politiques et les campagnes électorales »[2071]. Les dernières actualités en matière de numérique ou de politique, tel qu'il a pu être observé, confirment l'exploitation de ce capital-peur, dorénavant facilitée par le capitalisme de surveillance[2072].

Ainsi, ce capital-peur peut être investi différemment afin de générer des profits politiques, en fonction de l'enjeu politique du moment, à travers les discours politiques principalement, des profits économiques, financiers ou médiatiques. *In fine*, ce capital-peur est une constante de la société mondialisée, ce qui pousse Bauman à affirmer, avec réalisme, que tout gouvernement a tout intérêt à maintenir un volume de peur officiel lui permettant de l'instrumentaliser et de l'exploiter suivant les stratégies, les finalités et les volontés du moment. Dans ce contexte, les États entretiennent la peur pour opérer un contrôle et une surveillance plus efficace de la société, tout en se positionnant comme meilleur défenseur des dangers qui menacent, caractérisant *ipso facto* la genèse de l'État sécuritaire. Conséquemment, c'est toujours plus de discours politiques portant sur la sécurité et la défense, plus de dépenses et de budgets prévus pour la sécurité et la défense, plus de promesses prononcées, afin d'apaiser l'anxiété des populations. La peur constitue indéniablement un capital d'une particulière utilité pour les sociétés marchandes et démocratiques, entraînant simultanément la nécessité d'avoir plus de défense face à une adversité grandissante et un capital-peur entretenu avec intérêt[2073].

À cet égard, ce furent principalement les évènements du 11 septembre 2001 qui ont facilité l'augmentation de manière assez significative, dans la majorité des États occidentaux, des législations en matière de prévention et de sécurité, des organismes et brigades mis en place pour la défense ou la sécurité, des différentes techniques et pratiques informatiques propres à la sécurité et à la défense, des budgets abondants alloués à la défense et la sécurité du territoire, au nom du besoin de sécurité et de protection face à la menace terroriste que les attentats ont réactualisée et que d'autres attentats, survenus quelques années plus tard, ont consolidé[2074]. Pourtant, seuls les États-Unis étaient touchés par ces attentats, mais la sensibilité de la société face à ce drame, fortement médiatisé, a été exploitée et instrumentalisée permettant aux gouvernements d'adopter des mesures sécuritaires draconiennes et d'instaurer un état de vigilance permanent.

[2071] Z. BAUMAN, *Le présent liquide*, *Ibidem.*, p. 22.
[2072] *Cf.* p. 371, 380 et 444.
[2073] *Cf.* p. 390.
[2074] *Cf.* p. 498 et s.

Ces mesures et pratiques sécuritaires peuvent ainsi, entre autres, viser un « *durcissement du contrôle des migrations alors que les frontières s'ouvrent aux marchandises et aux capitaux* », produire une « *aggravation des exclusions sociales, alors que la prospérité économique globale s'accroît* », faciliter « *la multiplication des menaces sur l'environnement* » face à *« l'aspiration des États au développement économique* », ou encore contribuer « *à la persistance des crimes internationaux "les plus graves"* » face à « *la résistance des États et parfois à l'implication des entreprises transnationales* »[2075]. Ce qui permet de mesurer « *les faiblesses des droits de l'homme face à la puissance des marchés* », d'observer « *les insuffisances du droit mondial* », ou encore de constater « *l'impuissance de la justice pénale universelle* », voire de découvrir « *comment le rêve de libérer l'homme de ses contraintes porte en lui les risques d'asservissements créés par les nouvelles technologies tels que la marchandisation du corps et/ou la globalisation de la surveillance* »[2076].

Cela permet alors de comprendre, indique Delmas-Marty, « *comment la mondialisation conjugue les faiblesses de l'universalisme juridique aux effets de la globalisation économique pour favoriser les risques de déshumanisation* »[2077].

B. L'illusion de sécurité et de liberté

La conciliation entre sécurité et liberté fait constamment l'objet d'un débat prédominant, notamment, dans les domaines politique et juridique. En France, ce fut principalement la loi renforçant la sécurité et protégeant la liberté des personnes[2078], plus communément connue sous sa forme abrégée loi sécurité et liberté, qui a ravivé ce débat en caractérisant l'alliance difficile entre ces deux notions porteuses de valeurs fondamentales nécessaires pour le corps social. Cette loi fit l'objet d'un contrôle de constitutionnalité devant le Conseil constitutionnel qui a indiqué qu'une conciliation « *doit être opérée entre l'exercice des libertés constitutionnellement reconnues et les besoins de la recherche des auteurs d'infractions et de la prévention d'atteintes à l'ordre public, notamment à la sécurité des personnes et des biens, nécessaires, l'une et l'autre, à la sauvegarde de droits de valeur constitutionnelle* »[2079] ; position confirmée et

[2075] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper*, Ed. du Seuil, 2013, p. 17.
[2076] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper*, *Id.*, p. 17.
[2077] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper*, *Ibid.*, p. 16-17.
[2078] Loi n° 81-82 du 2 février 1981 renforçant la sécurité et protégeant la liberté des personnes.
[2079] Conseil Constitutionnel, Décision n° 80-127 DC du 20 janvier 1981 - Loi renforçant la sécurité et protégeant la liberté des personnes, point 62 ; le Conseil affirme, par ailleurs, que *« […]si la législation française a fait une place importante à l'individualisation des peines, elle ne lui a jamais conféré le caractère d'un principe unique et absolu prévalant de façon nécessaire et dans tous les cas sur les autres fondements de la répression pénale ; qu'ainsi, à supposer même que le principe de l'individualisation des peines puisse, dans ces limites, être regardé comme l'un des principes fondamentaux reconnus par les lois de la République, il ne saurait mettre obstacle à ce*

maintenue par la suite dans la jurisprudence du Conseil qui, en matière de sécurité et de liberté, reste centré sur une conception de la sécurité largement marquée par l'ordre public, et se contente d'affirmer que « *le législateur a adopté des dispositions qui assurent, entre la sauvegarde de l'ordre public et la garantie des droits constitutionnellement protégés, une conciliation qui n'est pas manifestement disproportionnée* »[2080].

Compte tenu des attentes et des demandes de plus en plus fortes et étendues en matière de sécurité, la confrontation entre la sauvegarde de l'ordre public et la garantie des droits constitutionnellement protégés peut paraître réductrice, dénotant la volonté des magistrats de laisser une grande marge de manœuvre au législateur en matière de sécurité et sa conciliation avec la liberté. Néanmoins, la position adoptée par le Conseil n'a nullement amenuisé l'ardeur des débats confrontant ces deux notions, demeurant « *vifs, voire polémiques, souvent colorés de préoccupations partisanes* »[2081]. En outre, « *faire valoir que le souci de sécurité ne peut contrecarrer la liberté, aller jusqu'à soutenir comme le font tant de discours politiques qu'il en est même la condition première, peut paraître procéder d'une analyse de fond trop rapide, pour parvenir à des conclusions apparemment rassurantes* »[2082].

Bauman, dans sa réflexion sur les obsessions et mesures sécuritaires, entreprend une analyse de cette conciliation équilibrée entre liberté et sécurité, qu'il trouve impossible et paradoxale, et que l'ère de la mondialisation et de la consommation, porteuse d' « infortunes individuelles » et de « frissons existentiels », a accentué, en renversant les anciennes tendances qui faisaient privilégier la liberté au détriment de la sécurité[2083]. Au demeurant, toute augmentation de liberté peut être vécue comme une baisse de sécurité, ce qui conduit à ce que trop de liberté soit en permanence compensé par un surplus de sécurité, dans un monde où l'incertitude et la peur sont en croissance progressive démultipliant, par conséquent, les obsessions sécuritaires face à la criminalité, le terrorisme, la maladie, l'alimentation, l'environnement, l'économie, et ainsi de suite. C'est un paradoxe auquel tant la société moderne que la société postmoderne se trouve confrontée : deux valeurs contradictoires sont, de manière égale, proportionnelle et conciliatrice, convoitées, toutes deux indispensables à la vie et à une véritable autonomie de l'individu.

---

que le législateur, tout en laissant au juge ou aux autorités chargées de déterminer les modalités d'exécution des peines un large pouvoir d'appréciation, fixe des règles assurant une répression effective des infractions ; », point 16.

[2080] Conseil Constitutionnel, Décision n° 2010-613 DC du 7 octobre 2010 - Loi interdisant la dissimulation du visage dans l'espace public, point 5 ; et, *Cf.* p. 174, 190, 297 et s., 415 et s.

[2081] O. SCHRAMECK, « Sécurité et liberté », RFDA 2011, p. 1093.

[2082] O. SCHRAMECK, « Sécurité et liberté », *Id.*, p. 1093

[2083] Z. BAUMAN, *Le présent liquide*, *op. cit.,* p. 22.

Selon le Professeur, c'est le « *phénomène de « l'inversion du pendule ». Si l'on considère que deux valeurs essentielles, la liberté et la sécurité, structurent notre vie sociale et politique ; alors la grande majorité de ma vie s'est déroulée à une époque où les gens voulaient plus de liberté et étaient prêts à renier un peu de sécurité dans le but d'obtenir plus de liberté. Aujourd'hui le pendule est en train de s'inverser.* [Les gens] *sont en effet prêts à abandonner une part de leur liberté dans le but de bénéficier de plus de sécurité* »[2084]. Mais l'auteur insiste sur le fait que « *cette tendance ne fait que renforcer la réalité dérégulée de la mondialisation, du fait que les racines de la « liquidité » sont mondiales et que cette « inversion du pendule » ne concerne pas du tout ce niveau systémique – il n'est effectif qu'au niveau individuel, même massif. En se coupant nous-mêmes de ces réalités globales et en « prenant soin de notre sécurité locale », nous ne faisons que nous priver d'une part de nous-mêmes au lieu de tenter de résoudre des problèmes générés à l'échelle globale. En ne nous occupant que de nos « petits jardins », nous préférons des solutions hypocrites et rassurantes qui finiront bien par nous apparaître pour ce qu'elles sont : incohérentes* »[2085].

Par ailleurs, Bauman observe que, progressivement, la question de la sécurité, « qui est relative à la condition existentielle », s'est transférée, « de manière mensongère », vers la question de la sûreté, qui se réfère plutôt au fait d'être physiquement à l'abri d'individus considérés malveillants, dangereux ou indésirables[2086]. Or, la sécurité se distingue de la sûreté et ne doivent pas faire l'objet d'une confusion, pas plus que la liberté et la sûreté, cette dernière comprenant « *un noyau dur des libertés qui s'attache à la personne humaine dans son autonomie irréductible* », constituant ainsi une condition de sa sécurité sans pour autant évoquer toutes les implications ou toutes les applications de celle-ci[2087]. Néanmoins, comme il a pu être observé, la modernité et la postmodernité assistent plutôt à un foisonnement des mesures de sûreté au nom de la sécurité et de la défense. À ce titre, M. Ancel en 1966, dans la défense sociale nouvelle, souligne que les mesures de sûreté, qui doivent être soumises au principe de légalité et à l'intervention judicaire, « *constituent ainsi les instruments d'action d'une politique*

[2084] S. TABET, « Du projet moderne au monde liquide. Entretien avec Zygmunt Bauman », Socio - La nouvelle revue des sciences sociales, Ed. de la Maison des sciences de l'homme, n° 8, juin 2017, Zygmunt Bauman, critique de la modernité/Entretien (p. 35-56), p. 50 : https://hal.archives-ouvertes.fr/hal-01565599/document
[2085] S. TABET, « Du projet moderne au monde liquide. Entretien avec Zygmunt Bauman », *Id.,* p. 50.
[2086] S. TABET, « Du projet moderne au monde liquide. Entretien avec Zygmunt Bauman », *Ibid.,* p. 55.
[2087] O. SCHRAMECK, « Sécurité et liberté », *Id.*, p. 1094.

criminelle inspirée sans doute par les données de la science, mais envisagées avant tout comme un art social de lutte contre le crime, dont le droit pénal lui-même est un moyen »[2088].

À la même époque, Ancel se penche sur la question des mesures *ante delictum* en considérant que, par le biais d'une « logique interne », la politique criminelle fondée sur la protection, la précaution et la prévention, sera inévitablement menée à prendre des mesures de sûreté pré-délictuelles : « *Si en effet la mesure de sûreté est considérée, non sous son seul aspect juridique, qui l'oppose à la peine, mais comme l'instrument d'une réaction sociale rationnelle contre le crime, on peut se demander si cette politique criminelle nouvelle n'est pas conduite, par une sorte de logique interne, à préconiser des mesures de sûreté ante delictum. L'état dangereux ou les manifestations dangereuses de la personnalité de l'individu peuvent en effet se manifester avant même qu'une infraction proprement dite ait été commise. L'admission comme base de la Politique criminelle des notions de prévention et de protection ne conduira-t-elle pas alors presque nécessairement à ces mesures de sûreté pré-délictuelles ?* »[2089]. Toutefois, l'auteur, en 1981, revient sur ses positions, en émettant plusieurs observations lui permettant de conclure qu'une politique criminelle de défense sociale « saine » doit, prioritairement, défendre l'Homme, et surtout, l'Homme dans son milieu social, tout en affirmant que les mesures de sûreté *ante delictum* discrétionnaires représentent l'« adversaire » de la défense sociale, et citant un auteur qui, après avoir soutenu pendant longtemps la prise en considération des risques et des caractéristiques dangereuses afin de justifier de telles mesures, se ravise après avoir aperçu « *les dangers qu'une telle politique criminelle pouvait faire courir à la liberté individuelle* »[2090].

Néanmoins, même après avoir changé d'opinion, un argument cité lors des débats confrontant le droit pénal classique et la défense sociale caractérise en quelque sorte les pratiques actuelles, et met en lumière une évidence vécue à l'ère numérique, qui a pu être observée à travers les développements de cette étude : en effet, l'argument consistait à dire que « *si le critère de l'état dangereux, posé par les sciences criminologiques et décelé par la clinique criminologique, présentait une sécurité absolue, le juriste, qui saurait que tel sujet va inéluctablement commettre un délit, pourrait et devrait prendre la mesure préventive appropriée. Mais ni la science ni l'art criminologique n'en sont là* »[2091] ; désormais, ils en sont là.

[2088] M. ANCEL, *La défense sociale nouvelle*, Paris, Cujas, 2ème éd., 1966, p. 210-211.
[2089] M. ANCEL, *La défense sociale nouvelle, Id.*, p. 267.
[2090] J. DANET, « Les politiques sécuritaires à la lumière de la doctrine de la défense sociale nouvelle », RSC 2010, p. 49.
[2091] « Confrontation du droit pénal classique et de la défense sociale », XIIe Journées de défense sociale, RSC 1964, p. 721 ; cité par J. DANET, « Les politiques sécuritaires à la lumière de la doctrine de la défense sociale nouvelle », *Id.*, p. 51.

En outre, Ancel relève également les limites des experts psychiatres, notamment dans le régime de responsabilité atténuée mis en œuvre, soulignant que « *les illusions que l'on pouvait avoir au début du siècle sur la possibilité pour le médecin-expert de doser presque mathématiquement la responsabilité du sujet ont rapidement disparu* »[2092]. Ces pratiques illusoires semblent toutefois réapparaître dans la modernité et la postmodernité centrées, principalement, sur la précaution et la prévention et les mesures sécuritaires et préventives compte tenu de l'avancée et du développement de la science, du droit, de la criminologie et de la technologie, accordant tous les moyens et toutes les garanties scientifiques nécessaires pour pouvoir désormais adopter des mesures préventives anti-délictuelles fondées « *scientifiquement sur une appréciation rigoureuse de l'état dangereux pré-délictuel* »[2093].

L'étude et l'analyse de l'individu dangereux et de la dangerosité, voire de la personnalité du délinquant, ont continué à se maintenir et à se développer, au nom de la défense et de la sécurité nationale, alors même qu'elles risquent de porter atteinte aux libertés individuelles. Le contrôle du juge, à la lumière des données scientifiques, constituera l'étape suivante, « *un juge éclairé par la Science et protecteur de la société, telle est encore l'idéal, l'utopie de la Défense sociale nouvelle* »[2094].

Ainsi, les libertés sont mises en péril au nom de la sécurité qui apparaît comme gage de protection pour les individus face à l'ère du danger, de la relativité et de l'incertitude, caractéristiques de la mondialisation et de la globalisation émergentes[2095]. L'anéantissement des « idéologies rassurantes et le désenchantement du monde »[2096] placent l'individu au cœur de la société des menaces, le poussant à se protéger lui-même et à investir pour assurer sa sécurité, contribuant par conséquent au développement du marché de la sécurité. En effet, le délitement de l'État providence et les nombreuses crises l'affectant ont rompu le pacte social de l'après-guerre et l'esprit de liberté qui l'animait, de sorte que, « *à partir du milieu des années 1970, une insécurité polymorphe s'installe durablement* »[2097], remettant en cause la conception de la sécurité.

Dès lors, de nombreux risques et incertitudes voient le jour menant à un foisonnement massif des demandes et exigences de sécurité, qu'elle soit nationale, sociale, environnementale,

---

[2092] J. DANET, « Les politiques sécuritaires à la lumière de la doctrine de la défense sociale nouvelle », *Id.*, p. 60 (Note de bas de p. n° 72).
[2093] J. DANET, « Les politiques sécuritaires à la lumière de la doctrine de la défense sociale nouvelle », *Ibid.*, p. 52.
[2094] J. DANET, « Les politiques sécuritaires à la lumière de la doctrine de la défense sociale nouvelle », *Ibidem*, p. 52.
[2095] *Cf.* p. 480.
[2096] O. SCHRAMECK, « Sécurité et liberté », *Id.*, p. 1094.
[2097] D. SALAS, *La volonté de punir, op. cit.,* p. 42.

sanitaire, économique, alimentaire, financière, voire orientée vers l'avenir dans une perspective de développement durable dû à la « *crainte de l'épuisement des ressources naturelles* »[2098]. À ce titre, « *le développement durable devient vite une formule passe-partout* », indique Delmas-Marty, et « *risque de servir à couvrir les dissymétries et de devenir un « discours de légitimation » du commerce* » à l'échelle mondiale[2099]. Quelle que soit finalement la forme de sécurité recherchée, celle-ci est « *amplifiée par sa résonance psychologique, un sentiment de crainte, voire de désarroi né de ce que même une sécurité partielle, difficilement et opiniâtrement atteinte, n'apparaît jamais comme un fait définitivement acquis* »[2100]. Ces sentiments de peur et de menace se propagent et se diffusent en conséquence, touchant l'ensemble des hiérarchies sociales, facilitant ainsi « *la transposition du principe de précaution des risques naturels ou technologiques à la criminalité, réelle ou potentielle, au point de justifier presque sans protestation du public, l'autonomisation de la dangerosité, le scandale des sites noirs et de la torture, ou cette redoutable transposition du concept de traçabilité [...]* »[2101].

Dès lors, l'obsession de sécurité a entraîné une prolifération des législations et des règlementation sécuritaires et préventives, menant à la création du concept de sécurité juridique comme garantie face à l'inflation des normes juridiques aspirant à répondre à tous les aléas de la vie, ainsi qu'à un asservissement, une oppression, des libertés et des droits fondamentaux des personnes. Or, « *il n'y a pas de liberté, ferment de la recherche et du développement, sans prise de risques* », les débats entourant les principes de précaution et de prévention, érigés dorénavant au rang constitutionnel, révèlent la fragilité de cette alliance entre sécurité et liberté, sans compter que « *la restriction des libertés, qui se réclame parfois de l'exigence de sécurité, peut au contraire justifier ou au moins dissimuler la pire des insécurités. L'État nazi a organisé la shoah, l'État soviétique le goulag. Celui-ci n'a pu éviter Tchernobyl, avant qu'un libéralisme débridé ne soit à son tour dénoncé pour son rôle dans la catastrophe de Fukushima ; et sur un tout autre plan, les « printemps arabes » ont clairement montré que la sécurité peut être l'alibi de l'étouffement des libertés* »[2102].

[2098] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper*, *op. cit.*, p. 53.
[2099] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper*, *Id.*, p. 55.
[2100] O. SCHRAMECK, « Sécurité et liberté », *Id.*, p. 1095.
[2101] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *loc. cit.*, p. 107.
[2102] O. SCHRAMECK, « Sécurité et liberté », *Id.*, p. 1095.

En réalité, les notions de liberté et sécurité, évoquant plus la contradiction que la conciliation, ne se situent pas juridiquement sur le même pied : la liberté est « un idéal saisi par le droit »[2103], édictée dans les divers dispositifs de protection des droits de l'homme, affirmant que « *toute personne a droit à la liberté* »[2104], qu'elle représente un « *droit naturel et imprescriptible de l'Homme* »[2105] dont le fondement est constitué par la « *reconnaissance de la dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables* »[2106], puisque « *l'ignorance, l'oubli ou le mépris des droits de l'Homme sont les seules causes des malheurs publics et de la corruption des Gouvernements* »[2107], et que « *la méconnaissance et le mépris des droits de l'homme ont conduit à des actes de barbarie qui révoltent la conscience de l'humanité et que l'avènement d'un monde où les êtres humains seront libres de parler et de croire, libérés de la terreur et de la misère, a été proclamé comme la plus haute aspiration de l'homme* »[2108]. La sécurité, toutefois, caractérise la recherche d'une tranquillité, d'une sauvegarde, qui se trouve être pourtant à la merci des faits divers, et ne peut donc *« être considérée comme une valeur fondatrice, un concept juridique intangible mais comme une finalité toujours recherchée, opiniâtrement poursuivie, jamais atteinte* »[2109]. Mais la propagation de la peur, des risques et des incertitudes a transformé la conception de la sécurité tout en élaborant un « nouveau modèle fondé sur le risque et la précaution »[2110], un changement accentué et démultiplié depuis les attentats du 11 septembre, l'érigeant en valeur fondamentale sacrée qu'il faut à tout prix assurer.

De ce fait, plusieurs rapports et études tentent de modéliser les corrélations entre différentes catégories de risques globaux en vue de désigner, facilement et le plus tôt possible, un ennemi clairement identifié[2111] ; mais il est « *plus facile aussi d'utiliser systématiquement le fait divers,*

[2103] O. SCHRAMECK, « Sécurité et liberté », *Ibid.*, p. 1095.
[2104] Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950, Art. 5.
[2105] Déclaration des Droits de l'Homme et du Citoyen de 1789, Art. 2.
[2106] Déclaration universelle des droits de l'homme de 1948, préambule.
[2107] Déclaration des Droits de l'Homme et du Citoyen de 1789, préambule.
[2108] Déclaration universelle des droits de l'homme de 1948, préambule.
[2109] O. SCHRAMECK, « Sécurité et liberté », *Id.*, p. 1095.
[2110] D. SALAS, *La volonté de punir, Id.,* p. 195.
[2111] Par ex., World Economic Forum, Global Risks 2018, The Global Risks Report 2018, 13th edition, Genève: "*Each year the Global Risks Report works with experts and decision-makers across the world to identify and analyze the most pressing risks that we face. As the pace of change accelerates, and as risk interconnections deepen, this year's report highlights the growing strain we are placing on many of the global systems we rely on. The Global Risks Report 2018 is published at a time of encouraging headline global growth. Any breathing space this offers to leaders should not be squandered: the urgency of facing up to systemic challenges has intensified over the past year amid proliferating signs of uncertainty, instability and fragility.*
This year's report covers more risks than ever, but focuses in particular on four key areas: environmental degradation, cybersecurity breaches, economic strains and geopolitical tensions. And in a new series called "Future Shocks" the report cautions against complacency and highlights the need to prepare for sudden and dramatic disruptions.": https://www.weforum.org/reports/the-global-risks-report-2018; http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

qui paraît s'imposer avec la force de l'évidence, alors qu'il permet toutes sortes de manipulations et n'est rien d'autre qu'une diversion »[2112]. Dans ce contexte, indique Delmas-Marty, « *la diversion, et la confusion, ainsi créées entre les exemples les plus particuliers (le dernier fait divers et la compassion bruyamment exprimée à l'égard des victimes) et les études de risque les plus générales, inspirées des méthodes relatives aux risques globaux, conduisent tout droit à l'illusion qu'il existe un moyen d'abolir le hasard et de prévenir les menaces : exclure toute personne identifiée comme dangereuse* », lui permettant conséquemment d'en déduire que « *diversion, confusion et illusion s'unissent alors pour démontrer que la sécurité est un droit qui doit l'emporter sur les libertés et finalement justifier le recours à la force* »[2113]. C'est bel et bien l'avènement de « l'ère spéculative », où le danger invisible qui environne les personnes crée une « communauté de la peur », dominée par la souffrance des victimes qui « ont des voix, des yeux et des larmes » et à laquelle répond « un totalitarisme légitime de la prévention »[2114] ; « *Ainsi se sédimente dans nos vies "l'inacceptable", au nom d'une exigence démultipliée de protection et de sécurité* »[2115].

Cependant, il est utile de noter qu'il n'existe pas véritablement de choix entre liberté et sécurité dans un État de droit qui ne peut garantir une sécurité absolue, « *qui serait contraire à la condition humaine* »[2116], en préconisant les droits de l'homme. Mais depuis le 11 septembre 2001, la multiplication des attentats en Europe, et l'accroissement des flux migratoires, un retour aux concepts de l'individu dangereux et de la dangerosité s'est manifesté avec force, caractérisant un esprit sécuritaire « *devenu à ce point dominant qu'il entraîne la négation des droits fondamentaux et le renouveau des pratiques guerrières qui mènent à la déshumanisation du droit pénal et à la dépersonnalisation de l'individu* », et engage donc « *le contrôle social dans une logique infernale où chaque attentat – voire chaque fait divers – appelle une nouvelle réforme sans que l'on puisse entrevoir la fin d'un tel engrenage* »[2117].

Même la notion de dangerosité est en elle-même fondée sur une incertitude, impliquant une évaluation de l'état de dangerosité, entendue par le Code de procédure pénale comme « *une probabilité très élevée de récidive* [en raison] *d'un trouble grave de la personnalité* »[2118], alors que c'est un terme « *lui-même difficile à manier car il est impossible de prédire avec exactitude*

[2112] M. CRÉPON, *La culture de la peur - I. Démocratie, identité, sécurité*, Galilée, 2008, p. 67.
[2113] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *Id*., p. 108.
[2114] U. BECK, *La société du risque : Sur la voie d'une autre modernité*, Paris, Ed. Aubier, Coll. Alto, 2001, p. 111 et 145.
[2115] M. CRÉPON, *La culture de la peur - I. Démocratie, identité, sécurité*, *Id.,* 4ème de couverture.
[2116] M. DELMAS-MARTY, *Aux quatre vents du monde – Petit guide de navigation sur l'océan de la mondialisation*, Ed. du Seuil, 2016, p. 83.
[2117] M. DELMAS-MARTY, *Aux quatre vents du monde*, *Id.,* p. 83.
[2118] Code de procédure pénale, Art. 706-53-13 (Modifié par Loi n°2010-242 du 10 mars 2010 - art. 1)

qui commettra des actes dangereux à l'avenir. Ces mauvaises prédictions peuvent entraîner non seulement la détention inutile de nombreuses personnes, sans que la société soit protégée, mais aussi une anxiété accrue dans la population »[2119]. Les dispositions relatives aux droits de l'homme avaient tenté de substituer une « *anthropologie humaniste à une anthropologie guerrière* », toutes deux ayant finalement subi des évolutions : « si la perspective guerrière s'est élargie, d'une anthropologie déterministe à une anthropologie « probabiliste », qui intègre des études statistiques de probabilité, la perspective humaniste, grâce au principe de la dignité humaine, s'est approfondie, du libre arbitre qui valorise les libertés, à l'égale dignité qui symbolise « l'irréductible humain », qui n'est ni la vie, ni la liberté, mais ce mystère qui fait que « tout homme est tout l'homme » »[2120]. Cela dit, le retour de la dangerosité marque l'émergence d'une nouvelle pénalité centrée sur la dialectique du risque et de la précaution, accompagnant, parallèlement, les développements de la dangerosité.

L'échangeur dont parlait Foucault, caractérisé par la notion du risque, contribue « *insidieusement, lentement et comme par en bas et par fragments* » à organiser une « *pénalité sur ce qu'on est* » au nom de la sécurité[2121], préoccupation constante de la modernité et de la postmodernité, générant une politique sécuritaire « condamnée à entretenir l'inquiétude dont elle entend nous préserver » et imposant des « contraintes juridiques, techniques mais aussi psychologiques qui elles-mêmes peuvent être génératrices d'insécurité », sans compter que « les polémiques sur les chiffres de la délinquance, toujours récurrentes, renforcent l'incertitude et le désarroi »[2122]. Dans ce contexte d'insécurité, les citoyens veulent se sentir protégés mais, la plupart du temps, ne souhaitent pas véritablement savoir de quelle manière cette protection est assurée : *« Thus the openness mantra of Progressive Era reformers has been neatly reversed in favor of a Faustian (and credulous) bargain : just keep us safe and we won't ask about the details* »[2123].

Dès lors, afin d'assurer la protection revendiquée, la politique criminelle se développe graduellement autour des notions de risque et de dangerosité, notions qui ressurgissent, tout à

[2119] Comité Européen pour les problèmes criminels (CDPC) - Conseil de coopération pénologique (PC-CP), « La condamnation, la gestion et le traitement des délinquants "dangereux" », Rapport final rédigé par N. Padfield, Conseil de l'Europe, Strasbourg, 20 décembre 2010, PC-CP (2010) 10 rév 5, p. 33, point 108 : https://rm.coe.int/168070d6c8

[2120] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *Id.*, p. 108, et, M. DELMAS-MARTY, *Aux quatre vents du monde*, *Id.,* p. 85.

[2121] M. FOUCAULT, « L'évolution de la notion d'«individu dangereux» dans la psychiatrie légale du XIX^e^ siècle », *loc. cit.*

[2122] O. SCHRAMECK, « Sécurité et liberté », *loc. cit.*, p. 1094-1095.

[2123] F. PASQUALE, *The Black Box society, op. cit.,* p. 13.

la fois, à travers la question des anormaux mentaux, les concepts de dol éventuel et de mise en danger d'autrui, la multiplication des infractions-obstacles et formelles, les infractions de risque, ou encore les régimes d'exception établis au nom du risque, envahissant progressivement la sphère du droit commun avec une prolifération des lois, comme les lois sur la récidive par exemple, et induisant *in fine* la restructuration de cette nouvelle pénalité ; structuration à laquelle se joignent également les aspirations européennes visant à promouvoir, difficilement, une Europe de la liberté et de la sécurité et de la justice qui entend répondre, simultanément, aux menaces et aux risques pour la sécurité. D'où l'inadéquation des réponses apportées, indique Delmas-Marty, réponses « *marquées par une certaine porosité entre différents secteurs du droit : l'évolution de la responsabilité civile, de la réparation à la prévention, puis à la précaution, transposée en droit pénal, contribue à légitimer, au nom de la sécurité, l'atteinte à des libertés (liberté d'aller et venir), ou à des droits essentiels (l'égale dignité, le droit à la vie privée)* »[2124].

En outre, le risque, à l'instar de la dangerosité, « *met à distance l'individu, lui applique un modèle statistique, une échelle d'intensité, une catégorie comportementale* », et prévenir « *c'est d'abord surveiller, c'est-à-dire se mettre en position d'anticiper l'émergence d'évènements indésirables au sein de populations statistiques signalées comme porteuses de risques* »[2125] ; concrétisant, par là même, le modèle de la précaution et de la prédiction engendrant une rupture dans la rationalité pénale. En effet, « *le besoin de sécurité, ferment d'inquiétude inévitable et parfois même nécessaire, en appelle au-delà à la solidarité, au sentiment de l'altérité, aux eaux mêlées de notre société interconnectée* »[2126] mais de manière renouvelée, rompant avec la tradition, invoquant les « *solidarités de combat reposant sur l'opposition binaire « ami/ennemi », chère à Carl Schmitt* »[2127], et la pérennisation d'un droit pénal de l'individu dangereux, d'un droit pénal de l'ennemi cherchant continuellement à prédire l'ensemble des risques et des menaces pouvant atteindre la société. Ainsi, précise Giudicelli-Delage, « *se mettent en place des leurres de sécurité, qui ne protégeront pas la société, mais que les atteintes aux libertés individuelles, elles, sont ou seront bien réelles* »[2128].

Selon Zaffaroni, « dans un État de droit, il n'y a que des délinquants », ce qui sous-entend qu'il n'y aurait pas, au sein de cet État, d'individus dangereux en raison de ce qu'ils sont, ou en raison

[2124] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *Id.*, p. 107.
[2125] D. SALAS, *La volonté de punir, Id.,* p. 195-196.
[2126] O. SCHRAMECK, « Sécurité et liberté », *Id.*, p. 1095.
[2127] A. SUPIOT, *La gouvernance par les nombres, op. cit.,* p. 15.
[2128] G. GIUDICELLI-DELAGE, « Droit pénal de la dangerosité - Droit pénal de l'ennemi », *loc. cit.*, p. 78.

de leur comportement ou de leur entourage, ni d'ennemis à proprement parler[2129]. Il alerte sur le danger que courent les États de droit à vouloir admettre certaines pratiques sécuritaires, tout en affirmant que *« tous les États de droit de ce monde sont en réalité un processus de contradiction permanente entre l'État de droit et l'État de police,* […seulement celui-ci] *reste enfermé à l'intérieur de l'État de droit, encapsulé et contenu, mais avec des pulsions constantes essayant de le perforer et, si possible, de le faire éclater. Aussitôt que la capsule contenant l'État de droit s'affaiblit, l'État de police émerge avec la tendance à dériver vers un État absolu* »[2130]. De manière générale, le recours permanent et aggravé aux mesures de surveillance, de prévention, de neutralisation voire d'élimination, combiné à l'arsenal de sécurité ainsi mis en place au nom de la prévention des risques et de la protection des victimes « potentielles », mais aussi du libéralisme émergent, peuvent à long terme conduire à délégitimer l'action pénale, mais aussi l'action politique.

En tout état de cause, comme le souligne Foucault, « la liberté et la sécurité, le jeu liberté et sécurité, c'est cela qui est au cœur même de cette nouvelle raison gouvernementale » qui se met en œuvre, « liberté et sécurité, c'est cela qui va animer de l'intérieur » les problèmes de « l'économie de pouvoir propre au libéralisme »[2131], et les discours servent à légitimer n'importe quelle action ou mesure envisagée puisqu'il « *n'y a pas de pouvoir qui subsiste sans le discours qui le légitime ; ou, du moins, il s'affaiblit dans une bonne mesure* »[2132].

Foucault indique ainsi que « *le libéralisme s'engage dans un mécanisme où il aura à chaque instant à arbitrer la liberté et la sécurité des individus autour de cette notion de danger. Au fond, si d'un côté, le libéralisme c'est un art de gouverner qui manipule fondamentalement les intérêts, il ne peut pas – et c'est là le revers de la médaille –, il ne peut pas manipuler les intérêts sans être en même temps gestionnaire des dangers et des mécanismes de*

[2129] E. R. ZAFFARONI, « Dans un État de droit il n'y a que des délinquants », *loc. cit*., p. 43.

[2130] E. R. ZAFFARONI, « Dans un État de droit il n'y a que des délinquants », *Id.*, p. 56, où l'auteur précise que « *De cette façon, les États de droit de ce monde ne sont pas quelque chose de statique, un donné une fois pour toutes ; mais ce sont des processus dynamiques, dans une contradiction constante pulsionnelle avec l'État de police qu'ils enferment, contiennent et encapsulent. Le compromis ne tient pas compte de la réalité dans laquelle tout est en mouvement, aux dires du vieil Héraclite, et il se fonde sur un paradigme parménidien qui n'est pas de ce monde, parce qu'il ne peut pas comprendre le caractère impraticable de sa proposition. L'État de police n'aura jamais à se limiter à une parcelle secondaire et définie, bien qu'il le promette et le jure en prenant à témoin le plus sacré de sa conscience sacrilège et idolâtre, en exploitant la bonne foi de ceux qui proposent une solution de compromis, parce qu'une brèche emporte l'ouverture d'un espace dans la ligne de flottaison de l'État de droit qui le contient, et inexorablement il provoque son naufrage.* »

[2131] M. FOUCAULT, *Naissance de la biopolitique*, Cours au collège de France 1978-1979, Ed. Gallimard – Seuil, Coll. Hautes Études, EHESS, 2004, Leçon du 24 janvier 1979 - p. 67.

[2132] E. R. ZAFFARONI, « Dans un État de droit il n'y a que des délinquants », *Id.*, p. 57.

sécurité/liberté, du jeu sécurité/liberté qui doit assurer que les individus ou la collectivité seront le moins possible exposés au danger »[2133].

Section 2 – La mise en œuvre d'une politique criminelle liberticide

Le caractère liberticide de la politique criminelle nouvellement mise en œuvre se manifeste, particulièrement, à travers l'élaboration d'une politique de sécurité et de défense centrée sur « la connaissance », « l'anticipation » et « la prévention » (§1), aspirant à prévenir et à prédire tous les dangers pouvant atteindre la société et les institutions régaliennes, induisant conséquemment la fabrique d'un État d'exception (§2).

§1. Une politique de sécurité et de défense centrée sur « la connaissance », « l'anticipation » et la « prévention »

Une politique de sécurité et de défense renouvelée est ainsi instaurée, centrée sur les notions de connaissance, d'anticipation et de prévention et qui s'exprime par le biais d'une politique axée, d'une part, sur le numérique, la posture cyber et l'autonomie stratégique (A), et, d'autre part, sur la surveillance, le renseignement et l'accès à l'information (B).

A. Une politique axée sur le numérique, la posture cyber et l'autonomie stratégique

Prises dans le cadre de l'application du Livre blanc de 2013[2134], les lois de programmation militaire de 2013[2135] et de 2018[2136] s'inscrivent dans la continuité des objectifs poursuivis par le gouvernement « dans un monde plus instable et violent, dans un environnement stratégique multipolaire dont l'instabilité et l'imprévisibilité sont les figures dominantes »[2137], à savoir, principalement, une politique de défense maintenue, accentuée, renforcée et modernisée pour garantir, aujourd'hui et « à l'avenir », la défense et la sécurité nationale, ainsi qu'une programmation financière pour redonner aux armées les moyens et les capacités nécessaires pour remplir leurs missions, en prévoyant de nombreux nouveaux équipements et une évolution

[2133] M. FOUCAULT, *Naissance de la biopolitique*, *Id.*, Leçon du 24 janvier 1979 - p. 67.
[2134] Livre blanc sur la défense et la sécurité nationale, Avril 2013 : https://www.defense.gouv.fr/actualites/la-reforme/livre-blanc-2013
[2135] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
[2136] Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.
[2137] Revue stratégique de défense et de sécurité nationale de 2017 : https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017

modernisée du modèle d'armée. Les premières dispositions de ces lois constituent des dispositions programmatiques prises sur le fondement de l'article 34 de la Constitution[2138], modifié par la révision constitutionnelle du 23 juillet 2008, fixant les objectifs de défense et la programmation financière qui lui est associée[2139].

À la suite du Livre blanc de 2008, un défi stratégique d'adaptation et de redéfinition des priorités géostratégiques et de défense a été relevé tenant compte des évolutions qui résultent des crises manifestées, des inflexions nouvelles des politiques étrangères, ou des révolutions dans le monde (arabe ou africain), *in fine*, d'un environnement national et international en mutation et en évolution rapide marqué par un contexte géostratégique ainsi que des risques, crises et menaces en évolution progressive[2140]. Ainsi, pour faire face aux engagements opérationnels actuels ou futurs, nationaux ou internationaux, et aux menaces et risques potentiels qui pèsent sur la France, la loi de programmation de 2018 a augmenté significativement le budget de défense d'une moyenne de 23% par rapport à l'ancienne loi de 2013, prévoyant, conformément à la volonté du Président de la République de porter l'effort national de défense à 2% du produit intérieur brut (PIB), un budget total de 197,8 milliards d'euros, hors pensions, pour la mission « Défense »[2141]. L'ambition première manifestée par la nouvelle loi de programmation militaire de 2018, qui ne remet pas cependant en cause les priorités et objectifs poursuivis par la loi de 2013 mais s'inscrit plutôt dans sa continuité tout en la renforçant et en y apportant diverses modifications législatives, est celle de construire un modèle d'armée à la hauteur des enjeux stratégiques tout en maintenant un modèle complet et équilibré en mesure de renforcer des aptitudes clés, à savoir « *renseigner et commander, entrer en premier, combattre et protéger, soutenir et durer* »[2142].

Cette loi engage ainsi un profond renouveau de la défense et porte, en particulier, une double ambition : d'une part, redonner dès à présent aux armées les moyens de remplir durablement

---

[2138] Art. 34, al. 6, de la Constitution, modifié par la Loi constitutionnelle n° 2008-724 du 23 juillet 2008 de modernisation des institutions de la V^e^ République, : « *Des lois de programmations déterminent les objectifs de l'action de l'État* ».

[2139] Loi du 18 décembre 2013 relative à la programmation militaire, Chap. I^er^ : Dispositions relatives aux objectifs de la politique de défense et à la programmation financière ; Loi du 13 juillet 2018 relative à la programmation militaire, Titre I^er^ : Dispositions relatives aux objectifs de la politique de défense et à la programmation financière.

[2140] Loi du 18 décembre 2013 relative à la programmation militaire, Rapport annexé approuvé fixant les orientations relatives à la politique de défense et aux moyens qui lui sont consacrés au cours de la période 2014-2019 et précise les orientations en matière d'équipement des armées à l'horizon 2025 (Art. 2) ; Loi du 13 juillet 2018 relative à la programmation militaire, Rapport annexé approuvé fixant les objectifs de la politique de défense et la programmation financière qui lui est associée pour la période 2019-2025 ainsi que les conditions de leur contrôle et de leur évaluation par le Parlement.

[2141] Loi du 13 juillet 2018 relative à la programmation militaire, Art. 3.

[2142] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 1.2. *Une Ambition 2030 pour construire un modèle d'armée à la hauteur des enjeux stratégiques*

leurs missions, et, d'autre part, préparer la défense de la France pour demain, tout en renouvelant la stratégie de défense fixée par le Livre blanc de 2013 et la loi de programmation de 2013. Dès lors, pour faire face aux menaces et aux défis futurs et afin de répondre aux enjeux auxquels la France aura à faire face, une « indispensable capacité d'autonomie stratégique » est nécessaire et prévue, qui se décline en un socle de capacités opérationnelles fondamentales, dont la dissuasion qui « demeure la clef de voûte de la stratégie de défense », ainsi qu'en un certain nombre de priorités, notamment, « *accentuer l'effort sur le renseignement, consolider la capacité des armées à prévenir les crises internationales, renforcer la présence de la France dans les nouveaux espaces de confrontation stratégique, en particulier en matière de cyberdéfense, développer la capacité d'innovation et entretenir une ambition industrielle et technologique élevée* »[2143].

Ce qui révèle, selon le rapport annexé à la loi, le lien « affirmé », « indissociable », entre autonomie stratégique nationale et construction d'une autonomie stratégique européenne dans le contexte européen actuel de prise de conscience d'intérêts de sécurité partagés, l'autonomie stratégique désignant la « *conduite d'une opération sans avoir à demander à d'autres pays ou alliance des moyens supplémentaires en matière d'effectif, de transport, de renseignement* ... »[2144]. Pour ce faire, un effort de renouvellement de l'approche des coopérations européennes, en vue de donner « un nouvel élan à des partenariats de défense équilibrés, contribuant à la maîtrise des capacités nécessaires », est primordial, favorisant par là même la consolidation et le développement « *d'une culture stratégique commune, au sein d'une Europe de la défense plus forte* », et, en complément, une « *stratégie proactive de développement de coopérations technologiques et industrielles à la fois bilatérales et européennes, au travers d'un degré de dépendance mutuelle consentie adaptée aux technologies concernées* » est également essentielle pour aboutir à l'autonomie recherchée[2145].

La nouvelle loi de programmation militaire se structure alors autour de quatre axes prioritaires : le placement de la loi « à hauteur d'homme » en améliorant les conditions d'exercice du métier d'arme et les équipements ainsi que celui du « quotidien du soldat », notamment les conditions de vie et de travail du personnel militaire comme civil et de leurs familles, mais aussi en augmentant de manière dynamique les effectifs pour répondre aux besoins numériques et

[2143] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 1.2.3. *Un lien affirmé entre autonomie stratégique nationale et construction d'une autonomie stratégique européenne*
[2144] Ministère des armées, « La Loi de programmation militaire de A à Z », du 08/02/2018 : https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/le-lexique/la-loi-de-programmation-militaire-de-a-a-z#S
[2145] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 1.2.3. *Id.*

technologiques nouveaux et prioritaires ; le renouvellement des capacités opérationnelles des armées à travers deux actions « complémentaires l'une de l'autre », à savoir « réduire les impasses capacitaires » consenties par la précédente loi de programmation, qui avait toutefois déjà permis un renforcement des capacités opérationnelles notamment en matière de cyberdéfense et de cybersécurité, ainsi que moderniser les équipements des armées « de manière accélérée » ; le maintien et le rééquilibrage des cinq fonctions stratégiques « dissuasion, connaissance et anticipation, prévention, protection, intervention » qui couvrent la mise en œuvre de la stratégie de défense et de sécurité, en renforçant particulièrement les capacités de « connaissance et d'anticipation » et de « prévention », permettant alors davantage de souplesse et d'agilité pour agir « en amont comme en aval des crises », notamment dans les nouveaux espaces numérique et exoatmosphérique, tout en assurant la « complémentarité entre autonomie stratégique nationale et européenne » et en favorisant la « consolidation d'une défense en Europe, au travers d'une stratégie proactive et pragmatique de coopération avec nos partenaires européens » ; et, enfin, l'innovation des armées et du ministère, « au moyen d'équipements tirant pleinement avantage de la révolution numérique ou des technologies de rupture[2146], désormais plus fréquemment issues des développements du secteur civil, dans des temps de plus en plus courts », permettant aux armées de disposer « des équipements adaptés aux menaces futures » tout en étant « au cœur de la transformation d'un ministère plus performant »[2147]. Les deux derniers axes permettent dès lors de « préparer l'avenir » et de faire face « à l'évolution du contexte géostratégique et des risques et menaces potentiels »[2148].

Dans le but de poursuivre ces axes principaux ainsi déterminés, de nombreuses dispositions sont prévues, en complément de celles de l'ancienne loi de programmation de 2013 ou encore de celles de la loi de 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme[2149], afin d'assurer cette nouvelle politique de défense et de sécurité principalement axée sur la modernisation et la numérisation des techniques, services et infrastructures ; les bâtiments et équipements technologiques permettant d'adopter une « posture cyber permanente ».

Afin de répondre à ces exigences comme à l'accroissement des besoins, il est prévu, *inter alia*, une modernisation des « processus et des outils » du maintien en condition opérationnelle (MCO), « en particulier dans le domaine de la gouvernance », et le « renouvellement des systèmes d'informations techniques et logistiques », ainsi que la « rationalisation de la chaîne

[2146] *Cf.* p. 402 et 415.
[2147] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 1.2.5. *Une Ambition déclinée en axes prioritaires dans la loi de programmation militaire 2019-2025*
[2148] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 1.2.5. *Id.*
[2149] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

d'approvisionnement (*supply chain*) »[2150]. En outre, le MCO « *s'appuiera également sur une industrie tant étatique que privée où les nouvelles technologies (numérisation, robotisation, impression 3D, Big Data, fusion de données, développement de la maintenance prédictive) occuperont une place croissante* », sans compter que l'effort de régénération des matériels terrestres « *nécessite également qu'une part de la charge soit prise en compte par l'industrie privée comme cela a déjà été initié pour plusieurs parcs* »[2151].

Le renforcement de la « sécurité-protection » du Ministère des Armées et de sa « résilience face à des attaques de toute nature » est aussi un « enjeu majeur » de la nouvelle loi de programmation dans un contexte « où nos forces font face à des menaces à l'extérieur de nos frontières, sur notre propre territoire, mais également dans le monde numérique »[2152]. Pour ce faire, les systèmes intégrés de protection seront « optimisés et déployés » pour durcir la sécurité des sites, et les « opérations d'armement d'ores et déjà lancées » pour la protection et la lutte contre les drones malveillants seront poursuivies[2153]. Il est, par ailleurs, prévu d'attirer et de fidéliser les compétences, y compris par la simplification du recrutement de contractuels et personnels civils, en vue de préserver, en particulier, les compétences « émergentes (cybernétique, automates, intelligence artificielle ...) à haute valeur ajoutée pour les forces armées »[2154]. De même, en ce qui concerne les personnels civils, désormais la transition professionnelle « se développera, au cours de la programmation militaire, dans le sens d'un développement d'une relation plus directe entre les candidats et les employeurs potentiels, par voie numérique », et seront également mis en place « un parcours d'accès à la création ou la reprise d'entreprise et un réseau d'ambassadeurs », propres à favoriser « des contacts privilégiés avec les recruteurs, les entreprises et les administrations »[2155].
En outre, 3000 effectifs supplémentaires sont prévus pour répondre aux besoins prioritaires des armées, et seront ainsi affectés « *de manière ciblée pour consolider les domaines prioritaires, en matière de renseignement (1 500 sur 2019-25), de cyberdéfense et d'action dans l'espace*

[2150] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.1.2. *Garantir un niveau de disponibilité des matériels des armées et d'activité opérationnelle compatible avec la préparation et la réalisation des missions*
[2151] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.1.2. *Id.*
[2152] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.1.3. *Sécurité-Protection et résilience*
[2153] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.1.3. *Id.*
[2154] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.3.2. *Attirer et fidéliser les compétences*
[2155] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.3.3. *Faciliter la manœuvre RH pour maintenir une armée jeune, de haute technicité et d'une structure conforme au modèle d'armée complet et équilibré*

numérique (1 500 sur 2019-25, notamment afin de porter à 4 000 le nombre de « combattants cyber ») »[2156]. Pour renforcer le lien entre « soldat, armées et Nation », il est prévu, entre autres, de s'appuyer sur la Réserve en mettant en œuvre la « numérisation de l'information, du recrutement et de la gestion des activités des réservistes » et en développant des « partenariats avec les employeurs des réservistes, publics ou privés »[2157], mais aussi d' « affermir le lien » entre la jeunesse et les armées, « enjeu essentiel de la cohésion sociale », qui contribue « à forger chez les jeunes une conscience citoyenne dont se nourrit l'esprit de défense » et qui nécessite de porter une « attention particulière à la numérisation des supports » et d'assurer un contenu pédagogique qui « comportera les informations utiles sur les enjeux de sécurité nationale et la pertinence de l'outil de défense »[2158].

Par ailleurs, dans le cadre du renouvellement des capacités opérationnelles, il est notamment envisagé de « moderniser » les principaux programmes conventionnels pour faire face « à l'évolution des menaces », exigeant l'intégration « *des technologies innovantes adaptées »* et, *« en particulier, l'autonomisation des systèmes* [qui] *constitue un axe important de modernisation et d'innovation des capacités* »[2159]. À cet égard, il s'agit de mettre en œuvre des « concepts entièrement nouveaux » fondés sur la collaboration entre « des plateformes et des systèmes de drones », tels que « les programmes de drones aériens (comme le drone MALE européen[2160] ou le système de drones aéromaritimes embarqués SDAM[2161]), le système de

---

[2156] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.3.4. *6 000 effectifs supplémentaires pour répondre aux besoins prioritaires des armées, dont 3 000 dès 2019-2023*

[2157] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.4.1. *S'appuyer sur la Réserve*

[2158] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.4.2. *Affermir le lien entre la jeunesse et les armées*

[2159] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1. *Moderniser les principaux programmes conventionnels*

[2160] Institut de recherche stratégique de l'école militaire (IRSEM), « Un espace européen des drones », Note de recherche n° 52, rédigée par C. Lavallée et O. Zubeldia, du 7 mars 2018 : « *Le MALE est un système aérien inhabité de moyenne altitude et longue endurance dédié aux missions de renseignement, de surveillance, de ciblage et de reconnaissance* » ; « *Depuis le début des années 2000, les États membres, les institutions et agences de l'Union européenne (UE) ont multiplié les tentatives pour dynamiser la coopération dans le secteur des drones. D'abord, dans le secteur militaire avec le développement d'un drone de Moyenne Altitude Longue Endurance (MALE) européen, et plus récemment dans le secteur civil en vue de mettre en place un cadre politique européen. Un nouvel élan de coopération émerge à l'échelle européenne. D'une part, il s'agit de renforcer la Base industrielle et technologique de défense européenne (BITDE) avec le développement, voire la mutualisation, des capacités militaires. De l'autre, il est animé par la volonté d'encadrer légalement l'utilisation croissante et la multiplication des applications des drones civils* » :
https://www.defense.gouv.fr/content/.../NR_IRSEM_n52_2018.pdf

[2161] Système de Drone Aérien pour la Marine ; Naval Group, « Le futur système de drone aérien », publié le 1er mars 2019 *: « Destinés aux frégates de premier rang et aux porte-hélicoptères amphibie de type Mistral (PHA), ces UAS [Unmanned Aerial System] pourront transporter 100 kg de charge utile (radar de surveillance maritime, tourelles électro-optiques, ESM, AIS…) pendant 8 heures à au moins 80 nautiques du bâtiment. En synergie avec le système de combat du navire et en complément de l'hélicoptère embarqué, le drone est pour le commandant un moyen d'accès à l'espace aérien en autonomie complète et un véritable « capteur déporté »,*

guerre des mines futur (SLAMF[2162]) ou encore les robots du domaine terrestre intégrés aux systèmes d'information et de communication infovalorisés »[2163]. De plus, l'intégration des systèmes d'information et des nouvelles technologies est envisagée pour de multiples composantes, telles que la composante terrestre, navale, aérienne ou Interarmées dans laquelle, par exemple, les moyens (GRAVES[2164], SATAM[2165]) de veille des orbites basses seront modernisés en priorité et le système d'informations spatiales (SIS)[2166] sera amélioré pour assurer le domaine de la surveillance de l'espace exoatmosphérique[2167].

Un accent est mis sur le renforcement des capacités de renseignement, ainsi que sur la modernisation et le développement des systèmes d'information et de communication. En ce qui concerne le renseignement, qui constitue, selon la loi de programmation de 2013, « l'une des priorités majeures du Livre blanc de 2013 », et dont, plus précisément, « le développement des capacités de recueil, de traitement et de diffusion du renseignement sera prioritaire sur toute la durée de la planification d'ici à 2025-2030 »[2168], voit l'ensemble de ces capacités renforcées

[permettant d'] augmenter la perception et le traitement des menaces. » : https://www.naval-group.com/fr/episode/le-futur-systeme-de-drone-aerien/

[2162] Système de Lutte Anti-mines Marines Futur « *Ce nouveau système permettra aux marins d'opérer à distance de la zone de danger. Le programme comprend d'une part des systèmes de drones constitués de drones navals de surface et de drones sous-marins. Il comprend par ailleurs [...] le renouvellement du système d'exploitation des données de guerre des mines.* », Direction générale de l'armement, Ministère des armées, publié le 24/03/2016 : https://www.defense.gouv.fr/dga/equipement/naval/le-systeme-de-lutte-anti-mines-marines-futur-slamf

[2163] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1. *Id.*

[2164] Ministère des armées, « La Division Surveillance de l'Espace du Commandement de la Défense Aérienne et des Opérations Aériennes », du 20/03/2012 : « *Surveillance des orbites basses : le principal outil national d'appréciation autonome de la situation spatiale est le système de veille GRAVES (Grand Réseau Adapté à la VEille Spatiale) qui permet la surveillance de la quasi-totalité des satellites d'observation et d'écoute* », https://www.defense.gouv.fr/portail/dossiers/l-espace-au-profit-des-operations-militaires/fiches-techniques/dse-cdaoa ; Communiqué de Presse, « GRAVES : vers une surveillance spatiale française plus performante », Onera et Degreane Horizon, du 12 décembre 2016 : « *Le système GRAVES (Grand Réseau Adapté à la VEille Spatiale) est un système de surveillance de l'espace dont la mission principale est le renseignement militaire via l'élaboration de la situation spatiale. C'est le seul système européen capable d'assurer de façon autonome la détection et le catalogage des objets spatiaux en orbite basse. Les données générées permettent de connaître à tout instant la position de l'ensemble des satellites suivis. Demain, certaines performances seront accrues grâce notamment à des interventions au niveau des antennes de réception et du traitement du signal, supportées par un nouveau calculateur.* » : https://www.onera.fr/sites/default/files/communiques/pdf/2017-06/20161212-CP-Graves-ONERA.pdf

[2165] Ministère des armées, « La Division Surveillance de l'Espace du Commandement de la Défense Aérienne et des Opérations Aériennes », *Id.*, « *Orbitographie de précision : les radars SATAM, complémentaires au système de veille, servent à trajectographier précisément certains objets d'intérêt* ».

[2166] Dit aussi « *SIRS : Systèmes d'Information à Référence Spatiale qui accompagne les acteurs internationaux et locaux dans la gestion des territoires* », Groupe CLS, « SIRS - Des données d'observation pour une meilleure gestion des territoires » : https://www.sirs-fr.com/sirs/fr/

[2167] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.7. *Composante Interarmées*

[2168] Loi du 18 décembre 2013 relative à la programmation militaire - Rapport annexé, § 1.3.3. *Les cinq fonctions stratégiques, les contrats opérationnels et les capacités militaires associées*

« dans tous les segments » avec la nouvelle loi de 2018[2169]. Dès lors, le segment spatial sera renouvelé avec la livraison « des 2 derniers satellites du système d'observation spatial MUSIS[2170], qui permet l'acquisition d'image à très haute résolution », et le système spatial CERES[2171], « qui permettra de disposer d'une cartographie exhaustive des activités électromagnétiques global », sera également mis en service ; les systèmes aéroportés de « drones aériens » poursuivront « leur montée en puissance » : en ce sens, des « systèmes de drone tactique (SDT)[2172] PATROLLER[2173] » seront livrés, des « drones tactiques légers, avec capacité de renseignement multi-capteurs et une option d'armement », seront acquis en 2019 et

[2169] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.4. *Capacités dédiées au renseignement*

[2170] Direction générale de l'armement, « Le programme Musis », Ministère de l'armée, du 24/03/2016 : « *Dans une logique européenne, et afin de remplacer les systèmes existants (systèmes optiques français Hélios et Pléiades, systèmes radar allemand et italien SAR-Lupe et Cosmo-SkyMed), l'Allemagne, la Belgique, l'Espagne, l'Italie, la Grèce et la France ont recherché au travers de l'initiative MUltinational Space-based Imaging System (Musis), à se doter de moyens d'observation spatiale. Cette initiative inclut une composante spatiale optique (CSO) (sous leadership français), deux composantes radar (respectivement italienne et allemande) et une composante optique champ large. Ces moyens permettront de disposer des capacités de suivi de situation et de veille stratégique, d'une aide à la prévention et à l'anticipation des crises ainsi qu'à la planification et à la conduite des opérations.* » : https://www.defense.gouv.fr/dga/equipement/information-communication-espace/musis

[2171] Direction générale de l'armement, « Le programme CERES (capacité de renseignement électromagnétique spatiale) », Ministère de l'armée, du 24/03/2016 : « *Le programme CERES (capacité de renseignement électromagnétique spatiale) vient compléter les moyens nationaux terrestres, maritimes et aéroportés de recherche et d'interception des émissions électromagnétiques. Il comprend des fonctions d'interception, de caractérisation et de localisation des signaux électromagnétiques par des moyens satellitaires, leur programmation ainsi que les moyens sols de contrôle des satellites. Le système CERES est basé sur une constellation de 3 satellites. Il permettra de recueillir régulièrement sur l'ensemble du globe les informations permettant de cartographier et d'analyser le fonctionnement des émetteurs électromagnétiques dans les bandes de fréquences d'intérêt radar et télécommunication. Le système CERES comprend également un segment sol utilisateur et un segment sol de contrôle.* » : https://www.defense.gouv.fr/dga/equipement/information-communication-espace/le-programme-ceres-capacite-de-renseignement-electromagnetique-spatiale

[2172] Direction générale de l'armement, « Le système de drone tactique (SDT) », Ministère de l'armée, du 24/03/2016 : « *Le programme SDT vise à acquérir une capacité pérenne de drones tactiques pour l'armée de terre, en remplacement du système intérimaire actuel SDTI (« Sperwer » de SAGEM). Le SDT devra, par rapport au SDTI, offrir des performances accrues (endurance, qualité des images produites) et permettre une approche multi-capteurs permettant d'orienter efficacement les recherches. Le SDT aura donc une capacité d'emport simultané de deux charges utiles (optique/Infra-rouge et radar dans un premier temps, une charge de guerre électronique/communications pouvant dans un second temps se substituer au radar).* » : https://www.defense.gouv.fr/english/dga/equipement/missiles-et-drones/le-systeme-de-drone-tactique-sdt

[2173] Avis n° 110 (2017-2018) de C. PERRIN et H. CONWAY-MOURET, fait au nom de la Commission des affaires étrangères, de la défense et des forces armées sur le projet de loi de finances pour 2018, t. VIII - Défense : Équipement des forces, déposé le 23 novembre 2017, Sénat : « *La LPM 2014-2019, au titre de l'étape 1 du programme, prévoit la livraison de deux systèmes opérationnels et d'un système d'entraînement, pour un total de 14 vecteurs aériens. La réalisation de cette étape a été lancée en février 2016, le drone « Patroller » de Sagem ayant été choisi, par préférence au drone « Watchkeeper » de Thalès, dans le cadre de la compétition sans publicité que la DGA avait ouverte en 2014. Un des points forts du Patroller tient à sa boule optronique, offrant des performances remarquables pour l'identification d'objectifs.* ». Par ailleurs, *« la décision annoncée par la ministre des armées, en septembre dernier, de procéder à l'armement des drones* », est saluée, la ministre ayant depuis lors précisé qu'en la matière, « *même si aujourd'hui notre priorité reste le [drone MALE] Reaper, nous avons également l'intention d'armer les drones [tactiques] Patroller* » : https://www.senat.fr/rap/a17-110-8/a17-110-813.html et https://www.senat.fr/rap/a17-110-8/a17-110-81.pdf

un « deuxième avion léger de surveillance et de reconnaissance (ALSR)[2174] » sera livré[2175] ; un drone étant défini, dans le cadre de cette loi, comme un « *engin mobile terrestre, aérien ou naval, sans équipage embarqué, programmé ou télécommandé, et qui peut être réutilisé. Les drones militaires sont équipés de systèmes d'armes ou de collecte d'informations* »[2176].

En outre, les moyens de renseignement électromagnétique, « indispensables à la connaissance des intentions de l'adversaire », seront modernisés, « notamment avec la livraison de la capacité universelle de guerre électronique (CUGE)[2177], permettant de disposer d'une capacité spécialisée de recueil de renseignement aéroportée renforcée, avec la modernisation de nos moyens de renseignement stratégique fixes ainsi que la commande d'un bâtiment léger de surveillance et de recueil de renseignement (BLSR) » ; et ces moyens seront, d'autre part, également modernisés à travers le programme « ROEM tactique » visant à renforcer les capacités de renseignement de contact des unités aéroterrestres déployées »[2178]. Selon le rapport annexé à la loi de 2018, « *l'adaptation de nos capacités d'exploitation pour faire face à l'afflux de données se concrétisera par la mise en service du système d'information SORIA[2179] et la*

[2174] Ministère des armées – Actualités « La DGA commande des avions légers de surveillance et de reconnaissance (ALSR) » du 24/06/2016 : « *Mercredi 22 juin 2016, la direction générale de l'armement (DGA) a confié aux sociétés Sabena Technics et Thalès la réalisation des avions légers de surveillance et de reconnaissance (ALSR). La commande prévoit la livraison de deux systèmes opérationnels. Chacun se compose d'un vecteur aérien, lui-même composé de différentes charges utiles permettant de recueillir du renseignement d'origine électromagnétique et d'origine image, et de stations sol, pour la préparation des missions et le recueil des informations. L'acquisition de ce type d'aéronefs par l'armée de l'air, au profit du renseignement militaire français, a pour but d'apporter une capacité complémentaire de celle des drones MALE (moyenne altitude longue endurance) Harfang et Reaper, déjà mis en oeuvre par les aviateurs*. » : https://www.defense.gouv.fr/espanol/actualites/communaute-defense/la-dga-commande-des-avions-legers-de-surveillance-et-de-reconnaissance-alsr

[2175] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.4. *Id.*

[2176] Ministère des armées, « La Loi de programmation militaire de A à Z » : https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/le-lexique/la-loi-de-programmation-militaire-de-a-a-z#S

[2177] Ministère des armées – Actualité « Communiqué de Florence Parly, ministre des Armées : Capacité universelle de guerre électronique – CUGE, Lancement d'un nouveau programme d'avions de renseignement », du 28/02/2018 : « *Ce nouveau programme sera doté d'un capteur inédit pour les Armées françaises, permettant simultanément les interceptions des émissions radio et radar. Résultat de près de 10 années d'études sur des technologies de pointe, ce nouveau capteur développé par Thales sera intégré sur un avion Falcon construit par Dassault Aviation* ». Ces *« avions de renseignement stratégique CUGE [...] viendront renforcer les capacités du renseignement d'origine électromagnétique et contribueront à l'effort particulier sur la fonction « connaissance et anticipation »* » : https://www.defense.gouv.fr/actualites/economie-et-technologie/cp-florence-parly_lancement-d-un-nouveau-programme-d-avions-de-renseignement_cuge

[2178] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.4. *Id.*

[2179] Rapport n° 476 (2017-2018) de C. CAMBON, fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, Sénat, déposé le 16 mai 2018 : « *Un effort crucial sera engagé pour mettre en œuvre, en utilisant les « technologies des données massives » et de l'intelligence artificielle, des processus plus performants de traitements et d'analyse. Pour faire face à l'afflux des données issues des différents capteurs, mais aussi pour assurer la sécurité de ces flux, la modernisation des systèmes d'information de la fonction interarmées du renseignement est nécessaire. La mise en service d'un* ***système optimisé du renseignement interarmées*** *(SORIA) est prévue d'ici à 2025. Elle s'inscrit dans les efforts de convergence et de rationalisation des* ***systèmes d'informations opérationnels et de communication*** *(SIOC) des armées qui seront poursuivis avec*

modernisation progressive du système d'information de la fonction interarmées du renseignement »[2180].

Quant aux Systèmes d'Information et de Communication (SIC), définit par le Ministère des Armées comme un « *système intégré d'appui au commandement destiné à fournir dans les délais requis aux autorités et à leur état-major les données nécessaires à la planification, à la conduite et au contrôle de leurs activités,* [et intégrant] *le personnel, les équipements, l'organisation, les procédures, les liaisons et les éléments de doctrine* »[2181], ils seront modernisés « avec la mise en service de DESCARTES (réseau à base de fibres optiques permettant de relier tous les sites fixes en métropole et outre-mer du Ministère des Armées) et de SYRACUSE IV (système de télécommunication composé de 2 satellites militaires et des stations-sol permettant d'assurer les communications sur le champ de bataille et avec la métropole) »[2182]. Le programme « Successeur MELCHIOR » envisagé apportera, en plus, « une amélioration importante des débits et de la robustesse des transmissions numériques à très grande distance par liaison radio haute fréquence » et la connectivité sera renforcée par la « livraison de nombreux équipements de radio numérique CONTACT (8 400 nouveaux postes) »[2183].

De même, les « équipements de navigation par satellite des armées (OMEGA) » seront modernisés, et une « capacité autonome de géolocalisation, capable d'utiliser les signaux GPS et Galileo et résistant aux interférences comme au brouillage », sera également développée[2184].

Enfin, « les efforts de convergence et de rationalisation des Systèmes d'Information Opérationnels et de Communication (SIOC) des armées seront poursuivis avec la mise en service opérationnel progressive du Système d'Information des Armées (SIA), du niveau opératif au niveau tactique haut, interopérables avec nos principaux alliés et en national »[2185] ; ainsi, le SIA « *évoluera pour prendre en compte les potentialités offertes par l'intelligence artificielle et le Big Data afin de garantir la fluidité des échanges et de permettre de conserver la maîtrise de la supériorité informationnelle dans un contexte d'accroissement des risques*

---

la mise en service opérationnel progressive du système d'information des armées (SIA). Cet enjeu a été perçu par la DGA qui travaille notamment à la conception d'un programme ARTEMIS - pour ***Architecture de Traitement et d'Exploitation Massive de l'Information Multi-source*** *- qui devrait constituer un outil particulièrement précieux pour la conduite de la fonction « connaissance et anticipation ».* » : http://www.senat.fr/rap/l17-476/l17-4767.html#fn30 et http://www.senat.fr/rap/l17-476/l17-4761.pdf

[2180] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.4. *Id.*

[2181] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*

[2182] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.5. *Systèmes d'Information et de Communication*

[2183] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.5. *Id.*

[2184] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.5. *Ibid.*

[2185] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.5. *Ibid.*

cyber et des volumes de données à traiter », sans oublier que, dans le domaine de la connaissance du milieu géophysique, le « système d'information GEODE 4D » est attendu pour mettre à disposition des armées des données géographiques à haute valeur ajoutée[2186].

Le cyberespace, qualifié par le rapport annexé à la loi de 2018 de « nouveaux espaces stratégiques communs ou partagés », fait l'objet d'une attention particulière compte tenu de l'enjeu de rivalité et de lutte[2187] qu'il représente entre grands États et dont « l'intensité croît alors que les règles communes qui les gouvernent sont insuffisantes », nécessitant donc de « consolider l'autonomie stratégique de la France, en s'appuyant sur des capacités spécifiques ou modernisées, qu'elles relèvent du domaine de la cyberdéfense ou du spatial »[2188], et ce par le biais, entre autres, d'une « structuration volontariste de l'action du ministère dans l'espace numérique »[2189], ou encore d'une « meilleure prise en compte de l'espace exoatmosphérique »[2190]. En effet, « *le développement du cyberespace à l'échelle planétaire, la rapidité d'accroissement de la dépendance au numérique de nos moyens militaires ainsi que l'extension des risques d'attaque sur nos systèmes électroniques, nécessitent le développement de capacités de cyberdéfense dans toutes leurs dimensions* »[2191].

À ce titre, la loi « renforce les capacités des armées en matière de prévention, de détection et d'attribution des cyberattaques », celles-ci représentant un « *ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité [...]* »[2192], et les dote de « moyens de réaction rapides, efficaces et coordonnés » afin de garantir « une protection et une défense des systèmes et réseaux, cohérente dans tous les secteurs (cyberprotection, lutte informatique défensive[2193], influence numérique, lutte informatique offensive[2194] et moyens de commandement et d'entraînement) », tout en établissant une « posture permanente cyber

---

[2186] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.2.1.5. *Ibidem.*
[2187] *Cf.* p. 319 et s., 400 et s.
[2188] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3. *Agir dans les nouveaux espaces de confrontation stratégique*
[2189] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.1. *Une structuration volontariste de l'action du ministère dans l'espace numérique*
[2190] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.2. *Une meilleure prise en compte de l'espace exoatmosphérique*
[2191] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.1. *Id.*
[2192] Ministère des armées, « La loi de programmation militaire de A à Z », *Id.,* « *[...]. Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée.* »
[2193] Ministère des armées, « La loi de programmation militaire de A à Z », *Id.,* « *Lutte informatique défensive : ensemble coordonné d'actions menées par un État, qui consiste à détecter, à analyser et à prévenir des cyberattaques, et à y réagir le cas échéant* »
[2194] Ministère des armées, « La loi de programmation militaire de A à Z », *Ibid.,* « *Lutte informatique offensive : ensemble coordonné d'actions menées dans le cyberespace par un État contre des systèmes d'information ou de données pour les perturber, les modifier, les dégrader ou les détruire.* »

(PPC) » pour garantir la surveillance des réseaux ainsi que le caractère opérationnel des capacités actives ou passives de lutte informatique défensive, eu égard à « la numérisation croissante de nos adversaires »[2195].

En outre, le libre accès et l'utilisation de l'espace exoatmosphérique, « conditions de l'autonomie stratégique dans la mesure où les satellites fournissent des services essentiels, dont les communications, la navigation, la surveillance et l'écoute spatiales », représentent « un intérêt stratégique de premier ordre » compte tenu du fait que « l'accès à l'espace, milieu en forte mutation et peu régulé, tend à se banaliser, de même que l'usage de services spatiaux »[2196]. Face à « *l'accroissement des risques et menaces, la capacité à détecter et attribuer un éventuel acte suspect, inamical ou agressif dans l'espace constitue donc une condition essentielle de notre protection* », nécessitant alors la consolidation des « capacités nationales de surveillance de l'espace exoatmosphérique (*Space Surveillance and Tracking, SST*) et de connaissance de la situation spatiale (*Space Situational Awareness, SSA*) », ainsi que la recherche systématique des « opportunités de développement de coopérations plus étroites avec des partenaires stratégiques clés »[2197]. De même, en vue d'atténuer les risques associés à la dépendance à l'espace exoatmosphérique, une attention particulière est portée, « notamment dans le cadre de la coopération européenne, à l'émergence de technologies de rupture comme les « pseudo-satellites de haute altitude » »[2198].

L'innovation numérique représente, par ailleurs, « un levier majeur » de la nouvelle loi de programmation militaire exigeant qu'un effort « accru » soit réalisé en matière d'équipements « pour les études, la préparation des programmes structurants pour l'avenir et le maintien de l'excellence de notre base industrielle et technologique de défense (BITD[2199]) »[2200]. En effet, « *la capacité à intégrer rapidement l'innovation et à tirer parti de la révolution numérique constitue un axe prioritaire* » de la loi[2201].

À cet égard, « une partie des efforts consentis dans le domaine des systèmes d'information et de la cyberdéfense » est consacrée à repenser l'organisation des infrastructures et systèmes d'information et de communication, à sécuriser les réseaux et à développer les moyens de lutte

---

[2195] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.1. *Id.*
[2196] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.2. *Id.*
[2197] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.2. *Ibid.*
[2198] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.2. *Ibid.*
[2199] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.* : « *BITD : Acronyme pour « base industrielle et technologique de défense ». Ce terme désigne l'ensemble des industries nationales d'un pays prenant part aux activités de défense*. »
[2200] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4. *Innover et se transformer pour répondre aux défis futurs*
[2201] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4., *Id.*

informatique[2202], celle-ci désignant l'« *ensemble des actions de protection, de surveillance, de réaction rapide et d'action offensive menées dans le cyberespace, par tous les moyens disponibles, et portant sur les systèmes civils ou militaires utilisant l'informatique, d'une part, les logiciels, les données ou les matériels d'autre part* »[2203]. De plus, compte tenu des « enjeux opérationnels et financiers majeurs et des importantes mutations en cours sur le plan industriel et technologique », une « réforme en profondeur de la gestion des programmes d'équipement » sera mise en œuvre afin de « mieux incorporer l'innovation issue de l'industrie et du secteur civil et de tirer parti de l'ensemble des opportunités offertes par la révolution numérique », entre autres ; réforme qui concernera « tous les stades du cycle de vie des équipements et impliquera l'ensemble des acteurs concernés (armées, DGA, industrie) », et qui portera, en particulier, sur les champs fonctionnels suivants: « la gouvernance et l'organisation, les méthodes, les normes, les processus qualité et les outils techniques mis en œuvre, les relations entre l'État et l'industrie, les financements et le partage des risques »[2204].

Pour ce faire, « trois leviers clé de performance seront utilisés : *i)* le travail collaboratif et le décloisonnement des acteurs (équipes et plateau projet) à tous les stades, *ii)* l'utilisation des outils numériques et notamment l'ingénierie systèmes, la simulation, le Big data, l'intelligence artificielle, *iii)* le renforcement des compétences » ; sans oublier que cette réforme des processus de conduite des projets, qui sera appliquée « pour les programmes nouveaux lancés et, à chaque fois que possible, sur des programmes d'ores et déjà engagés », « tirera partie des meilleures pratiques appliquées dans le domaine civil et chez nos partenaires internationaux »[2205].

In fine, aux termes du rapport annexé à la loi de programmation en question, « *au-delà de l'adoption de nouvelles technologies, la transformation numérique est une démarche volontaire visant à s'approprier au plus vite et dans les meilleures conditions les technologies émergentes […]. Il s'agit de transformer les organisations et les domaines d'emploi, en exploitant en particulier la donnée numérique* »[2206].

[2202] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.4. *Innovation et numérisation au cœur de la transformation du ministère*
[2203] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*, « Lutte informatique »
[2204] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.4., *Id.*
[2205] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.4., *Ibid.*
[2206] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.4., *Ibidem.*

B. Une politique axée sur la surveillance, le renseignement et l'accès à l'information

À la lumière des évènements ayant eu lieu depuis l'adoption de la stratégie de défense et de sécurité nationale par le Livre blanc de 2013, il est apparu nécessaire au gouvernement de « *consolider les cinq fonctions stratégiques qui sont interdépendantes et dont l'équilibre garantit la cohérence et la crédibilité du modèle d'armée complet qui structure la Défense française et préserve l'autonomie stratégique de notre pays* », ce qui requiert alors « *un rééquilibrage visant à porter l'effort sur la fonction « connaissance et anticipation » et à rendre à la fonction « prévention » toute son importance, dans une logique d'approche globale et de coopération accrue avec nos partenaires et alliés dans la gestion et la prévention des crises* », tout en notant que ce « *rééquilibrage ne remet pas en cause la distinction entre les fonctions qui sont préservées* »[2207].

La fonction « connaissance et anticipation », définie comme étant une « *fonction stratégique couvrant cinq domaines : renseignement ; connaissance des zones d'opérations potentielles ; action diplomatique ; analyse prospective ; maîtrise de l'information* »[2208], met à disposition des « autorités politiques et militaires » les capacités d'appréciation autonome de situation, tout en permettant de conserver la « supériorité informationnelle » dans les opérations[2209]. Le renseignement, « *source de cette supériorité informationnelle* », repose sur un socle de capacités nationales, humaines et techniques, mais aussi sur « tous les dispositifs qui contribuent à enrichir la connaissance de l'environnement stratégique »[2210]. Cette fonction est également, selon le rapport annexé à la loi, soutenue et complétée par l'apport de partenaires, « en particulier de l'Alliance atlantique », mais « sans remettre en cause l'autonomie de la France »[2211].

Priorité de la stratégie de défense, la fonction « connaissance et anticipation » nécessite alors un effort accru en matière d'équipements dans le domaine du renseignement, « avec notamment l'acquisition de deux avions légers de surveillance et de reconnaissance, de trois avions de reconnaissance stratégique (CUGE) et la commande d'un bâtiment léger de surveillance et de reconnaissance, ainsi que la mise en service des systèmes spatiaux CERES (Capacité d'Écoute et de Renseignement Électromagnétique Spatiale) et MUSIS (*Multinational Space-based*

[2207] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1. *Une consolidation des cinq fonctions stratégiques*
[2208] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*
[2209] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1. *La connaissance et l'anticipation*
[2210] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1., *Id.*
[2211] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1., *Id.*

Imaging System for Surveillance, Reconnaissance and Observation) »[2212]. Dans ce cadre, les effectifs supplémentaires sont « principalement consacrés au renforcement des capacités humaines et techniques de traitement des données collectées » afin de « mieux anticiper les évolutions liées à la nouvelle donne stratégique », et le recours à l'intelligence artificielle « vise à améliorer la sécurisation, le traitement et l'exploitation des flux d'informations en croissance exponentielle », puisque, « *essentielle dans le traitement de données de masse, l'intelligence artificielle complète le travail humain effectué pour recueillir et traiter le renseignement. Dans un univers industriel dominé par des entreprises étrangères et caractérisé par des innovations technologiques rapides, le développement de ces technologies s'avère ainsi un enjeu majeur de souveraineté* »[2213].

Un effort doit ainsi être entrepris pour organiser une « posture permanente « renseignement stratégique », fédérant les moyens de collecte (satellites, moyens fixes et déployables, renseignement humain, cyber ...) et d'analyse du ministère (animation, exploitation et diffusion du renseignement) » compte tenu du fait que, « *dans le domaine du cyberespace et des moyens techniques associés, les activités du renseignement sont développées afin de consolider nos capacités de recherche dans la profondeur de l'espace numérique et d'être en mesure d'y rechercher le renseignement utile. Il s'agit également d'être en mesure d'attribuer, avec une certitude suffisante, les éventuelles attaques, d'évaluer les capacités offensives des adversaires potentiels et, si nécessaire, d'y réagir* »[2214]. En même temps, les services de renseignement poursuivront leur transformation afin de conforter leur « résilience »[2215] et continuer « l'adaptation et la modernisation de leur capacités de recueil et d'analyse, conformément au plan national d'orientation du renseignement[2216] (PNOR) », et, d'autre part, la « mutualisation »

[2212] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1., *Ibid.*
[2213] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1., *Ibid.*
[2214] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1., *Ibidem.*
[2215] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.* « *Résilience : volonté et capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeure, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile tout entière.* »
[2216] Rapport n° 424 (2017-2018 Sénat) – n° 875 (2017-2018 Assemblée Nationale) de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017, par P. Bas, déposé le 12 avril 2018, p. 21 « *Le Plan national d'orientation du renseignement - PNOR est la déclinaison annuelle de la stratégie nationale, à destination des services. Il s'agit donc d'un document à vocation opérationnelle, couvert par le secret de la défense nationale* » : http://www2.assemblee-nationale.fr/content/download/69939/714118/version/1/file/Rapport+DPR+2017_version+publique.pdf

des moyens est poursuivie dans le sens d'une « meilleure interopérabilité[2217] et d'un partage des efforts entre les services »[2218].

Quant à la prévention, elle désigne une « *fonction stratégique qui vise à éviter l'apparition, le développement ou la résurgence d'une crise par la mise en œuvre de mesures de tous ordres (diplomatique, économique, militaire, juridique, etc.). D'un point de vue militaire, elle repose sur : des services de renseignements disposant de moyens humains et techniques (interception des télécommunications et satellites d'observation) ; des dispositifs de coopération militaire pour aider les pays avec lesquels la France a des accords à se doter de moyens autonomes de résolution des conflits ; des forces prépositionnées à l'extérieur des frontières permettant d'intervenir le plus rapidement possible* »[2219].

La loi de 2018 aspire à rendre à cette fonction toute son importance dans une « logique d'approche globale pour la gestion des crises »[2220]. En effet, « *la prévention vise à agir en amont, sur leurs facteurs de déclenchement, pour en réduire les risques d'occurrence et en maîtriser les effets. Son renforcement permettrait de susciter une mobilisation accrue de nos partenaires et alliés, notamment européens, dans le cadre d'une approche préventive conjointe.* »[2221]. Pour ce faire, est confirmée la « configuration du réseau de bases opérationnelles avancées (Côte-d'Ivoire, Djibouti, Émirats arabes unis) et de pôles opérationnels de coopération (Gabon et Sénégal) » en tant que réseau de point d'appui, qui constitue un « instrument clé de la stabilisation et de l'anticipation des crises » et concourt directement à la mise en œuvre de la fonction « intervention »[2222]. À ce titre, et en vue d'améliorer « la capacité globale de prévention », la possibilité est ouverte aux États européens qui le souhaitent de stationner leurs propres unités dans ce réseau ; l'objectif étant, qu'à long terme, cette évolution accompagne le renforcement de « la sécurité du continent africain », et accroisse « la réactivité des armées ainsi que notre influence dans le monde »[2223].

D'autre part, la prévention s'appuie sur différents déploiements ou manœuvres, « ponctuels ou récurrents », dont des moyens de l'armée et des forces spéciales françaises qui contribueront à développer des coopérations régionales, à augmenter la connaissance des espaces concernés ainsi qu'à marquer la présence de la France, déploiements qui pourront concerner tous types

[2217] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.* : « *Interopérabilité : capacité de plusieurs systèmes, unités ou organismes à opérer ensemble grâce à la compatibilité de leurs organisations, doctrines, procédures, équipements et relations respectives.* »
[2218] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1., *Id.*
[2219] Ministère des armées, « La Loi de programmation militaire de A à Z », *Ibid.*
[2220] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.2. *La prévention*
[2221] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.2., *Id.*
[2222] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.2., *Ibid.*
[2223] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.2., *Ibid.*

d'unités tels que les avions de surveillance ou les systèmes de détection ; et au-delà de leur mission de protection, « les forces de souveraineté contribuent à la prévention des crises par les partenariats régionaux dans lesquels elles s'inscrivent »[2224].

Les fonctions « dissuasion », « intervention » et « protection » sont, par ailleurs, ravivées et font l'objet d'une consolidation avec la nouvelle loi de programmation. La première, qui se réfère à la dissuasion nucléaire, s'entend comme une « *dissuasion exercée pour la défense des intérêts vitaux de la France par la menace de provoquer, par l'emploi de tout ou partie de ses armes nucléaires, des dommages de toute nature, hors de proportion avec l'enjeu des intérêts mis en cause et, de ce fait, inacceptables pour tout adversaire qui voudrait leur porter atteinte. Fonction stratégique, la dissuasion nucléaire reste la garantie ultime de la sécurité et de l'indépendance de la France vis-à-vis de toute agression. […]* »[2225]. La dissuasion, qui « demeure au cœur de la protection de l'indépendance de la Nation », permet à la France de préserver ses « intérêts vitaux » contre n'importe quelle source ou forme d'agression d'origine étatique, et contribue « *de facto* à la sécurité de l'Alliance atlantique et à celle de l'Europe »[2226] ; ces intérêts vitaux désignant, pour un pays, les « *intérêts contribuant à l'intégrité du territoire national et de ses approches, au libre exercice de la souveraineté nationale et à la protection de la population* »[2227]. En ce sens, la « modernisation des deux composantes » de cette fonction, notamment océanique et aéroportée moyennant les nouvelles technologies, garantit la capacité à « répondre à l'évolution du contexte stratégique et à l'émergence de nouvelles menaces » ; cela dit, les « effets de cette modernisation se répercutent sur les autres fonctions stratégiques »[2228].

La protection désigne, pour sa part, une « *fonction stratégique visant, en permanence, à prévenir ou à réprimer l'exercice d'un chantage, de représailles ou d'agressions limitées contre le territoire ou les populations, notamment en cas de risque résultant de crises internationales dans lesquelles la France serait directement ou indirectement impliquée. Cette fonction se traduit en particulier par l'action permanente de sécurité des forces de gendarmerie (surveillance, neutralisation…), la posture permanente de sauvegarde maritime et la posture*

[2224] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.2., *Ibidem.*
[2225] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.* : « *[…]. La doctrine nucléaire reste celle du non-emploi. La capacité nucléaire française est constituée de : missiles balistiques qui équipent les sous-marins nucléaires lanceurs d'engins (SNLE) ; missiles aérodynamiques (ASMPA pour air-sol moyenne portée amélioré) pour la composante aéroportée dont font partie des avions de l'armée de l'Air et de l'aviation navale.* »
[2226] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.1. *La dissuasion*
[2227] Ministère des armées, « La Loi de programmation militaire de A à Z », *Ibid.*
[2228] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.1., *Id.*

permanente de sûreté aérienne (assistance aux aéronefs, détection et intervention…) »[2229]. Elle a donc pour objet de garantir « l'intégrité du territoire et d'assurer aux français une protection efficace contre l'ensemble des menaces, physiques comme immatérielles », impliquant dès lors une articulation autour des « postures permanentes de sûreté »[2230] tout en intégrant la « posture de protection terrestre mise en place à la suite des attentats de 2015 et 2016 »[2231]. De plus, en raison de la « réalité et de la permanence d'une menace cybernétique significative », le contrat de protection est également étendu « au domaine de la cyberdéfense, avec la création d'une posture permanente « cyber » »[2232] ; la cyberdéfense se référant à l' « *ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité. La cyberdéfense met notamment en œuvre la lutte informatique défensive et la lutte informatique offensive* »[2233].

De même, « pour répondre aux menaces croissantes dans les nouveaux espaces de compétition stratégique », il est prévu un renforcement des « capacités de détection et de réaction » dans l'espace exoatmosphérique, s'appuyant sur des moyens et des équipements, physiques ou numériques, mais aussi sur la « recherche de partenariats efficaces, notamment européens »[2234].

Il est, par ailleurs, utile de noter que selon les rapporteurs de cette loi de programmation, la vocation de celle-ci étant de répondre aux besoins des armées, elle est exclusivement concentrée sur la mission « Défense », et n'aborde pas, par conséquent, la question des « capacités du Ministère de l'Intérieur (notamment la capacité blindée de la gendarmerie nationale) qui contribuent directement à la fonction « protection » de la politique de défense et de sécurité nationale et sont indispensables à la continuité de l'action de l'État »[2235].

Quant à l'intervention, elle est définie comme une *« fonction stratégique qui vise à acheminer et déployer des capacités d'un point à un autre, hors de métropole, qui se décline en projection extérieure et projection intérieure et peut prendre la forme d'une projection de forces ou de puissance. Dans le domaine des opérations militaires, phase initiale d'une opération, au cours de laquelle une force est engagée pour résoudre en priorité les volets militaire et sécuritaire d'une crise et qui vise la défaite militaire de l'adversaire, l'arrêt des combats ou l'abaissement*

[2229] Ministère des armées, « La Loi de programmation militaire de A à Z », *Ibidem.*
[2230] Ministère des armées, « La Loi de programmation militaire de A à Z », *Ibidem* : « *Posture permanente de sûreté (PPS) : ensemble des dispositions permanentes prises pour mettre le pays, en toutes circonstances, à l'abri d'une agression, même limitée, contre son territoire et ses intérêts immédiats.* »
[2231] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.2. *La protection*
[2232] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.2., *Id.*
[2233] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*
[2234] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.2., *Id.*
[2235] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.2., *Ibid.*

du niveau de violence »[2236]. C'est donc une fonction qui vise à agir « au loin » pour défendre les intérêts de la Nation ou protéger les ressortissants français, « la défense de l'avant contribuant ainsi directement à la sécurité du territoire national » ; une fonction devant donc s'inscrire « systématiquement dans le cadre d'une approche globale »[2237]. À cet égard, il est prévu que la fonction « intervention » doit relever le « défi de stratégies hybrides et de dénis d'accès dans tous les milieux » ; la montée en « compétence technologique et opérationnelle des différentes menaces » exigeant, dès lors, que les armées « conservent un différentiel technologique suffisant et demeurent interopérables avec leurs alliés occidentaux les plus capables »[2238].

À cet effet, et compte tenu d'un « environnement opérationnel toujours plus exigeant »[2239], des « contrats opérationnels »[2240] et des « formats » particuliers sont prévus afin d'assurer des « *postures permanentes de dissuasion, de sûreté et de protection du territoire national, de renseignement stratégique, de cyberdéfense, [...] et d'opérer dans les espaces exoatmosphérique et numérique* »[2241]. Ce qui exige « un volume cumulé de forces » dont des « moyens de renseignement interarmées, de guerre électronique ou cyber », un « groupement de renseignement multi-capteurs ou un groupement de transmissions », mais aussi des systèmes de drones moyenne altitude longue endurance MALE ou des avions légers de surveillance et de reconnaissance (ALSR) ou encore une « composante « cyber » »[2242]. En outre, les capacités de commandement et de contrôle (C2) seront renforcées en vue de gagner en autonomie, et s'appuieront notamment sur le « Système d'information des armées (SIA) » qui fournira à l'ensemble des acteurs opérationnels les « outils indispensables au commandement et à la conduite des opérations, tant au niveau stratégique qu'opératif »[2243], de sorte que, en s'appuyant sur un « socle technique commun interarmées (STCIA) et des applications logicielles communes, il facilitera la numérisation de l'espace des opérations »[2244].

[2236] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*
[2237] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.3. *L'intervention*
[2238] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.3., *Id.*
[2239] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2. *Des contrats opérationnels et des formats au service de l'Ambition 2030*
[2240] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.* : « *Contrat opérationnel : contrat qui stipule ce que les armées doivent être capables de faire en permanence et de manière ponctuelle.* »
[2241] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.1. *Une Ambition déclinée en contrats opérationnels*
[2242] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.1., *Id.*
[2243] « *[...] : SIA C2 pour les fonctions métiers C2 et l'obtention des effets, SORIA (3) et SILRIA (4) pour les fonctions renseignement et logistique.* » : Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.2.1 *Les capacités de commandement et de contrôle (C2)*
[2244] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.2.1, *Id.*

Parallèlement, les forces spéciales, « issues des trois armées », voient leur rôle se renforcer « tant pour la capacité d'entrée en premier que dans le cadre de la lutte contre le terrorisme », et constituent « un outil dans la main du commandement dont la polyvalence, l'interopérabilité, la réactivité, la protection et les capacités de renseignement continueront d'être renforcées, notamment par une modernisation de leurs équipements (véhicules spécialisés, avions de renseignement, drones) »[2245]. Cet ensemble leur assurera en conséquence « *l'aptitude à répondre au spectre des missions allant de l'anticipation stratégique à la capacité de renseignement et d'action face à un dispositif ennemi moderne et complexe, en passant par la lutte dans la durée contre le terrorisme, par la prévention et le partenariat militaire opérationnel (PMO)* »[2246].

En outre, les armées doivent être en mesure d'agir « de façon autonome et durable dans les domaines du renseignement (autonomie d'appréciation), de la protection face aux menaces asymétriques, de la démonstration de puissance en appui de la volonté politique, ou encore des actions d'influence »[2247]. Ces menaces asymétriques ou conflits asymétriques désignent, aux termes du lexique de la loi de programmation, un « *type de conflit dans lequel il y a disparité totale d'ordre et de nature des buts de guerre, des moyens et des manières d'agir. Le terrorisme transnational illustre particulièrement bien l'asymétrie, dans ses modes d'action à l'encontre d'États souverains ou d'organisations internationales* »[2248]. Découlant indirectement des attentats de 2001, et plus directement encore, des attentats de 2004 à Madrid, de 2005 à Londres, de 2015 à Paris, ou encore de 2016 à Bruxelles, ces menaces ou conflits semblent jouer, « *dans un contexte international globalisé, [...] un rôle déterminant dans l'évolution de la politique européenne* »[2249] et semblent toucher, en particulier, les Nations impliquées dans l'occupation militaire du Proche et Moyen-Orient. Ces derniers représentent, dans cette perspective, les produits d'une « guerre asymétrique »[2250] qui laisse peu de choix à ceux qui pensent combattre ces « attentats » en vue d'aboutir à une démocratie. Et depuis le sommet de Gleneagles[2251], où les dirigeants tentaient de trouver des solutions profondes à la violence, la priorité de ces États

[2245] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.2.5 *Forces spéciales*
[2246] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.2.5, *Id.*
[2247] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.1, *Id.*
[2248] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*
[2249] M. DELMAS-MARTY, *Aux quatre vents du monde*, *op. cit.,* p. 75.
[2250] B. COURMONT et D. RIBNIKAR, *Les guerres asymétriques : Conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces*, Presse Universitaire de France (PUF), Coll. Enjeux stratégiques, Paris, 2002.
[2251] Sommet du G8 - Gleaneagles, Écosse, Royaume-Uni, 6-8 Juillet 2005 : http://www.jacqueschirac-asso.fr/archives-elysee.fr/elysee/elysee.fr/francais/actualites/deplacements_a_l_etranger/2005/juillet/sommet_du_g8_de_gleneagles_en_ecosse.30502.html; http://www.g8.utoronto.ca/francais/2005gleneagles/sommaire.pdf

a été de fournir une réponse technocentrée, visant un éventail de personnes, voire une population, signalées dans des « fichiers », souvent pour des raisons indépendantes du terrorisme ou des infractions majeures, tels que les fichiers de police nationaux ou le SIS II[2252]. Ces menaces, conflits et crises nécessitent, par conséquent, « de garantir notre autonomie » tout en soutenant la « construction d'une autonomie stratégique européenne », exigeant alors d'investir un effort particulier sur le « rééquilibrage des fonctions stratégiques et sur les coopérations » qui consiste, notamment, à renforcer les fonctions « connaissance et anticipation » et « prévention »[2253] : il s'agit ainsi *« de mieux comprendre les enjeux et d'anticiper les crises, de mieux les prévenir et les gérer selon une logique d'approche globale* », de renforcer « *l'Europe de la défense* », mais aussi de répondre « *à des menaces ou à des scénarios d'intervention plus diversifiés, qu'il s'agisse de faire face à des modes d'action adverses ambigus, notamment dans les espaces cyber et exoatmosphérique, ou à agir dans des environnements moins permissifs* »[2254]. Dès lors, le renforcement de la fonction « connaissance et anticipation » permet, tout à la fois, « une meilleure compréhension des causes et conséquences des crises, de mieux en appréhender les enjeux et d'apporter les réponses les mieux adaptées », tout comme l'effort énoncé au profit de la fonction « prévention » permet « de réduire les facteurs de tension, en amont des crises, et de limiter ainsi le recours à des interventions lourdes »[2255].

[2252] Système d'Information Schengen de 2ème génération (SIS II) qui a pour objet « *d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, ainsi que d'appliquer les dispositions du titre IV, chapitre 3, du traité relatives à la libre circulation des personnes sur les territoires des États membres, à l'aide des informations transmises par ce système.* », Règlement CE N° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), Art 1er : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX%3A32006R1987&from=EN ; Version consolidée par le Règlement UE N° 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), modifiant le règlement (CE) no 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) no 1077/2011 : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32018R1726&from=EN ; et par le Règlement N° 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) no 1987/2006 : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32018R1861&from=EN

[2253] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3. *Garantir notre autonomie et soutenir la construction d'une autonomie stratégique européenne*

[2254] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3., *Id.*

[2255] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.1. *Accentuer notre effort en matière de connaissance, d'anticipation et de prévention*

La fonction « connaissance et anticipation » constitue une priorité des objectifs fixés par le Livre blanc de 2013 mais surtout par la nouvelle loi de programmation de 2018, « qui accentue encore l'effort déjà initié sur le renseignement » ; effort qui intégrera *ipso facto* « l'acquisition d'équipements supplémentaires de collecte et d'exploitation de données, ou le renforcement des capacités humaines et techniques de traitement de ces données », en vue de « mieux anticiper » les évolutions »[2256]. De plus, le renseignement représente également « un enjeu de coopération », compte tenu du fait que la « mise à disposition de capacités nationales et le partage de l'information constituent un véritable levier d'influence et un facteur de crédibilité au sein des coalitions », sans oublier que « ces capacités permettent en outre de maîtriser l'emploi de nos moyens et d'optimiser nos processus de ciblage ». *In fine*, « les capacités de renseignement, mises à disposition de nos partenaires, constituent un outil stratégique à haute valeur ajoutée, apprécié de nos partenaires dans le cadre d'une coalition »[2257].

Dans la même perspective, l'efficacité de cette fonction s'appuie « sur des capacités de veille stratégique, sur la maîtrise et le traitement automatisé de l'information ainsi que sur de nouveaux moyens de surveillance et d'interception électromagnétique »[2258]. À ce titre, « la mutualisation de capacités techniques interministérielles essentielles est poursuivie et approfondie »[2259]. De même, il est apparu nécessaire au gouvernement de rendre son importance à la fonction « prévention » puisque, « indissociable des formats de coopération internationale », l'action de prévention contribuera à « la stabilisation des zones présentant un enjeu direct pour nos intérêts de sécurité » : « *s'inscrivant naturellement dans le cadre d'une approche globale, elle s'appuie sur une coordination étroite entre les armées et l'action diplomatique, mais aussi sur la mobilisation de capacités humaines et financières interministérielles, multinationales, voire privées dans les cas pertinents* »[2260].

Cet ensemble a, dès lors, induit le développement d'une « politique volontariste de coopération européenne et internationale ». En effet, « dans un environnement stratégique plus instable et imprévisible qu'anticipé », il est « indispensable » de renforcer les liens qui unissent la France à ses partenaires à travers le monde, « dans les cadres multilatéraux – notamment européens – comme bilatéraux », exigeant donc un renouvellement du « cadre d'action »[2261]. Renforcer l'autonomie stratégique française passe, en particulier, par un renforcement de l'Europe de la

[2256] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.1., *Id.*
[2257] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.1., *Id.*
[2258] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.1., *Ibid.*
[2259] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.1., *Ibid.*
[2260] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.1., *Ibidem.*
[2261] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2. *Développer une politique volontariste de coopération européenne et internationale*

défense « au moyen de propositions pragmatiques et concrètes : c'est le sens de l'Initiative européenne d'intervention (IEI) voulue par le Président de la République qui doit permettre de construire une culture stratégique commune »[2262]. En la matière, diverses initiatives comme la « coopération structurée permanente » ou le « Fonds européen de défense » se renforcent entre elles « afin de créer une dynamique permettant de développer les capacités militaires européennes dans un cadre collectif, d'inciter à la consolidation de l'industrie de défense par la coopération et de faire naître une véritable autonomie stratégique européenne »[2263].

Il est utile de noter qu'avec le Fonds européen de défense, « l'Union européenne financera pour la première fois depuis sa naissance des actions dans le domaine de la défense et de la sécurité, ce qui constitue un tournant majeur » nécessitant ainsi le « développement d'un réflexe européen » dans la conduite de la « politique industrielle de défense », en vue d'assurer « la crédibilité de ce nouvel instrument »[2264]. Ces initiatives multilatérales sont complémentaires des « relations bilatérales » entretenues avec les partenaires, « notamment allemand, britannique et américain », et elles le sont également « en matière de lutte commune contre le terrorisme djihadiste » ; et, au-delà, les partenariats stratégiques, noués en Asie et dans la région Pacifique, « participent également de cette ambition de partage d'une vision de la sécurité internationale » [2265]. Dès lors, l'établissement de ce cadre rénové facilitera « la protection de nos intérêts économiques et de nos ressortissants, l'assistance apportée à nos partenaires et la préservation de nos marges de manœuvre politico-militaires », et doit aussi conduire à un ajustement des actions de coopération nécessitant, à cet égard, que la France poursuive le « développement de ses partenariats stratégiques en Afrique, au Moyen-Orient ou dans la région indopacifique, qui sont prioritaires »[2266].

En outre, « dans le cadre du rééquilibrage des fonctions stratégiques au profit des fonctions « connaissance et anticipation » et « prévention » », un approfondissement de cette volonté de coopération avec les partenaires et alliés est envisagé, afin que les armées françaises puissent capitaliser sur des « capacités discriminantes à forte valeur ajoutée, pouvant jouer un rôle moteur, voire fédérateur dans des coalitions, en s'appuyant sur l'accélération de l'arrivée de

---

[2262] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Id.*
[2263] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Id.*
[2264] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibid.*
[2265] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibid.* : ainsi, « *l'aptitude de l'Italie et de l'Espagne à se déployer avec un large spectre de capacités justifie un approfondissement des relations bilatérales. […]. La France a noué des partenariats stratégiques majeurs avec l'Inde et l'Australie, qui sont structurants et de longue durée. La France accompagne également le Japon dans son effort d'engagement international accru sur les questions de défense et de sécurité.* »
[2266] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibid.*

matériels nouveaux et le renforcement de la préparation de l'avenir »[2267]. Quant à l'effort manifesté au profit de la fonction « prévention » en particulier, il s'inscrira « dans le cadre d'une approche globale consolidée, alliant sécurité, développement et diplomatie » : dans ce cadre, « l'interopérabilité » entre armées européennes constitue un « facteur clé de succès » et le renforcement des capacités de prévention, « notamment sur le continent africain », est en phase avec la volonté des partenaires de « faire face aux menaces sécuritaires de ces régions, et avec l'objectif de contenir localement les menaces potentielles pour l'Europe »[2268]. Par ailleurs, en matière de coopération capacitaire, le maintien d'une « base industrielle et technologique de défense performante » demeure une condition de l'autonomie de la France, entraînant la quête d'une protection du « capital des entreprises de recherche et développement comme de production industrielle du secteur de la défense »[2269].

Ainsi, le « passage à une échelle européenne » représente, de manière égale, un « enjeu essentiel » pour l'industrie de défense « afin de mutualiser les développements de nouveaux systèmes entre États sur la base de besoins militaires convergents, permettant de réaliser des économies d'échelle »[2270]. À cet égard, la « nouvelle dynamique européenne désormais enclenchée permettra de donner un nouvel élan à la recherche de coopérations résolues et maîtrisées, dont le degré d'interdépendance consentie variera selon les technologies concernées »[2271]. De même, le « passage à une échelle européenne » constitue un « enjeu majeur en matière de recherche et de développement », d'où la mise en œuvre, « dans le cadre du Fonds européen de défense ou d'autres instruments », d'un mécanisme de financement de projets de recherche et de développement « dans un vaste champ de technologies de rupture », permettant à la recherche et à l'industrie l'acquisition de certains équipements « comme les capacités de calcul intensif »[2272].

[2267] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem.*
[2268] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem.*
[2269] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem* : dès lors, « *afin de contribuer au maintien et à la compétitivité de la base industrielle et technologique de défense, la mise en œuvre du principe de préférence européenne pour les marchés publics de défense ou de sécurité, tel que prévu au II de l'article 2 de l'ordonnance no 2015-899 du 23 juillet 2015 relative aux marchés publics, constitue un objectif stratégique.* »
[2270] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem.*
[2271] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem* : ainsi, « *outre la poursuite des programmes en coopération européenne en cours (A400 M, NH90, FREMM, FSAF, MUSIS, Tigre, MIDE-RMV, ANL, TEUTATES) et à l'exclusion des programmes relevant directement de la souveraineté nationale, les programmes d'équipement lancés au cours de la LPM 2019-2025 seront prioritairement conçus dans une voie de coopération européenne. Sont notamment concernés le programme de drone MALE européen (avec l'Allemagne, l'Espagne, l'Italie), les futurs programmes de missiles FMAN et FMC (avec le Royaume-Uni), […], le programme SLAMF (avec le Royaume-Uni), le SCAF-Avion-NG ou la surveillance de l'espace exoatmosphérique (avec l'Allemagne), le FCAS-brique technologique (avec le Royaume-Uni).* »
[2272] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem.*

De plus, dans le domaine industriel, la « politique d'exportation d'armement » contribue à « consolider la position de la France sur la scène internationale » ou à « garantir son autonomie stratégique », mais aussi, « s'inscrivant dans une logique économique, industrielle, opérationnelle et diplomatique, elle contribue à la soutenabilité financière de notre politique de défense et au développement d'un haut niveau d'interopérabilité de nos capacités »[2273]. Cette politique d'exportation d'armement, et plus généralement « l'industrie de défense », constituent un « vecteur de renforcement des liens militaires et politiques, y compris en intra-européens » tout en permettant de « renforcer et de moderniser les capacités des forces des pays alliés et partenaires confrontés aux mêmes défis engendrés par les nouvelles menaces », sans oublier qu'elles valoriseront, également, « l'engagement au combat des équipements » des armées françaises, « véritable atout partagé par peu de pays »[2274].

Il est par conséquent important de s'assurer, « afin de faciliter les coopérations technologiques et industrielles bilatérales et européennes », que les acteurs industriels concernés « puissent exporter ou laisser exporter des matériels d'armement issus de développements ou de productions menés en coopération »[2275]. Le gouvernement s'est récemment félicité d'avoir réussi à « vendre à l'étranger du matériel de guerre français pour un montant de 9,1 milliards d'euros en 2018, en augmentation de 30 % par rapport à 2017 » ; les principales commandes émanant du Moyen-Orient ou d'Asie-Pacifique, notamment de l'Arabie Saoudite, le Riyad, le Qatar, l'Égypte ou l'Inde[2276].

De ce fait, il est prévu des « moyens accrus et une organisation renouvelée pour renforcer et accélérer l'innovation », la nouvelle politique d'innovation s'articulant autour de trois axes : « *i)* des moyens renforcés, *ii)* des outils et des processus permettant d'accélérer la diffusion des innovations, de mieux intégrer l'innovation issue du secteur civil et de mieux prendre en compte l'innovation de rupture, *iii)* un champ d'application élargi à l'ensemble des activités du

[2273] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem.*
[2274] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem.*
[2275] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Ibidem.*
[2276] N. GUIBERT, « La France a vendu des armes pour 9,1 milliards d'euros en 2018 », Le monde, publié le 04 juin 2019 : « *[…]. Les ONG, qui dénoncent depuis de nombreux mois l'emploi d'armes françaises par les belligérants engagés au Yémen, renouvellent leurs critiques. « Les contrats et les livraisons avec des pays accusés de crimes de guerre (Arabie saoudite) ou de répression contre leur population (Égypte) atteignent des montants très élevés », regrette Tony Fortin, de l'Observatoire des armements, qui accuse la France de violer ses engagements pris dans le cadre du traité sur le commerce des armes (TCA). […]. La ministre des armées justifie la position française par ses intérêts stratégiques. « Aujourd'hui, 13 % des emplois industriels sont dans le secteur de l'armement », souligne Florence Parly, en préface du rapport. Et cette politique d'exportation « est également vitale pour notre diplomatie ». Mme Parly se réjouit qu'en 2018 la part des Européens dépasse pour la première fois 25 % des commandes – avec la fourniture de vingt-trois hélicoptères à l'Espagne, pour 1,5 milliard d'euros.* » : https://www.lemonde.fr/international/article/2019/06/04/la-france-a-vendu-des-armes-pour-9-1-milliards-d-euros-en-2018_5471354_3210.html

ministère et intégrant les innovations d'usage »[2277]. Des moyens sont à cet égard prévus (1 Md€ par an dès 2022 contre 730 M€ par an en moyenne dans la précédente LPM) permettant de financer le développement des « technologies nécessaires à la préparation des programmes d'équipement futurs » et d'autres dispositifs « pour soutenir l'innovation technologique et l'innovation d'usage, tels que les aides à l'innovation ou l'investissement en fonds propres (*Definvest*) pour les PME, ainsi que les plateformes d'innovation, notamment avec la création d'un « Défense Lab » »[2278].

Cet « effort financier », consenti par la nouvelle loi de programmation, et les nouveaux outils mis en place permettront principalement de : « capter en cycle court l'innovation issue du marché civil, en tirant parti de la révolution numérique et en mettant l'accent sur l'innovation d'usage, démarche qui s'appuiera largement sur la construction d'un écosystème d'innovation, interne au Ministère des Armées et connecté avec les écosystèmes d'innovation civils » ; « maintenir l'investissement dans la maturation des technologies spécifiques au domaine de la défense » ; « mieux investir dans l'innovation de rupture et de supériorité opérationnelle, notamment dans la robotique, l'intelligence artificielle, l'informatique quantique, la cryptographie, la génération d'énergie, l'hypervélocité, la furtivité[2279] et la cyberdéfense »[2280]. Ces trois axes « d'efforts complémentaires » conduiront « nécessairement à faire évoluer » les processus existants, « notamment dans le sens d'une démarche incrémentale permettant de tester et d'intégrer en boucle courte les innovations », et supposent aussi « un recours plus fréquent à l'expérimentation technico-opérationnelle »[2281].

En outre, l'importance d'une « industrie de défense française forte » a été soulignée, « dans la mesure où elle s'avère une composante essentielle de l'autonomie stratégique de la France et peut seule garantir la sécurité de notre approvisionnement en équipements de souveraineté et en systèmes d'armes critiques »[2282]. Cette base industrielle et technologique de défense (BITD), « fruit d'un investissement continu », est caractérisée par un niveau « très élevé de recherche et de développement » et conforte « *notre compétitivité technologique » : « au quotidien, ce sont une dizaine de grands groupes industriels, 4 000 PME et ETI* [entreprise de taille intermédiaire] *et 200 000 personnes qui animent un tissu industriel et technologique de défense de très haut*

[2277] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.1. *Des moyens accrus et une organisation renouvelée pour renforcer et accélérer l'innovation au service de nos armées*
[2278] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.1., *Id.*
[2279] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id. :* « *Furtivité : caractéristique d'un engin terrestre, aérien ou naval, dont la signature est rendue difficilement détectable.* »
[2280] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.1., *Id.*
[2281] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.1., *Ibid.*
[2282] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.3. *Renforcer la BITD pour garantir notre autonomie stratégique*

niveau »[2283]. La direction générale de l'armement, « dans une période où les opérations militaires connaissent des évolutions rapides », conduit un travail « permanent d'évaluation des compétences » nécessaires à la réalisation et au maintien d'équipements de défense, l'objectif étant de maintenir un haut niveau d'excellence mondiale des « compétences accessibles ou maîtrisées par l'industrie française », afin d'être en mesure de « développer de nouvelles technologies et de nouveaux types d'armements intégrant les évolutions récentes observées dans les domaines comme la cybernétique, l'espace, le traitement de l'information, les drones, la robotique, les technologies relatives à l'énergie dirigée, etc. »[2284].

Cet effort consenti dans le domaine de la « recherche et technologie » contribue, *ipso facto*, au développement et au renforcement de la « culture d'innovation », une des conditions essentielles pour « l'adaptation des compétences comme des équipements à l'évolution des systèmes adverses et concurrents »[2285]. De même, cet effort s'inscrit dans « l'esprit du Pacte Défense PME et profitera à l'ensemble de la BITD, plus particulièrement aux start-up et PME du secteur ou celles susceptibles d'apporter des innovations de rupture », et permet de compléter « les dispositifs de soutien industriel en place (RAPID, fonds d'investissement *Definvest*) »[2286]. Par ailleurs, en termes de « perspectives d'exportation », le portefeuille des armements dont disposera la BITD sera « très largement renouvelé grâce aux investissements consentis » au cours de cette loi de programmation[2287], sans compter les opportunités offertes par des mécanismes comme « le Fonds européen de défense » qui seront « pleinement exploitées », ou encore les « rapprochements industriels susceptibles de consolider la base industrielle et technologique de défense à un niveau européen » qui seront fortement encouragés, « sous réserve de préserver les branches de la BITD française relevant de la souveraineté nationale »[2288].

Cette loi de programmation militaire de 2018 est donc un « *levier majeur de notre économie* »[2289], techno-centrée visant principalement l'exploitation et la maîtrise de l'information, « condition de la supériorité informationnelle » et de la modernisation des équipements et dispositifs, contribuant, *in concreto*, au « capitalisme de surveillance »[2290] mais

[2283] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.3., *Id.*
[2284] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.3., *Id.*
[2285] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.3., *Ibid.*
[2286] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.3., *Ibidem.*
[2287] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.3., *Ibidem.*
[2288] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.2., *Id.*
[2289] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.4.3., *Id.*
[2290] *Cf.* p. 371, 380 et 444 et s.

aussi à la fabrication d'un État d'exception généralisé, grandement régulé par le numérique et les nouvelles technologies de l'information et de la communication.

§2. La fabrique d'un État d'exception

La fabrique et la mise au point d'un État d'exception, banalisé graduellement, se caractérise, en particulier, par une nouvelle conception des notions de souveraineté et de gouvernance, donc quand la souveraineté devient numérique (A), mais aussi par une conception innovante des notions d'urgence et d'exception, à savoir quand l'exception devient la règle (B).

A. Une nouvelle conception de souveraineté et de gouvernance, ou quand la souveraineté devient numérique

Un Livre blanc désigne un document qui « *fixe la stratégie française de défense et de sécurité nationale, et précise notamment son articulation avec la politique de sécurité et de défense commune de l'Union européenne et avec l'Alliance Atlantique, et les capacités requises pour la mettre en œuvre dans les quinze à vingt ans à venir* »[2291]. La politique de défense et de sécurité mise en œuvre, initialement par le Livre blanc de 2008[2292], puis reprise et renforcée par celui de 2013, et dont ont découlé les lois de programmation de 2013 et de 2018 susmentionnées, semble tracer les contours d'une nouvelle conception de la souveraineté et de la gouvernance centrée sur le numérique, le renseignement, la connaissance et l'information. Désormais « *entrés dans une ère de grandes turbulences* », les manifestations des « *risques* [et des] *menaces auxquels nous sommes confrontés* » se sont multipliées, « *leurs effets se sont amplifiés et rapprochés* », leur « accumulation » traduisant un « *affaiblissement du système international et l'émergence d'acteurs qui cherchent à le contester ouvertement* »[2293], et nécessitant, de manière pragmatique, l'adoption d'une « vision stratégique » renouvelée afin de maintenir la souveraineté et les intérêts de la France ; vision consacrée par la nouvelle loi de programmation dressant une stratégie de défense et de sécurité innovante. Selon le Président Macron, « *la sécurité et la défense de la Nation engagent bien sûr l'intégralité de la communauté de défense. Mais c'est l'ensemble de l'État et, au-delà, toutes les ressources vives*

[2291] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*
[2292] Livre blanc sur la défense et la sécurité nationale, Ed. Odile Jacob/ La Documentation française, Paris, 2008 : http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html
[2293] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », DICoD - Bureau des Éditions, Octobre 2017, p. 5 ; disponible en ligne : https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017

de la communauté nationale - ses collectivités, ses forces politiques, ses entreprises, sa jeunesse - qui doivent se mobiliser autour de ces enjeux »[2294], semblant suggérer un retour à « *l'état de nature défini par Hobbes : la guerre de tous contre tous* »[2295].

De manière liminaire, il est utile de relever que la réponse apportée par ces dispositifs juridiques mélange, unanimement, les notions de « défense » et de « sécurité » qui, pourtant, ne doivent pas faire l'objet de confusion, puisque la défense traitant de la sécurité, celle-ci n'en est finalement qu'une composante, et leur traduction, que ce soit en anglais ou en allemand, est différente de surcroît[2296]. Autrement dit, ces notions « *n'ont ni les mêmes traductions, ni les mêmes réalités historiques, ni les mêmes réalités constitutionnelles, ni les mêmes pratiques actuelles chez nos partenaires, chez nos alliés ou encore chez nos adversaires potentiels et ennemis éventuels* »[2297]. La notion structurante d' « adversaire » voire celle d' « ennemi » donne l'impression d'élaborer une politique de défense qui viserait l'ennemi, là où celle de sécurité viserait l'adversaire ; or, ce n'est pas le cas, ces notions étant souvent employées de manière interchangeables, reprises d'ailleurs par le Livre blanc de 2013 ainsi que les lois de programmation qui ont suivi marquant, *in concreto*, le retour de l'individu dangereux, de la dangerosité et de la dichotomie ami/ennemi susmentionnés[2298].

Ces confusions se sont concrétisées grâce au Livre blanc de 2008 principalement, ayant établi le concept de « politique de défense et de sécurité nationale » signifiant un « *continuum* » entre la défense et la sécurité alors même que le terme lui-même « n'est jamais employé par les rédacteurs » de ce Livre, « l'idée qu'il exprime est cependant omniprésente dans ce texte » et non remis en cause par le Livre de 2013[2299]. Ce vocable paraît ainsi être « *celui qui traduit le mieux le rapprochement entre le champ de la défense et celui de la sécurité intérieure, tel qu'il est vécu depuis la chute du Mur de Berlin* », mais aussi celui qui « *témoigne de la fin d'une époque dominée par l'alternat paix/guerre, avec un temps pour le « civil » et un temps pour le « militaire », une distinction entre l'ennemi et l'adversaire, une séparation entre le front et l'arrière, etc.* »[2300]. Pourtant, la Constitution française place, à son article 15, le Président de la République en « chef des armées » qui « préside les conseils et comités supérieurs de la défense

---

[2294] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », *Id.*, p. 7.

[2295] P. BROUILLET, « Sécurité intérieure et gestion de la violence », *In* F. Debove et O. Renaudie (Dir.), *Sécurité Intérieure : Les nouveaux défis*, Ed. Magnard-Vuibert, 2013, p. 10.

[2296] En allemand par ex., la défense « *Verteidigung* » est perçue bien différemment de la sécurité « *Sicherheit* », terme qui comprend une notion de sûreté (Sicher = sûr).

[2297] Amiral J. LAUNAY, « Sécurité et défense », RFDA 2011, p. 1099.

[2298] *Cf.* p. 463 et s.

[2299] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *In* F. Debove et O. Renaudie (Dir.), *Sécurité Intérieure : Les nouveaux défis*, *Id.*, p. 303.

[2300] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *Id.,* p. 303.

nationale », et place le Premier ministre, à son article 21, en « responsable de la défense nationale ». Mais il semble que face aux « *menaces diffuses, réelles ou supposées, liées à la mondialisation accusée de détruire les frontières et donc d'accroître les dangers : la distinction entre sécurité intérieure et défense serait désormais caduque* »[2301], que ce soit dans l'esprit de l'État ou de la société.

À travers l'évolution du monde, des cultures et des mentalités, la distinction entre sécurité et défense n'a plus lieu d'être « ou, plus précisément, la sécurité nationale inclut désormais la défense, qui lui est subordonnée », alors même que les « modalités d'intervention ne sont pas les mêmes »[2302], que leurs traductions sont distinctes, que la sécurité est parfois confondue avec ou rapprochée de la sûreté, et ce même dans les textes des Livres et lois en cause. Certes, l'ordonnance du 7 janvier 1959[2303] avait déjà consacré l'idée innovante d'une « combinaison des moyens militaires, civils et économiques » ainsi que celle de « défense globale »[2304], apparaissant, dès cette époque, « comme le socle d'une défense globale prenant en compte la permanence et l'universalité des menaces » ; mais la guerre froide avait déplacé « le centre de gravité du tryptique au profit de la défense militaire »[2305]. Néanmoins, le Livre blanc de 2008 et son successeur ainsi que les nombreuses réformes législatives adoptées ont modifié ou plutôt entériné le prisme des considérations de défense et de sécurité[2306], mais aussi la confusion entre celles de menaces et de risques, de sécurité intérieure et de sécurité extérieure, de cybersécurité et de cyberdéfense, d'adversaire et d'ennemi, et notamment de stratégie et d'intérêts stratégiques.

L'ancien Président de la République Sarkozy ayant commandé la rédaction du Livre de 2008 l'avait annoncé en affirmant qu' « *émerge un nouveau concept : celui d'une stratégie de sécurité*

[2301] P. BROUILLET, « Sécurité intérieure et gestion de la violence », *Id.,* p. 3.
[2302] P. BROUILLET, « Sécurité intérieure et gestion de la violence », *Ibid.,* p. 10.
[2303] Ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense, abrogée le 24 avril 2007.
[2304] Amiral J. LAUNAY, « Sécurité et défense », *Id.*, p. 1099.
[2305] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *Id.,* p. 306, et l'auteur souligne (note de bas de p. n° 5) : « *La défense civile est restée cantonnée dans le domaine de l'ordre public, quant à la défense économique, elle a pris la forme d'une « économie de défense » et non d'une « défense de l'économie »* ».
[2306] L'Art. L. 1111-1 du Code de la défense (Modifié par la Loi n°2009-928 du 29 juillet 2009 - Art. 5) en fournit une parfaite illustration : *« La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter.*
L'ensemble des politiques publiques concourt à la sécurité nationale.
La politique de défense a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées. Elle contribue à la lutte contre les autres menaces susceptibles de mettre en cause la sécurité nationale. Elle pourvoit au respect des alliances, des traités et des accords internationaux et participe, dans le cadre des traités européens en vigueur, à la politique européenne de sécurité et de défense commune. »

nationale, qui associe, sans les confondre, la politique de défense, la politique de sécurité intérieure, la politique étrangère, et la politique économique »[2307], la défense devenant donc l'une des politiques publiques qui participent à la nouvelle stratégie de sécurité nationale. En effet, le Livre blanc en question « *expose une stratégie non seulement de défense, mais aussi de sécurité nationale. Son objet est de parer aux risques et aux menaces susceptibles de porter atteinte à la vie de la nation. […]. Cette stratégie inclut donc aussi bien la sécurité extérieure que la sécurité intérieure, les moyens militaires comme les moyens civils, la politique de défense proprement dite et la politique de sécurité intérieure et de sécurité civile, la politique étrangère et la politique économique* » ; une stratégie visant principalement à « *s'adapter aux bouleversements engendrés par la mondialisation* » et à préserver la souveraineté de l'État qui « *consiste en tout premier lieu à protéger sa population* »[2308].

Aborder la sécurité nationale en termes généraux et globaux, en faisant appel à toutes les forces de la Nation, révèle l'évolution vers ce monde globalisé que l'Amiral Labouérie nommait « le *stratomonde* »[2309], qui requiert une approche globale, décloisonnée et intelligente de la stratégie de sécurité, approche suivie fidèlement par les deux dernières lois de programmation et leurs rapports annexés fournissant l'orientation future de la politique de défense et de sécurité nationale. Le terme intelligent employé doit s'entendre dans sa version anglaise « *intelligence* » ou encore dans un sens étymologique, du latin « *intellegentia* », faculté de comprendre, dérivé de « *intellegere* », comprendre, et où *inter* (entre), et *legere* (choisir, cueillir) ou *ligare* (lier) évoquent, notamment, l'aptitude à relier des éléments qui sans elle resteraient scindés, une capacité de lire à l'intérieur, de discerner, de recueillir, voire de recueillir par les oreilles ou les yeux[2310]. L'intelligence représente l'anticipation utile, se mesurant *a posteriori* par la satisfaction des besoins de l'entité qui l'emploie, mais aussi la faculté d'adapter des moyens à des fins, la faculté de comprendre, de saisir des rapports et d'organiser, à l'image d'un musicien agençant les notes et les rythmes, ou un politicien ou un militaire développant une stratégie[2311].

[2307] Livre blanc sur la défense et la sécurité nationale 2008, « Préface du Président de la République », *Id.,* p. 10.

[2308] Livre blanc sur la défense et la sécurité nationale 2008, *Id.,* p. 16 et 123.

[2309] Amiral G. LABOUÉRIE, *Stratégie : Réflexions et Variations*, Ed. ADDIM, Coll. Esprit de défense, 1993, Chap. 2 notamment, p. 31 et *sq*., et l'Amiral précise, en avant-propos : *« […], nous sommes entrés dans un « stratomonde » où il n'existe guère que deux types d'acteurs, ceux qui en ont conscience et s'en donnent les moyens, intellectuels, conceptuels, matériels …, et tous les autres, conscients ou non, dépourvus ou non, qui subiront les évènements sans pouvoir les orienter.* », p. 11.

[2310] Courant philosophique, Lexique « Intelligence », du 09/03/2010 : http://www.histophilo.com/intelligence.php#cite_ref-2, et Encyclopédie de l'Agora, « Intelligence », du 12/04/2013 : http://agora.qc.ca/Dossiers/intelligence

[2311] Selon Thomas d'Aquin, « *l'intelligence tire son nom de l'intime pénétration de la vérité ; son acte consiste en quelque sorte à lire à l'intérieur, "dicitur enim intelligere quasi intus legere" ; elle a pour objet l'essence même des choses ; mais celle-ci ne peut être atteinte que par une vue qui pénètre plus loin que les apparences*

C'est donc détenir la capacité de discernement qui mène à la finalité que constitue la sécurité nationale, *« objectif jamais atteignable mais à poursuivre toujours »*[2312].

La défense doit alors disposer d'une action militaire renforcée, en coopération et en collaboration continues, et résiliente, caractérisée par le « retour » de l'armée sur le territoire national pour assurer la stratégie déterminée et les fonctions stratégiques afférentes, en accordant au gouvernement les moyens humains et techniques, quantitatifs et qualitatifs, adaptés, compte tenu du fait que la *« gouvernance du continuum appelle une approche globale, combinaison des politiques publiques »*[2313]. C'est bien l'ensemble du spectre composant cette vision stratégique de défense et de sécurité qui permet que l'action se déroule de manière continue et croissante dans la perception de l'intensité, de la connaissance, à l'anticipation, à la prévention, à la protection et à l'intervention, avec l'ultime défense que représente la stratégie de dissuasion « cette « assurance vie » de la Nation »[2314], qui justifie aux termes du Président Macron « *la raison pour laquelle j'ai décidé le maintien de notre stratégie de dissuasion nucléaire et le renouvellement de ses deux composantes : elles sont la garantie ultime de nos intérêts vitaux, de notre indépendance et, plus largement, de notre liberté de décision* »[2315].

Or, l'Amiral Launay précise que « *l'idée de dissuasion, théorisée depuis longtemps, est un acte militaire de tous les jours avec les marins et les aviateurs qui en assurent la permanence et l'opérationnalité, à la disposition du pouvoir politique, qui en exerce le contrôle, et le cas échéant décide sa mise en œuvre* »[2316]. Pour illustration, l'armée de l'air qui a vu ses capacités renforcées progressivement[2317], en particulier depuis les événements de septembre 2001, et « exerce désormais une véritable « police du ciel » »[2318] par le biais de la « posture permanente de sûreté (PPS) » susmentionnée, afin de poursuivre la stratégie de défense fixée. En effet, « *la*

---

extérieures », Encyclopédie de l'Agora, *Id.,* [Dictionnaire pratique des Connaissances religieuses, J. Bricout (dir.), édité par Librairie Letouzey et Ané, Paris, 1925-1927, p. 1055].

[2312] Amiral J. LAUNAY, « Sécurité et défense », *Id.*, p. 1099.

[2313] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *Id.,* p. 309.

[2314] Amiral J. LAUNAY, « Sécurité et défense », *Id.*, p. 1099-1100.

[2315] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », *Id.*, p. 6.

[2316] Amiral J. LAUNAY, « Sécurité et défense », *Ibid.*, p. 1100, et Décret n° 2009-1118 du 17 septembre 2009 relatif au contrôle gouvernemental de la dissuasion nucléaire, JORF n° 0216 du 18 septembre 2009, p. 15200, texte n° 1.

[2317] Ainsi, la Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.2.2.4 *Armée de l'air/Forces aériennes,* précise que « *L'armée de l'air continuera d'assurer les missions permanentes de la composante aéroportée de la dissuasion nucléaire, de protection de l'espace aérien national et de ses approches. Sa participation aux forces de souveraineté et de présence contribuera également à la prévention des crises. Elle mettra également en œuvre des capacités de supériorité aérienne, de frappe dans la profondeur, de renseignement, de transport stratégique et tactique, d'appui aux forces spéciales et aux composantes de surface, terrestre et maritime. L'aptitude des forces aériennes à être interopérables avec les forces alliées sera essentielle.* »

[2318] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *Id.,* p. 313.

défense c'est avant tout penser la guerre, penser les guerres, et mettre en œuvre une violence « légale » qu'on doit espérer légitime »[2319].

Par ailleurs, dans la mesure où le cyberespace est « devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires »[2320], et caractérise un « théâtre d'actions agressives régulières, aux conséquences potentiellement dramatiques »[2321], nécessitant le développement de capacités de lutte dans cet espace, il participe à ce *continuum* défense-sécurité mais aussi à l'implication des forces de l'armée, qui comprennent également la gendarmerie, au sein du territoire ; de sorte que, combinés aux autres espaces ayant également subis des conflits nécessitant l'intervention de l'armée pour la prévention et la protection, la présence des armées est, depuis un certain moment déjà, enracinée « dans le quotidien des Français »[2322].

En effet, « *en plus des crises ouvertes dans lesquelles elles sont impliquées ou susceptibles de l'être à travers les dispositifs de souveraineté et de prépositionnement, les armées sont également directement engagées sur le territoire national, outre-mer comme en métropole, dans le cadre de la posture de dissuasion, et de missions de protection (mission Sentinelle), de sauvegarde maritime et de sûreté aérienne. Ce dispositif s'appuie sur un réseau de bases, permanentes ou projetées, dont le maintien représente un investissement et un atout pour la sauvegarde de nos intérêts et l'exercice de nos responsabilités globales* »[2323].

Finalement, comme l'indique le Général Watin-Augouard, cette stratégie de sécurité nationale représente le *« fruit d'une rupture sémantique prenant acte du caractère désormais hybride des menaces* [qui] *est mise en œuvre par une gouvernance rénovée, plus centrée sur la fonction présidentielle et plus interministérielle, qui doit favoriser une gestion civilo-militaire des crises* », de sorte que « la nature des menaces conjuguée à l'intrication des modes d'action induit une « policiarisation » des opérations militaires et une « militarisation » des opérations

[2319] Amiral J. LAUNAY, « Sécurité et défense », *Id.*, p. 1100.
[2320] Livre blanc sur la défense et la sécurité nationale 2008, *Id.,* p. 53.
[2321] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », *Id.*, p. 5.
[2322] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *Id.,* p. 312, où le Général précise qu' « *en 1985, des forces sont déployés aux frontières et dans la capitale. En 1995, le dispositif Vigipirate se met en place à la suite d'une vague d'attentats ayant touché la capitale. Les attentats du 11 septembre 2001, ceux de Madrid (2004), de Londres (2005) ou de Bombay (2008) enracinent la présence de l'armée dans le quotidien des Français. Mais la lutte contre le terrorisme n'en est pas la seule motivation. En Guyane, l'opération Harpie, conduite contre les orpailleurs clandestins, témoigne de l'engagement conjoint de l'armée de terre aux côtés de la gendarmerie dans une mission de sécurité.* »
[2323] Revue Stratégique de défense et de sécurité nationale 2017, *Id.,* p. 28, point 61.

policières » ; le *continuum* gommant les « frontières traditionnelles entre défense et sécurité » et pouvant conduire à « une forme de banalisation de la notion de militarité »[2324].

Le monde de l'après-guerre froide a très vite cédé « *la place à un monde plus mobile, plus incertain et imprévisible, exposé à des vulnérabilités nouvelles* » : « *dans ce monde qui vient, la sécurité de la nation sera assurée et la France jouera tout son rôle pour la défense de la paix et de ses valeurs* »[2325] ; et « *l'idée européenne même, projet de paix et de prospérité né des drames du siècle passé, est profondément ébranlée, par le Brexit, par la crise des réfugiés et par le doute qui naît dans nos populations sur la capacité de l'Europe à les protéger* »[2326]. Dans cet environnement, « *qui remet en cause les certitudes et les repères de trois décennies, seule une France forte, maîtresse de son destin, peut apporter des réponses aux grandes crises contemporaines, promouvoir ses valeurs et faire valoir ses intérêts. Cette ambition ne peut se passer d'une diplomatie et d'une défense de premier plan, soutenues par une grande armée, forte et crédible, capable d'agir face à toutes les menaces et dans tous les espaces* », impliquant la nécessité de conserver « *la capacité d'initiative et d'action qui garantit notre souveraineté* » ; c'est la raison pour laquelle, indique le Président Macron, « *je souhaite que nos armées et nos services de renseignement disposent de tous les moyens nécessaires à leurs missions, afin qu'ils puissent faire face tant aux engagements d'aujourd'hui qu'aux enjeux de demain. Dans cet environnement stratégique incertain, [...], nous avons besoin d'un outil de défense agile, projetable et résilient* »[2327].

C'est principalement grâce au Livre blanc de 2013 que fut créée une large communauté et culture de renseignement, amorcée avec celui de 2008 et concrétisée par le décret de 2014 portant désignation des services spécialisés de renseignement[2328], articulée autour de trois grands axes, l'intérieur, l'économie et les armées, et incluant des services "généralistes", notamment la Direction Générale de la Sécurité Intérieure (D.G.S.I.) et la Direction Générale de la Sécurité Extérieure (D.G.S.E.), plusieurs services spécialisés[2329] mais aussi un Conseil

[2324] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *Ibid.,* p. 304.
[2325] Livre blanc sur la défense et la sécurité nationale 2008, « Préface du Président de la République », *Id.,* p. 11.
[2326] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », *Id.*, p. 5-6.
[2327] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », *Ibid.*, p. 6.
[2328] Décret n° 2014-474 du 12 mai 2014 pris pour l'application de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires et portant désignation des services spécialisés de renseignement, JORF n°0111 du 14 mai 2014, p. 7968, texte n° 1.
[2329] Tels que : Le Traitement du Renseignement et de l'Action contre les Circuits Financiers clandestins (TRACFIN), la Direction Nationale de Renseignements et des Enquêtes Douanières (D.N.R.E.D.), la Direction

National du Renseignement (C.N.R.)[2330], comprenant la fonction de Coordonnateur National du Renseignement[2331], modifié par le décret du 14 juin 2017[2332] en fonction de Coordonnateur National du Renseignement et de la Lutte contre le Terrorisme[2333], sans compter les autres entités participant à l'action du renseignement[2334].

À cet égard, il est intéressant de noter qu'un rapport d'information de la délégation parlementaire au renseignement a été publié en 2013[2335], premier rapport relatif au renseignement publié depuis 1958, consacré à la « compréhension du renseignement », qualifié « d'activité essentielle à la protection de la démocratie », comprenant, toutefois, « plusieurs passages masqués au moyen de signes typographiques »[2336] et ce « en raison des impératifs du

---

du Renseignement Militaire (D.R.M.), ou la Direction du Renseignement et de la Sécurité de la Défense (D.R.S.D.)

[2330] Académie du Renseignement, « La coordination nationale du renseignement et de la lutte contre le terrorisme », Le Conseil National du Renseignement : « *Le Conseil national du renseignement, formation spécialisée du Conseil de défense et de sécurité nationale, définit les orientations stratégiques, les priorités en matière de renseignement et établit la planification des moyens humains et techniques des services de renseignement. Y siègent, sous la présidence du chef de l'État, le Premier ministre, les ministres concernés et les directeurs des services de renseignement dont la présence est requise par l'ordre du jour, ainsi que le coordonnateur national du renseignement. Ce conseil arrête la stratégie nationale du renseignement.* » : http://www.academie-renseignement.gouv.fr/coordination.html

[2331] Pour plus d'informations, Article (1/2) « L'organisation des services de renseignement français », Master 2 Pro ECA, publié le 18 mai 2017 : https://proeca-pantheon-sorbonne.com/2017/05/18/article-lorganisation-des-services-de-renseignements-francais-12/ ; et, l'Académie du Renseignement, « La communauté française du renseignement » : http://www.academie-renseignement.gouv.fr/communaute.html

[2332] Décret n° 2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme, JORF n° 0139 du 15 juin 2017.

[2333] Académie du Renseignement, « La coordination nationale du renseignement et de la lutte contre le terrorisme », Le Coordonnateur National du Renseignement et de la Lutte contre le Terrorisme, *Id.* : « *Le coordonnateur national du renseignement et de la lutte contre le terrorisme conseille le président de la République dans le domaine du renseignement. Il lui transmet, ainsi qu'au Premier ministre, les informations fournies par les services qui doivent être portées à sa connaissance. Il rapporte devant le Conseil national du renseignement dont il prépare les réunions et veille à la mise en œuvre des décisions. Il prépare la stratégie nationale du renseignement et le plan national d'orientation du renseignement. Garant de la cohérence et de l'efficacité de leur action, il s'assure de la bonne coopération des services spécialisés constituant la communauté française du renseignement. […].* »

[2334] Telles que : le commandement de cyberdéfense (COMCYBER) au sein de l'état-major des armées ; l'agence nationale de sécurité des systèmes d'informations (ANSSI) au sein du secrétariat général de la Défense et à la Sécurité nationale ; la sous-direction anti-terroriste (SDAT), l'unité de coordination de la lutte antiterroriste (UCLAT) ou le service central du renseignement territorial (SCRT) au sein de la direction générale de la Police nationale ; la direction du Renseignement de la préfecture de police de Paris (DRPP) au sein de la préfecture de police de Paris ; le Bureau de la lutte anti-terroriste (BLAT) ou la Sous-direction de l'anticipation opérationnelle (SDAO) au sein de la Gendarmerie nationale ; le Bureau central du renseignement pénitentiaire (BCRP) au sein de la Direction de l'Administration Pénitentiaire ; voir également les Art. D. 3126-1 et s. du Code de la défense.

[2335] Délégation parlementaire au renseignement, Rapport N° 1012 (Assemblée Nationale) N° 557 (Sénat) (1012/557) relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2012, Par Mme P. ADAM (Députée), du 30 avril 2013 ; Disponible en ligne : http://www.assemblee-nationale.fr/14/rap-off/i1012.asp#P139_3767

[2336] C. JOURNÈS, « Alternance et continuité en matière de sécurité intérieure », RSC 2013, p. 889.

secret de la défense »[2337]. Les rapports d'information de la délégation publiés en 2017[2338] et en 2018[2339] s'inscrivent dans la même lignée en masquant plusieurs passages[2340], conformément aux dispositions du Code pénal relatives au « secret de la défense nationale »[2341] qui, pourtant, requièrent « un nécessaire toilettage » dans la mesure où les « atteintes aux intérêts fondamentaux de la Nation »[2342] constituent des atteintes à la « sécurité nationale », mais la protection du secret de la défense nationale a « *pour objectif d'assurer la sauvegarde des intérêts fondamentaux de la Nation dans les domaines de la défense, de la sécurité intérieure et de la protection des activités économiques et du patrimoine de la France* »[2343].

Selon le Professeur Journès, cette « *vacuité des rapports publics de la délégation parlementaire au renseignement, par contraste avec ceux de l'Intelligence and Security Committee au Royaume Uni, alors que cet organe, [...], dépend pourtant du Premier ministre [...], justifie une formulation sévère : on peut se demander quelle est la cohérence d'une structure parlementaire dont la production n'est destinée à informer ni le Parlement, ni même les citoyens, mais seulement le pouvoir exécutif* »[2344].

Ces différents rapports parlementaires précités évoquent l'évolution des menaces où la « *menace du terrorisme djihadiste n'est pas la seule ; d'autres menaces s'affirment, des crises*

[2337] Avertissement du Rapport N° 1012/557 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2012, *Id.,* la formulation complète de l'Avertissement étant : « *Les parties en blanc correspondent à des éléments que la délégation parlementaire au renseignement a décidé de ne pas publier en raison des impératifs du secret de la défense nationale* ».

[2338] Délégation parlementaire au renseignement, Rapport N° 4573 (Assemblée Nationale) N° 448 (Sénat) relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016, Par Mme P. ADAM (Députée), du 2 mars 2017 ; Disponible en ligne : http://www2.assemblee-nationale.fr/static/14/DPR/i4573.pdf

[2339] Délégation parlementaire au renseignement, Rapport N° 875 (Assemblée Nationale) N° 424 (Sénat) relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017, Par M. P. BAS (Sénateur), du 12 avril 2018 ; Disponible en ligne : http://www2.assemblee-nationale.fr/content/download/69939/714118/version/1/file/Rapport+DPR+2017_version+publique.pdf

[2340] Délégation parlementaire au renseignement, Rapport N° 875/424 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017, *Id.*, p. 13, où il est annoncé « *Nonobstant son souci de répondre aux légitimes attentes de transparence des citoyens, les membres de la DPR ont également conscience que certaines informations portées à leur connaissance doivent être soustraites à la curiosité de nos rivaux comme de nos adversaires. C'est pour parvenir à concilier ces deux impératifs antagonistes qu'il a été décidé de masquer quelques passages sensibles au moyen d'un signe typographique (*****), invariable quelle que soit l'ampleur des informations rendues ainsi illisibles.* »

[2341] Code pénal, Art. 413-9 à 413-12 (Modifiés par la loi n°2009-928 du 29 juillet 2009) ; et *Cf.* p. 345 et s.

[2342] Code pénal, Art. 410-1 « *Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel* ».

[2343] Général d'Armée M. WATIN-AUGOUARD, « Le *continuum* défense sécurité intérieure », *Id.,* p. 307 ; et Circulaire de la DACG n° Crim 08-01/G1 du 3 janvier 2008 relative au secret de la Défense nationale, Bulletin Officiel du Ministère de la Justice de 2008, Texte 13/22, p. 1 ; Disponible en ligne : http://www.textes.justice.gouv.fr/art_pix/boj_20080001_0000_0013.pdf

[2344] C. JOURNÈS, « Alternance et continuité en matière de sécurité intérieure », *Id.*, p. 891.

peuvent survenir à tout moment »[2345], notamment dans le cyberespace moyennant des dispositifs et des techniques numériques hybrides et protéiformes. Ces rapports, et particulièrement celui pour l'année 2016, font aussi état, *inter alia*, des nombreux emplois et recours aux « fichiers », tout en soulignant la nécessité de leur consultation, surtout au regard du fait que les États-Unis ont acquis un monopole de consultation dans divers secteurs (bancaires, aériens etc.), du renforcement de la coopération, de la mutualisation, de la convergence et de l'interopérabilité, ou encore du renforcement de la surveillance et des capacités de renseignement pour assurer, en particulier, la fonction « connaissance/anticipation ».

Ces « fichiers » désignent, par exemple, le système PNR[2346], soit des données relatives aux passagers aériens, le fichier des personnes recherchées (FPR), soit des donnés sur les personnes recherchées mises en relation avec les données du système PNR par exemple, dans le cadre duquel les personnes suspectées de terrorisme sont recensées au moyen d'une « fiche S », la lettre S signifiant « atteinte à la sûreté de l'État »[2347] ; le fichier des signalés pour la prévention de la radicalisation à caractère terroriste (FSPRT), partagé entre différents services ; les fichiers administratifs et fichiers de police, partagés entre différentes administrations partenaires (police judiciaire, douane, services de renseignement, administration fiscale, organismes sociaux, etc.) ; le fichier central des comptes des personnes morales et physiques, promu par les actions du TRACFIN qui œuvre à la levée des entraves à la coopération internationale en faisant aussi la promotion du droit de communication de chaque cellule ou de l'accès direct aux données, par exemple ; le fichier des personnes signalées par le Service central du renseignement du territoire (SCRT), données pouvant être inscrites au fichier des signalés pour la prévention et la radicalisation à caractère terroriste. Il s'avère alors que, penser la sécurité « *sans l'apport des nouvelles technologies et, plus précisément, sans faire référence aux bases de données et traitements automatisés de données à caractère personnel, dits fichiers, paraît, en ces débuts du XXI*ème *siècle, inconcevable* »[2348]. Et les rapporteurs de 2016 ont tout de même relevé que la

---

[2345] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », *Id.*, p. 6.

[2346] *Cf.* p. 288 et s.

[2347] « *Par ailleurs, les fiches S ne se réduisent pas à la seule problématique du contre-terrorisme. Ainsi, au regard de ses missions et des possibilités offertes par le FPR, la DGSI utilise également la mise en surveillance de personnes au sein de ce fichier dans le cadre de ses autres missions : le contre-espionnage, la lutte contre les extrémismes violents, la lutte contre les organisations terroristes autres que sunnites et, de manière plus réduite, la contre-prolifération et la lutte contre la criminalité organisée.* » : Délégation parlementaire au renseignement, Rapport N° 4573/448 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016, *Id.,* p. 59.

[2348] G. KOUBI, « Les fichiers de police au service de la sécurité intérieure », *In* F. Debove et O. Renaudie (Dir.), *Sécurité Intérieure : Les nouveaux défis*, *op. cit.*, p. 237.

question de la coordination et de l'articulation des différents 'fichiers' « pose de délicates questions pratiques et juridiques »[2349].

Néanmoins, la dernière orientation de la politique de sécurité et de défense, face à l'accroissement des risques, crises et menaces, soit la « *possibilité d'agression envers les intérêts d'un État concrétisée par une capacité et une volonté de nuire* »[2350], provoque un durcissement ainsi que le renforcement des armées et de leurs capacités et moyens, notamment techniques et numériques, le renforcement de l'autonomie stratégique, le renforcement des moyens de surveillance et de renseignement ainsi que de coopération entre les services, mais conduit aussi à « *relancer l'Europe de la défense, en rapprochant nos cultures stratégiques, en nourrissant des partenariats pragmatiques avec les États européens qui ont la volonté politique et la capacité militaire d'assumer avec nous leurs responsabilités en opérations, en dégageant les ressources nécessaires au niveau européen, en consolidant nos industries de défense pour qu'elles conservent leur excellence technologique et demeurent compétitives à l'échelle mondiale* »[2351].

Cette politique vise, *in fine*, à promulguer une France forte, à réaffirmer sa souveraineté et son autonomie, souveraineté qui « *relève d'une approche nationale, non partageable où des garanties d'intégrité, de liberté d'emploi ou du maintien de la supériorité opérationnelle prévalent. Les technologies émergentes entrent a priori dans cette posture afin d'en évaluer le potentiel, d'atteindre un niveau de maîtrise suffisant et de décider, en connaissance de cause, de la conduite à tenir* »[2352], tout en exerçant une « souveraineté numérique », centrée sur les « stratégies », « l'autonomie stratégique », les « menaces », les « efforts », la « numérisation » et le « cyber » (cyberespace, cyberdéfense, cybersécurité, etc.) ; termes ayant une récurrence inédite dans l'ensemble des dispositifs juridiques présentant l'orientation de ladite politique.

À ce titre, la stratégie, qui désigne l' « *art, pour un État, de coordonner l'action de ses forces politiques, économiques, sociales et militaires dans le but d'atteindre, par la persuasion ou la force, un objectif déterminé* »[2353], est un des piliers principaux de la nouvelle politique de sécurité et de défense, et ce dans tous les espaces, y compris les « espaces publics mondiaux » (EPM) désignant un « *espace ne ressortissant à aucune souveraineté nationale et qui, dans l'intérêt commun, fait l'objet d'une règlementation internationale ; le cyberespace, l'espace*

[2349] Délégation parlementaire au renseignement, Rapport N° 4573/448 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016, *Id.,* p. 60.
[2350] Ministère des armées, « La Loi de programmation militaire de A à Z », *loc. cit.*
[2351] Revue Stratégique de défense et de sécurité nationale 2017, « Préface du Président de la République », *Ibid.*, p. 7.
[2352] Revue Stratégique de défense et de sécurité nationale 2017, *Id.,* p. 68, point 226.
[2353] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*

extra-atmosphérique, l'espace aérien international et l'espace maritime international sont des espaces publics mondiaux »[2354], et où l'espace numérique en particulier, « désormais considéré comme un champ de confrontation à part entière, fait l'objet d'une compétition stratégique intense »[2355].

De même, « *parce qu'elle conditionne l'exercice de notre souveraineté et de notre liberté d'action, notre autonomie stratégique demeure un objectif prioritaire de notre politique de défense. Dans un système international marqué par l'instabilité et l'incertitude, la France doit conserver sa capacité à décider et à agir seule pour défendre ses intérêts* »[2356] ; sans compter la nécessité de préserver et de protéger les intérêts stratégiques, « *intérêts, souvent communs aux États occidentaux, participant du maintien de la paix sur le continent européen et dans les zones qui le bordent à l'est et au sud, et de la stabilité et de la sécurité des espaces essentiels à l'activité économique du pays et à la liberté des échanges et des communications* »[2357].

La numérisation, qui se réfère à l' « *adaptation des possibilités techniques offertes par les Nouvelles technologies de l'information et de la communication et leur mise en œuvre coordonnée en vue d'optimiser l'efficacité globale des forces, en particulier dans les domaines de la prise de décision, de l'exécution de la manœuvre et du traitement de l'information* », participe pleinement à cette structure, dans la mesure où la « *numérisation massive que connaissent nos sociétés depuis une dizaine d'années et l'interconnexion globale des systèmes d'information et de communication suscitent l'émergence de nouvelles menaces comme de nouvelles opportunités. Elles mettent à portée de tous de puissants outils d'expression, d'influence, de propagande et de renseignement, d'immenses volumes de données mais aussi de redoutables vecteurs d'attaque. Elles favorisent la montée en puissance de nouveaux acteurs privés, qui s'imposent sur la scène internationale comme un défi à la souveraineté des États mais aussi comme des partenaires parfois essentiels. Elles transforment de fait les rapports de pouvoir entre acteurs étatiques, non étatiques et le secteur privé* »[2358].

De plus, « s'imposant désormais comme des acteurs majeurs de l'environnement géopolitique », les entreprises privées « nées de la révolution numérique », comme Google ou Facebook, collectent et contrôlent, « grâce au nombre considérable d'usagers qu'elles drainent », d'immenses volumes de données et assurent des services essentiels : « *la détention, le croisement et l'exploitation de ces informations constituent un avantage majeur dans le*

[2354] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*
[2355] Revue Stratégique de défense et de sécurité nationale 2017, *Id.,* p. 46, point 133.
[2356] Revue Stratégique de défense et de sécurité nationale 2017, *Ibid.,* p. 56, point 170.
[2357] Ministère des armées, « La Loi de programmation militaire de A à Z », *Ibid.*
[2358] Revue Stratégique de défense et de sécurité nationale 2017, *Id.,* p. 46, point 133.

domaine économique, mais aussi stratégique (connaissance, anticipation, etc.), [et] *sont au cœur des enjeux de la lutte antiterroriste comme de cybersécurité, de protection des données personnelles, et pour certaines de détection, d'attribution et de réponse aux cyberattaques* »[2359], la cybersécurité désignant l' « *état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace. La cybersécurité est assurée par la cyberprotection ainsi que, dans le cas d'un État, par la cyberdéfense* »[2360] ; celle-ci, transverse aux fonctions stratégiques qu'elle soutient, « *porte en son sein un enjeu de souveraineté nationale* »[2361].

Par ailleurs, l'aptitude à « *connaître, comprendre, caractériser et prévoir est centrale pour permettre à la France d'agir de manière autonome et souveraine, y compris dans les actions menées avec des partenaire et alliés* » : le renseignement, qui en est « l'élément premier », doit être « renforcé », et l'anticipation « à court et moyen terme des risques pesant sur la sécurité nationale comme des ruptures technologiques » justifie le développement par l'État « des capacités autonomes à la hauteur de ses besoins »[2362]. À ce titre, « conserver à la France l'indépendance de ses analyses et de ses positions » exige un « investissement accru » dans le renseignement, « *dans la poursuite des grands programmes techniques lui permettant de rester au meilleur niveau en la matière et dans le développement des capacités d'analyse nécessaires pour exploiter le volume considérable et en croissance rapide des données humaines et techniques recueillies* », caractérisant ainsi le besoin de « maîtrise de l'intelligence artificielle » qui représente également « un enjeu de souveraineté »[2363], ou encore de la mise en œuvre des « drones d'observation et drones armés » qui sont aussi « un enjeu de souveraineté »[2364].

De nombreux efforts sont dès lors prévus et consentis, comme en termes de ressources budgétaires permettant de « conjuguer souveraineté stratégique et souveraineté budgétaire »[2365] ; ressources qui, d'ailleurs, contribueront « *pour partie au projet ARTEMIS qui vise à offrir une capacité souveraine de traitement de données pour ne plus recourir au système américain PALANTIR, fournisseur de la CIA et de la NSA, et qui vient de recruter pour sa*

[2359] Revue Stratégique de défense et de sécurité nationale 2017, *Ibid.,* p. 46, point 134.
[2360] Ministère des armées, « La Loi de programmation militaire de A à Z », *Id.*
[2361] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.1. *Une structuration volontariste de l'action du ministère dans l'espace numérique*
[2362] Revue Stratégique de défense et de sécurité nationale 2017, *Id.,* p. 74, point 255.
[2363] Revue Stratégique de défense et de sécurité nationale 2017, *Ibid.,* p. 74, point 256.
[2364] Rapport d'information N° 559 (2016-2017) Drones d'observation et drones armés : un enjeu de souveraineté, fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, par MM. C. PERRIN, G. ROGER, J.-M. BOCKEL et R. VALL, Sénat, du 23 mai 2017 ; Disponible en ligne : https://www.senat.fr/notice-rapport/2016/r16-559-notice.html
[2365] Loi du 18 décembre 2013 relative à la programmation militaire - Rapport annexé, § 5. *Les ressources financières*

filiale française, l'ancien PDG d'Airbus »[2366]. Ce qui requiert alors le maintien de la vitalité de la BITD devant être « soutenue et entretenue à tous les niveaux (start-up, PME, ETI, grands groupes) », écosystème qui constitue « un enjeu de souveraineté »[2367].

De même, « *la préservation de la capacité de la France à agir de manière souveraine dans le cyberespace repose sur la maîtrise des technologies, des équipements, des services et des données et de leur traitement, tant sur les aspects industriels que règlementaires,* [et] *nécessite notamment de s'appuyer sur une base d'acteurs industriels de confiance, qu'il faut préserver et même développer, capables de produire des briques technologiques de qualité et de concevoir des systèmes complexes, intégrant des briques non nationales avec des partenaires de confiance* »[2368]. Ce qui justifie « *les efforts engagés afin d'améliorer l'homogénéité de nos systèmes de commandement et leur interopérabilité avec les systèmes alliés* » visant, en particulier, à : « *disposer de moyens de commandement interopérables avec les pays de l'Alliance atlantique et avec des partenaires de circonstance ; améliorer l'interconnexion et le partage d'information entre nos propres systèmes afin d'accélérer la boucle décisionnelle ; garantir la fluidité des échanges et conserver la maîtrise de l'information dans un contexte de risque cyber et d'un accroissement du volume de données à traiter, notamment en provenance des nouveaux capteurs* »[2369].

[2366] Rapport N° 1302 fait au nom de la Commission des finances, de l'économie générale et du contrôle budgétaire sur le Projet de loi de finances pour 2019 (n° 1255), par M. J. GIRAUD (Rapporteur Général – Député), Annexe N° 13, « Défense : Préparation de l'avenir », M. F. CORNUT-GENTILLE (Rapporteur spécial - Député), Assemblée nationale, du 11 octobre 2018, § 3. Les équipements dédiés au renseignement, p. 67, où le rapporteur précise « ***Avec ces différents capteurs, il convient de se préoccuper également des capacités de traitement des données***. *Selon le PAP 2019* [Projet annuel de performance], *dans le cadre des études amonts financées par le programme 144, « Dans les domaines du renseignement militaire et de la surveillance, les travaux conduits dans le domaine du renseignement image, des outils de recueil et de gestion des données de renseignement électromagnétique seront poursuivis et donneront lieu au lancement de nouvelles études. Dans les domaines des systèmes d'information et de communications et de la cybersécurité, les principaux engagements portent sur le lancement de la deuxième phase des travaux relatifs à la valorisation et aux traitements de données de masse (ARTEMIS). De nouvelles études seront également lancées sur les communications, les données d'environnement géophysique et les technologies de sécurité des systèmes d'information et de cyberdéfense ». 100 millions d'euros de crédits de paiement et 151 millions d'euros d'autorisations d'engagement sont inscrits pour 2019 au profit des études amont « information et renseignement classique »*. » ; Disponible en ligne : http://www2.assemblee-nationale.fr/documents/notice/15/budget/plf2019/b1302-tIII-a13/(index)/depots

[2367] Revue Stratégique de défense et de sécurité nationale 2017, *Id.,* p. 66, point 218, où il est indiqué que « *Garantir l'approvisionnement et le maintien en condition opérationnelle des équipements des armées, en particulier ceux concourant à la mise en œuvre de la dissuasion nucléaire, conditionne la liberté d'action de la France et, à ce titre, constitue un pilier de son autonomie stratégique. Plus largement, ce moteur industriel et technologique irrigue l'économie et contribue au rayonnement et à l'influence de la France dans le monde. […]* »

[2368] Revue Stratégique de défense et de sécurité nationale 2017, *Ibid.,* p. 67, point 223.

[2369] Revue Stratégique de défense et de sécurité nationale 2017, *Ibidem,* p. 81, point 292 ; *Cf.* p. 320.

En effet, dans un environnement industriel caractérisé par des innovations technologiques rapides et aujourd'hui dominé par des entreprises étrangères, « *le développement de ces technologies s'avère ainsi un enjeu majeur de souveraineté* »[2370], d'autant que « *les États-Unis, la Chine et la Russie ont favorisé l'émergence de géants nationaux de l'Internet dans le cadre de stratégies globales de puissance et de souveraineté. La suprématie des États-Unis dans toutes les dimensions de l'espace numérique (matérielle, technologique, économique, juridique, politique et militaire) offre un contraste saisissant avec la situation des Européens, qui demeurent fortement dépendants de l'extérieur et dont les investissements comme les acteurs peinent à atteindre une taille critique. La Chine investit massivement dans l'Internet du futur, l'innovation et l'e-commerce et le développement d'une « route de la soie numérique ». Ce faisant, elle vise à assurer un contrôle souverain sur la partie de l'espace numérique qu'elle assimile à son territoire national et à étendre son influence au-delà. Imposant la localisation des données relatives à ses citoyens sur son territoire, la Russie investit massivement dans la construction de data centres dans une stratégie de maîtrise des données et de sécurité informationnelle* »[2371], sans compter enfin que « *la fréquence, l'ampleur et la sophistication technologique des agressions augmentent sans cesse dans l'espace numérique, où les États se livrent à des affrontements constants, qui pourraient à l'avenir relever du seuil de l'emploi de la force ou de l'agression armée, avec des conséquences collatérales potentielles pour les acteurs privés* »[2372].

Il s'avère finalement que, comme le souligne la Professeure Koubi, « *diffluant une idée de « péril », parfois imminent, ou de danger, plus ou moins immédiat, le corps de la notion de sécurité accorde une vitalité composite à l'abstraction de « sentiment » afin de justifier la synchronisation des fichiers [...], engendrant progression du contrôle social et fabrication d'une société de surveillance* »[2373].

[2370] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.1.1. *La connaissance et l'anticipation*
[2371] Revue Stratégique de défense et de sécurité nationale 2017, *Id.,* p. 46-47, point 135.
[2372] Revue Stratégique de défense et de sécurité nationale 2017, *Ibid.,* p. 47, point 136.
[2373] G. KOUBI, « Les fichiers de police au service de la sécurité intérieure », *Id.*, p. 239.

B. Une nouvelle conception de l'urgence et de l'exception, ou quand l'exception devient la règle

C'est initialement dans l'ouvrage « La dictature »[2374] que Schmitt évoque la théorie de l'état d'exception, et établit et analyse le lien de proximité inhérent qui existe entre l'état d'exception et la souveraineté alors même que sa définition du souverain, à savoir « celui qui décide de l'état d'exception », a été amplement critiquée. Cela dit, une théorie définie et cohérente de l'état d'exception manque toujours dans le droit public sans pour autant gêner, la doctrine juridique considérant le problème plutôt comme une « *quaestio facti* » que comme un « authentique problème juridique »[2375]. Se situant à la limite entre le fait et le droit, dans la sphère de *necessitas non habet legem*, l'état d'exception semble constituer, selon une opinion répandue et majoritaire, un *« point de déséquilibre entre le droit public et le fait politique, qui – comme la guerre civile, l'insurrection et la résistance – se situe dans une frange ambiguë et incertaine, à l'intersection entre le juridique et le politique* »[2376]. Or, il apparaît à l'heure actuelle urgent de délimiter les frontières de cette notion et d'en tracer les contours notamment à l'ère du numérique et de l'avènement d'une nouvelle conception de souveraineté numérique, enjeu primordial hargneusement poursuivi par la dernière politique publique courante, et où le concept de souveraineté se caractérise « principalement par ses objets et ses moyens d'exercice », surtout dans ce nouvel « espace marchand de l'« économie-monde numérique » »[2377].

Si les mesures exceptionnelles, pré-délictuelles, caractéristiques principales de l'état d'exception, ne résultent que de périodes de crise politique, et si, pour la même raison, elles doivent être abordées sur le terrain politique, et non sur celui juridique ou constitutionnel, alors, paradoxalement, cela aboutit à des mesures légales qui ne peuvent pourtant être justifiées d'un point de vue juridique ; d'où l'impossibilité de définir une forme légale à l'état d'exception alors qu'il prétend en avoir une. Supprimer l'incertitude qui entoure le droit public et le fait politique, d'une part, et l'ordre juridique et la vie, d'autre part, permet de saisir l'enjeu de la différence, « ou de la prétendue différence », entre « le politique et le juridique », d'un côté, et entre « le droit et le vivant », de l'autre[2378]. En outre, ce qui, selon Agamben, complique davantage la

[2374] C. SCHMITT, *La Dictature*, Ed. du Seuil, Coll. L'Ordre Philosophique, Paris, 2000.
[2375] G. AGAMBEN, *État d'exception – Homo Sacer II, 1*, Ed. du Seuil, Coll. L'Ordre Philosophique, t. 1, 2003, p. 9.
[2376] G. AGAMBEN, *État d'exception*, *Id.*, p. 9.
[2377] CERNA, « La souveraineté à l'ère du numérique : Rester maîtres de nos choix et de nos valeurs », *loc. cit.*, p. 9.
[2378] G. AGAMBEN, *État d'exception*, *Id.*, p. 10 où l'auteur indique à ce titre « *Peut-être seulement alors sera-t-il possible de répondre à la question qui ne cesse de hanter l'histoire de la politique occidentale : que signifie agir politiquement ?* »

compréhension et la définition de la notion d'état d'exception, c'est la confusion qui existe entre celle-ci et les guerres, voire les révolutions et conflits extrêmes, comme la guerre civile, l'insurrection ou la résistance. Pendant ces évènements, la situation étant contraire à l'état normal, la seule solution est alors l'état d'exception qui constitue la réponse immédiate de l'État aux conflits les plus graves : « *prenons le cas de l'État nazi. Dès que Hitler eut pris le pouvoir (ou, comme on devrait plutôt le dire plus exactement, dès que le pouvoir lui fut livré), il promulgua le 28 février 1933 un « Décret pour la protection du peuple et de l'État », qui suspendait les articles de la constitution de Weimar relatifs aux libertés personnelles. Le décret ne fut jamais révoqué, si bien que tout le Troisième Reich peut être considéré, du point de vue juridique, comme un état d'exception qui a duré douze ans* »[2379].

De nos jours, et comme ont pu l'annoncer à de nombreuses reprises les différents Présidents de la République française depuis 2008[2380], les sociétés, notamment européennes, sont continuellement exposées à des menaces, des risques et des crises de toute forme et nature (terrorisme, cybercriminalité, etc.) nécessitant l'adoption de plusieurs mesures et dispositions afin d'assurer la sécurité nationale et protéger la population, en adoptant notamment des postures et stratégies de défense renforcées qui, comme il a été vu, suggèrent la « guerre de tous contre tous ». Dans cette perspective, c'est une sorte de concrétisation de la forme de totalitarisme moderne qu'Agamben définit comme « *l'instauration, par l'état d'exception, d'une guerre civile légale, qui permet l'élimination physique non seulement des adversaires politiques, mais de catégories entières de citoyens qui, pour une raison ou une autre, semblent non intégrables dans le système politique* »[2381], et qui instille, selon l'auteur, la volonté chez les États contemporains d'instaurer un « état d'urgence permanent » ; titre d'ailleurs d'un article juridique de 2017 où le Professeur indique, en prolégomènes, qu' « *afin, selon le législateur, de permettre une sortie maîtrisée de l'état d'urgence, la loi du 30 octobre 2017 reprend dans le code de la sécurité intérieure plusieurs pouvoirs inspirés de ce régime. Accusée d'organiser une sortie en trompe-l'œil, la nouvelle loi ne constitue pas un décalque de celle de 1955. Elle s'inscrit néanmoins dans la démarche préventive qui anime cette dernière depuis sa révision en 2015 et qui caractérise plus largement notre droit de la sécurité publique depuis trois ans* »[2382].

Le concept d'état d'exception est étranger à la doctrine française qui préfère parler d'état d'urgence ou d'état de siège, ce dernier remontant au décret napoléonien du 24 décembre 1811

[2379] G. AGAMBEN, *État d'exception*, *Id.*, p. 11.
[2380] *Cf.* p. 511 et 525.
[2381] G. AGAMBEN, *État d'exception*, *Ibid.*, p. 11-12.
[2382] O. LE BOT, « Un état d'urgence permanent ? (Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme) », RFDA 2017, p. 1115.

« *qui prévoyait la possibilité d'un état de siège que l'Empereur pouvait déclarer, indépendamment de la situation effective d'une ville assiégée ou directement menacée par les forces de l'ennemi* »[2383]. Cela dit, l'institution de l'état de siège se trouve originellement dans le décret du 8 juillet 1791 de l'Assemblée constituante française qui distinguait entre état de paix, état de guerre et état de siège, en limitant leur application « *aux places fortes et aux ports militaires ; mais par la loi du 19 fructidor an V, le Directoire assimila aux places fortes les communes de l'intérieur et, par la loi du 18 fructidor de la même année, s'attribua le droit de mettre une ville en état de siège. L'histoire ultérieure de l'état de siège est celle de sa progressive émancipation par rapport à la situation de guerre à laquelle il était lié à l'origine, pour être ensuite utilisé comme mesure extraordinaire de police en cas de désordres et de séditions internes ; ainsi, d'effectif ou militaire, devient-il fictif ou politique* »[2384]. L'état d'exception n'est donc pas un droit spécial à l'image du droit de guerre mais vu qu'il sert à suspendre l'ordre juridique en soi, il finit par en définir le seuil ou le concept limite.

Une des illustrations parfaites de l'état d'exception, entendue comme structure originale qui mène à inclure le vivant dans le droit à travers sa propre suspension, est le *military order* que le Président des États-Unis a décrété le 13 novembre 2001 à la suite des attentats de New-York, dans le cadre duquel une détention illimitée pour suspicion d'implication dans des activités terroristes a été instaurée pour les citoyens non-américains ; et si ceux-ci font l'objet d'un contrôle judiciaire, c'est dans le cadre de juridictions militaires spécialisées, les *military commissions* de Guantanamo[2385]. Déjà, le *USA Patriot Act* du 26 octobre 2001 autorisait la détention de tout étranger (*alien*) « suspecté » de mettre en danger la sécurité nationale, mais l'étranger, en suivant, devait être soit expulsé, soit accusé d'un crime ou d'une violation de la loi ; or, la nouveauté du *military order*, édicté la même année, est celle d'annuler radicalement tout statut juridique de la personne, créant *de facto* un « être juridiquement innommable et inclassable »[2386].

[2383] G. AGAMBEN, *État d'exception*, *Id.*, p. 15.
[2384] G. AGAMBEN, *État d'exception, Ibid.*, p. 15.
[2385] Human Rights Watch, "The Guantanamo Trials", du 9 août 2018: "*The military commissions at Guantanamo Bay were created by the Bush administration in 2001 to try foreign terrorism suspects in proceedings that lack the due process protections of US federal courts. […]. In the year* [2009], *Congress passed legislation that improved the military commissions by, among other changes, prohibiting the introduction of some evidence obtained through the use of torture or cruel and unusual punishment, and tightening the use of hearsay evidence. But even with these improvements, some evidence derived from torture and other forms of coercion remain admissible and, the military commissions are still in other respects substandard proceedings lacking independence, fairness, and time-tested procedures of US federal courts*.": https://www.hrw.org/guantanamo-trials
[2386] The USA PATRIOT Act - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism - of 2001, Public Law 107-56 – Oct. 26, 2001:

En France, depuis les évènements ayant frappé l'Europe en général et l'Hexagone en particulier, de nombreuses dispositions visant à protéger les citoyens en renforçant la sécurité et les mesures de sécurité, et à lutter contre le terrorisme et les formes graves de criminalité ont été adoptées. À la suite des attentats de 2015, l'état d'urgence a été décrété le 13-14 novembre 2015, prolongé six fois par le Parlement, et prenant fin le 1er novembre 2017 alors qu'est entrée en vigueur la loi du 30 octobre 2017[2387] précitée renforçant la sécurité intérieure et la lutte contre le terrorisme[2388]. C'est un dispositif exceptionnel accentuant les pouvoirs des autorités et restreignant certaines libertés publiques ou individuelles, défini par la loi de 1955 modifiée comme une mesure exceptionnelle, « déclaré par décret en Conseil des ministres, sur tout ou partie du territoire métropolitain, des départements d'outre-mer, des collectivités d'outre-mer régies par l'article 74 de la Constitution et en Nouvelle-Calédonie, soit en cas de péril imminent résultant d'atteintes graves à l'ordre public, soit en cas d'événements présentant, par leur nature et leur gravité, le caractère de calamité publique »[2389]. Dès lors, il est utile de s'interroger sur le fait que « *si le propre de l'état d'exception est une suspension (totale ou partielle) du système juridique, comment une telle suspension peut-elle être encore comprise dans l'ordre légal ? comment une anomie peut-elle être inscrite dans le système juridique ? si à l'inverse l'état d'exception n'est qu'une situation de fait, […], comment est-il possible que le système juridique contienne une lacune précisément pour ce qui concerne une situation cruciale ?* »[2390]. En réalité, précise Agamben, « *l'état d'exception n'est ni extérieur ni intérieur à l'ordre juridique et le problème de sa définition concerne un seuil ou une zone d'indistinction, où intérieur et extérieur ne s'excluent pas, mais s'indéterminent* »[2391].

Pour beaucoup, l'état d'exception est fondé sur le concept de nécessité, terme récurrent dans les dernières dispositions juridiques relatives à la politique de sécurité et de défense susvisée, trouvant sa légitimité et sa raison d'être dans la théorie du *status necessitatis*[2392]. En effet, le principe de *necessitas non habet legem* a initialement trouvé sa formulation dans le *Decretum* de Gratien qui semblait attribuer « à la nécessité le pouvoir de rendre licite l'illicite » mais où, en réalité, « plutôt que rendre licite l'illicite, la nécessité agissait comme justification d'une

https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf ; https://www.justice.gov/archive/ll/highlights.htm

[2387] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (1), JORF n° 0255 du 31 octobre 2017, Texte n° 1.

[2388] Vie-Publique.fr, « État d'urgence et autres régimes d'exception », du 10/11/2018 : https://www.vie-publique.fr/actualite/faq-citoyens/etat-urgence-regime-exception/

[2389] Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence (Dernière modification : 30 juin 2018), Art. 1 et 2.

[2390] G. AGAMBEN, *État d'exception*, *Id.*, p. 42-43.

[2391] G. AGAMBEN, *État d'exception*, *Id.*, p. 43.

[2392] G. AGAMBEN, *État d'exception*, *Ibid.*, p. 44.

transgression dans un cas spécifique par une exception » ; une vision également adoptée par Thomas d'Aquin dans son analyse sur ce principe et le pouvoir reconnu au Prince de dispenser de la loi, un pouvoir justifié selon lui car « la nécessité n'est pas soumise à la loi »[2393].

Toutefois, souligne Agamben, « *la théorie de la nécessité n'est ici rien d'autre qu'une théorie de l'exception (dispensatio), en vertu de laquelle un cas singulier est soustrait à l'obligation de l'observation de la loi. La nécessité n'est pas source de loi et ne suspend pas non plus au sens propre la loi : elle se limite à soustraire un cas singulier à l'application littérale de la norme. […]. C'est seulement avec les modernes que l'état de nécessité tend à être inclus dans l'ordre juridique et à se présenter comme un véritable « état » de la loi. Le principe selon lequel la nécessité définit une situation singulière où la loi perd sa vis obligandi se renverse en celui selon lequel la nécessité constitue pour ainsi dire, le fondement ultime et la source même de la loi* »[2394]. Or, la nécessité est un concept entièrement subjectif, relatif à l'objectif poursuivi par le sujet en cause et ne saurait résoudre toutes les problématiques entourant l'état d'exception, en raison même du fait que « *non seulement la nécessité se réduit en dernière instance à une décision, mais ce sur quoi elle décide est, en réalité, un indécidable de fait et de droit* »[2395].

Schmitt, dans ses ouvrages « La dictature » et la « Théologie politique »[2396], tente de construire une théorie de l'état d'exception, théorie toujours d'actualité ; son but étant de l'inscrire dans un contexte juridique. L'état d'exception, puisqu'il met en œuvre une « suspension de l'ordre juridique tout entier », écrit-il, semble donc se « soustraire à toute considération de droit »[2397]. Mais le but de Schmitt est de préciser la relation qui existe entre l'état d'exception et l'ordre juridique, indiquant alors que « la dictature, qu'elle soit de commissaire ou souveraine, implique la référence à un contexte juridique ; l'état d'exception est toujours quelque chose de différent de l'anarchie et du chaos, et, au sens juridique, il existe encore en lui un ordre, même si ce n'est pas un ordre juridique »[2398]. C'est tenter d'appréhender la notion de manière apophatique, en ce sens qu'elle correspond toujours à une suspension de l'ordre juridique même, tout en ayant un contexte juridique. Pour Schmitt, l'état d'exception introduit une « zone d'anomie » dans le droit qui peut être décidée par un souverain qui garantit, finalement, l'ancrage de cet état d'exception dans l'ordre juridique. Dès lors, la théorie de l'état d'exception se présente comme une doctrine de la souveraineté où le « *souverain se trouve en dehors de*

[2393] G. AGAMBEN, *État d'exception*, *Ibid.*, p. 44-45.
[2394] G. AGAMBEN, *État d'exception*, *Ibidem*, p. 45 et 47.
[2395] G. AGAMBEN, *État d'exception*, *Ibidem*, p. 53.
[2396] C. SCHMITT, *Théologie politique*, Ed. Gallimard, Coll. Bibliothèque des Sciences humaines, 1988.
[2397] G. AGAMBEN, *État d'exception*, *Id.*, p. 57.
[2398] G. AGAMBEN, *État d'exception*, *Id.*, p. 57-58.

l'ordre juridique normalement valide et cependant lui appartient, parce qu'il est responsable de la décision de savoir si la constitution peut être suspendue in toto »[2399].

J. Derrida a tenu, en 1989, une conférence à New-York intitulée « Force de loi : le fondement mystique de l'autorité »[2400], qui correspondait en réalité à une lecture de l'essai de W. Benjamin « Critique de la violence »[2401], et qui a seulement suscité des débats sans que des discussions concrètes sur la conférence et son thème n'aboutissent. Il est pertinent de s'intéresser à la notion de « force de loi », qui remonte à la tradition du droit romain et médiéval portant le sens, de façon générale, « d'efficacité, de capacité à obliger »[2402]. L'article 6 de la Constitution de 1791 précisait que « force de loi » désigne le caractère intangible de la loi, que même le souverain ne saurait abroger ou modifier[2403]. Cependant, que ce soit dans la doctrine classique ou la doctrine moderne, cette force de loi se réfère aux décrets ayant force de loi, et non plus à la loi elle-même, que le pouvoir exécutif est autorisé à promulguer dans certains cas, mais surtout, dans celui de l'état d'exception - l'état d'urgence.

Une illustration de ce procédé se retrouve dans les décrets, ordonnances ou mesures portant sur le renseignement et pris en application du Livre blanc qui, pour des raisons de secret-défense, ne font pas l'objet de publication officielle complète et ne constituent pas formellement une loi mais ont toutefois force de loi[2404], sans oublier les rapports d'information précités. Une confusion de la sorte entre les actes du pouvoir exécutif et ceux du pouvoir législatif est l'un des caractères essentiels de l'état d'exception, « le cas limite en est le régime nazi où, comme

---

[2399] G. AGAMBEN, *État d'exception*, *Id.*, p. 61, l'auteur précise à ce titre que la théorie de la souveraineté dans la *Théologie politique* de Schmitt *« représente une tentative d'ancrer sans réserve l'état d'exception dans l'ordre juridique ; mais cette tentative n'eut pas été possible si l'état d'exception n'avait pas été articulé précédemment dans la terminologie et dans la conceptualité de la dictature et, pour ainsi dire, « juridicisé » par la référence à la magistrature romaine, puis grâce à la distinction entre normes du droit et normes de réalisation* » ; finalement, indique Agamben, « *la doctrine schmittienne de l'état d'exception procède en établissant, dans le corps du droit, une série de césures et d'oppositions dont les termes sont irréductibles l'une à l'autre, mais qui, par leur articulation, permettent à la machine juridique de fonctionner* » (p. 62-63).

[2400] J. DERRIDA, *Force de loi : le "Fondement mystique de l'autorité",* Ed. Galilée, Coll. La philosophie en effet, Paris, 1994.

[2401] W. BENJAMIN, *Critique de la violence et autres essais*, Ed. Payot & Rivages, Coll. Petite Biblio Payot, Paris, 2012.

[2402] G. AGAMBEN, *État d'exception, Id.*, p. 66.

[2403] Constitution de 1791, Titre III, Chapitre III – Section III, « *Article 6. - Les décrets sanctionnés par le roi, et ceux qui lui auront été présentés par trois législatures consécutives, ont force de loi, et portent le nom et l'intitulé de lois.* » ; Disponible en ligne : https://www.conseil-constitutionnel.fr/les-constitutions-dans-l-histoire/constitution-de-1791

[2404] Par ex., Décret n° 2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme, JORF n° 0139 du 15 juin 2017, texte n° 1 ; Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, JORF n° 0225 du 29 septembre 2015, p. 17344, texte n° 1 ; ou même au niveau du Canada : Décret n° 14 sur les fichiers de renseignements personnels inconsultables (SCRS), DORS/92-688 : https://laws-lois.justice.gc.ca/fra/reglements/DORS-92-688/page-1.html

Eichmann ne se lassait pas de le répéter, « les paroles du Führer ont force de loi » »[2405]. Cela dit, l'apport spécifique de l'état d'exception est particulièrement l'isolement de la « force de loi » par rapport à la loi[2406] : « *dans le cas d'urgence, donc, la « force de loi » fluctue comme un élément indéterminé qui peut être revendiqué tant par l'autorité étatique (agissant comme dictature de commissaire) que par une organisation révolutionnaire (agissant comme dictature souveraine). L'état d'exception est un espace anomique où l'enjeu est une force de loi sans loi (que l'on devrait par conséquent écrire force-de-l~~oi~~). Une telle « force-de-l~~oi~~ », où la puissance et l'acte sont radicalement séparés, est certainement quelque chose comme un élément mystique – ou, plutôt, une fictio par laquelle le droit cherche à s'attribuer son anomie même* »[2407].

Dans les démocraties modernes et postmodernes, la création de nouvelles lois, dispositions et mesures exceptionnelles, au nom de la sécurité, par décrets gouvernementaux ensuite ratifiés par le Parlement, devient une pratique courante s'assimilant dans ce contexte à une sorte d'état d'urgence permanent, et évoquant « *l'un des paradigmes essentiels* [de l'état d'exception] *par lesquels, de parlementaire, la démocratie devient gouvernementale* »[2408] et dans laquelle les « régimes juridiques d'exception » sont qualifiés de « légalité de crise »[2409]. Il semble alors que, pour appliquer une norme, il faut, en dernière analyse, suspendre son application, produire une exception, mais, « *dans tous les cas, l'état d'exception marque un seuil où logique et praxis s'indéterminent et où une pure violence sans logos prétend réaliser un énoncé sans aucune référence réelle* »[2410].

Pendant longtemps, un débat opposa les philosophes Benjamin et Schmitt sur la théorie de l'état d'exception, le but du premier étant de garantir « *la possibilité d'une violence absolument « en dehors » et « au-delà » du droit, qui comme telle pourrait briser la dialectique entre violence qui fonde le droit et violence qui le conserve* »[2411]. Un des documents les plus décisifs de leurs débats fut la 8ème thèse sur le concept d'histoire rédigé par Benjamin, dans lequel il affirme que « *la tradition des opprimés nous enseigne que l' "état d'exception" dans lequel nous vivons est*

[2405] G. AGAMBEN, *État d'exception*, *Id.*, p. 67.
[2406] G. AGAMBEN, *État d'exception*, *Id.*, p. 67 où l'auteur explique que l'apport spécifique de l'état d'exception c'est qu'il « *définit un « état de loi » dans lequel, d'une part, la norme est en vigueur, mais ne s'applique pas (n'a pas de « force »), et où, de l'autre, des actes qui n'ont pas valeur de loi en acquièrent la « force »* ».
[2407] G. AGAMBEN, *État d'exception*, *Ibid.*, p. 67-68.
[2408] G. AGAMBEN, *État d'exception*, *Ibidem*, p. 33.
[2409] Vie-Publique.fr, « État d'urgence et autres régimes d'exception », du 10/11/2018, *Id.*
[2410] G. AGAMBEN, *État d'exception*, *Id.*, p. 71.
[2411] W. BENJAMIN, *Critique de la violence et autres essais*, *Id.,* p. 68 à 70, et l'auteur indique en amont « *[…]. Resterait toujours ouverte la question de savoir si la violence en général, en tant que principe, est elle-même morale en tant que moyen visant des fins justes. Cette question a besoin pour être résolue d'une critique plus affinée, d'une distinction dans la sphère des moyens eux-mêmes, sans considération des fins qu'ils servent.* », p. 56 ; et, G. AGAMBEN, *État d'exception*, *Id.*, p. 91.

la règle. Nous devons parvenir à une conception de l'histoire qui corresponde à cette situation. Alors nous aurons devant les yeux notre tâche, qui est de faire advenir l'état d'exception effectif (wirklich) ; cela renforcera notre position dans la lutte contre le fascisme »[2412]. Si l'état d'exception est devenu la norme, cela va à l'encontre de la théorie élaborée par Schmitt[2413], alors même que la thèse de Benjamin paraît, de plus en plus, se justifier. Ce dernier propose une distinction entre état d'exception fictif et effectif, ce que réfutait fortement Schmitt qui critiquait l'idée libérale d'un État de droit ; mais si l'état d'exception effectif s'installe, aucune distinction avec la règle de droit ne pourrait s'opérer, selon la thèse de Benjamin : ici, il n'existe plus de fiction entre la violence et le droit, il s'agit plutôt d'une « violence sans la moindre apparence juridique »[2414].

Ainsi, la violence semble représenter le déclencheur de l'action politique, notre époque en constitue une illustration parfaite où les nouvelles orientations de la politique de sécurité et de défense sont déterminées compte tenu du fait que « *la France et l'Europe sont directement exposées, désormais, au rapprochement des menaces et des crises de tous ordres : au retour de la guerre aux frontières européennes et aux attaques terroristes s'ajoute une concentration, sans précèdent depuis la fin de la guerre froide, de foyers de tension dans l'espace euro-méditerranéen, de l'Atlantique Nord au Sahel. En outre, la mondialisation des crises, par la contraction de l'espace géopolitique et l'accroissement des interconnexions, expose le continent européen aux conséquences directes des crises, même les plus éloignées. L'ensemble de ces phénomènes est aggravé par des fragilités de toute nature (démographiques, politiques, environnementales, sanitaires)* »[2415] justifiant, par conséquent, la nécessité d'adopter des

---

[2412] G. AGAMBEN, *État d'exception*, *Ibid.*, p. 98.

[2413] Puisque « *dans la perspective schmittienne, le fonctionnement de l'ordre juridique repose en dernière instance sur un dispositif – l'état d'exception – qui a pour but de rendre applicable la norme en en suspendant provisoirement l'efficacité. Quand l'exception devient la règle, la machine ne peut plus fonctionner. En ce sens, l'indécidabilité de la norme et de l'exception énoncée dans la huitième thèse met en échec la théorie schmittienne.* » : G. AGAMBEN, *État d'exception*, *Ibid.*, p. 99.

[2414] En effet, Schmitt « *appelle « fictif » un état d'exception que l'on prétend réglementer par la loi, afin de garantir dans une certaine mesure les droits et les libertés individuelles.* [… Mais] *une fois exclue toute possibilité d'un état d'exception fictif, dans lequel exception et cas normal sont distincts dans le temps et dans le lieu, effectif est maintenant l'état d'exception « où nous vivons » et qui est absolument indécidable par rapport à la règle. Toute fiction d'un lien entre violence et droit a ici disparu : il n'y a qu'une zone d'anomie où agit une violence sans la moindre apparence juridique. La tentative du pouvoir d'État de s'annexer l'anomie par l'état d'exception est démasquée par Benjamin pour ce qu'elle est : une fictio juris par excellence qui prétend maintenir le droit dans sa suspension même comme force-de-~~loi~~.* » : G. AGAMBEN, *État d'exception*, *Ibidem*, p. 100-101.

[2415] Revue Stratégique de défense et de sécurité nationale 2017, *loc. cit.,* « Conclusion » p. 67, où les rédacteurs indiquent par ailleurs : « *Les évènements survenus depuis le Livre blanc de 2013, dont plusieurs ont frappé le territoire de la France et sa population, ont confirmé la dégradation durable de l'environnement international. À la persistance d'une menace terroriste jihadiste s'ajoutent les incertitudes liées au retour des politiques de puissance et de la compétition militaire, par un nombre croissant d'États, susceptibles de mettre en cause nos intérêts de sécurité. L'émergence d'un monde multipolaire s'accompagne ainsi de rivalités accrues entre États*

mesures pour assurer la protection de la population et la sécurité nationale, et donc la souveraineté de l'État.

« Pour des raisons de sécurité » est une formule qui fonctionne, depuis un moment, comme argument d'autorité permettant non seulement de justifier une action, mais aussi d'imposer des mesures dans le quotidien qui, normalement, ne seraient pas acceptées, la notion de sécurité semblant avoir supplanté toute autre notion politique ou juridique. Là où les procédures d'exception des siècles derniers visaient une menace, immédiate et concrète, qui devait être éliminée, la suspension du droit paraissant alors nécessaire, les « raisons de sécurité » invoquées désormais constituent, plutôt, une technique, voire un paradigme, des gouvernements contemporains.

C'est la raison pour laquelle Foucault conseille de se pencher sur les études de Quesnay, de Graunt ou encore des physiocrates afin de comprendre la réalité et l'étendue du concept de sécurité moderne, en ce sens que la population n'est pas une « *espèce de donnée primitive, de matière sur laquelle va s'exercer l'action du souverain* » mais « *c'est une donnée qui dépend de toute une série de variables qui font donc qu'elle ne peut pas être transparente à l'action du souverain, ou encore que le rapport entre la population et le souverain ne peut pas être simplement de l'ordre de l'obéissance ou du refus d'obéissance, de l'obéissance ou de la révolte. […]. La population apparaît donc là, dans cette espèce d'épaisseur par rapport au volontarisme légaliste du souverain, comme un phénomène de nature. Un phénomène de nature que l'on ne peut pas changer par décret, ce qui ne veut pas dire, pourtant, que la population soit une nature inaccessible et qui ne soit pas pénétrable, au contraire. Et c'est là où l'analyse des physiocrates et des économistes devient intéressante, c'est que cette naturalité que l'on repère dans le fait de la population est perpétuellement accessible à des agents et à des techniques de transformation, à condition que ces agents et ces techniques de transformation soient à la fois éclairés, réfléchis, analytiques, calculés, calculateurs* »[2416], permettant de « gouverner » la population.

En effet, précise Foucault, « *c'est un jeu incessant entre les techniques de pouvoir et leur objet qui a petit à petit découpé dans le réel et comme champ de réalité la population et ses*

pour le contrôle d'espaces communs ou partagés, et d'évolution des formes d'affrontement vers des logiques d'intimidation ou des modes d'action ambigus, qui accroissent les risques d'incident ou d'escalade. L'incertitude générée par ces évolutions est d'autant plus forte qu'elle se double d'une contestation directe des normes et des institutions internationales censées encadrer le recours à la force, et d'une poursuite préoccupante des logiques de prolifération […]. »

[2416] M. FOUCAULT, *Sécurité, Territoire, Population*, Cours au collège de France 1977-1978, Coll. Hautes Études, EHESS, Ed. Gallimard – Seuil, 2004, Leçon du 25 janvier 1978 - p. 73.

phénomènes spécifiques. Et c'est à partir de la constitution de la population comme corrélatif des techniques de pouvoir que l'on a pu voir s'ouvrir toute une série de domaines d'objet pour des savoirs possibles. […]. De là cette conséquence : c'est que la thématique de l'homme, à travers les "sciences humaines" qui l'analysent comme être vivant, individu travaillant, sujet parlant, il faut la comprendre à partir de l'émergence de la population comme corrélatif de pouvoir et comme objet de savoir » nécessitant un gouvernement, « l'art de gouverner »[2417].

Dès lors, « gouverner » reprend son sens étymologique puisqu'il s'entend, dans ce cadre, comme le bon pilote, celui qui tient le gouvernail, qui ne peut éviter la tempête, mais qui, à sa survenance, doit être capable de diriger le bateau ; une « science de la gouverne » émerge donc[2418]. C'est dans ce sens qu'il faut comprendre l'idée des physiocrates qui appelle la formule « laisser faire, laisser passer », et qui, selon Agamben, désigne *« le paradigme d'un gouvernement, qui situe la sécurité, non pas dans la prévention des troubles et des désastres, mais dans la capacité à les canaliser dans une direction utile* » ; les dernières lois de programmation militaire en sont un exemple, notamment, selon l'auteur, celle de 2013 et son article 20 qui autorise une surveillance généralisée des données numériques, « *au point que l'on parle de « Patriot Act à la française ». Érigé en priorité absolue, l'impératif de sécurité change souvent de prétexte (subversion politique, « terrorisme ») mais conserve sa visée : gouverner les populations* »[2419]. Ce bouleversement appelle alors à une redéfinition de la relation hiérarchique qui existe entre cause et effet. Puisqu'il apparaît vain de tenter de régler les causes, le gouvernement se retourne plutôt vers une gestion des effets, ou une gestion des crises : c'est ce qui régit les sociétés contemporaines, mais permet également une meilleure compréhension de la convergence mystérieuse entre un libéralisme de plus en plus croissant en économie et un contrôle « sécuritaire » sans précèdent, qui de nos jours requièrent principalement des dispositifs et des pratiques technologiques et computationnels.

La loi de 2017[2420] précitée intègre la dimension numérique des dispositifs ayant vocation à permettre une prévention plus efficace du terrorisme et instaure plusieurs mesures administratives applicables, comme le périmètre de protection, l'élargissement des contrôles frontaliers, ou les dispositions en matière de recueil des données PNR et de renseignement, permettant de lutter plus activement. La sortie de l'état d'urgence a ainsi « conduit le législateur

[2417] M. FOUCAULT, *Sécurité, Territoire, Population*, *Id.*, Leçon du 25 janvier 1978 - p. 80-81
[2418] *Cf.* p. 558.
[2419] G. AGAMBEN, « Comment l'obsession sécuritaire fait muter la démocratie », Le monde diplomatique, janvier 2014, p. 22-23.
[2420] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

à pérenniser certaines dispositions faisant appel à des technologies numériques »[2421] afin d'assurer son objet, à savoir renforcer la sécurité et la lutte contre le terrorisme.

La loi crée ainsi, entre autres, les articles L. 229-1 à L. 229-5 du Code de la sécurité intérieure, modifiés pour certains par la loi du 23 mars 2019[2422], qui autorisent désormais de procéder à des « visites domiciliaires et saisies », y compris la « saisie des documents et données qui s'y trouvent »[2423], dans le but de « prévenir la commission d'actes de terrorisme » lorsqu'il existe des « raisons sérieuses de penser qu'un lieu est fréquenté par une personne dont le comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics »[2424] et/ou qu'elle est en relation habituelle avec des personnes physiques ou morales incitant, facilitant ou participant à des actes terroristes. Le terme de « perquisition » n'est pas repris ici mais est sous-entendu, puisque ces visites domiciliaires autorisent une introduction dans le domicile d'une personne sans obtenir son consentement[2425]. Se voulant un régime complémentaire aux perquisitions en matière pénale, les forces de l'ordre ont dans ce cadre « *vocation à y avoir recours à titre subsidiaire, lorsqu'il n'y a aucune suspicion d'infraction pénale, mais qu'une menace pour l'ordre et la sécurité publics est caractérisée* »[2426].

Par ailleurs, la loi met en place un régime de mesures individuelles de contrôle administratif et de surveillance dont le « placement sous surveillance électronique mobile »[2427], une extension des techniques spéciales d'enquête, notamment numériques, (comme l'infiltration, l'enquête sous pseudonyme, la captation de données ou le recours à l'IMSI-catcher) pour la poursuite des infractions relevant d'atteintes aux intérêts fondamentaux de la Nation[2428], ou encore une autorisation d'intercepter et d'exploiter des « *correspondances échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant*

[2421] M. QUÉMÉNER, « Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme », Dalloz IP/IT 2017, p. 657.

[2422] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

[2423] Ainsi l'Art. L 229-5 (Modifié par la loi n° 2019-222 du 23 mars 2019 - Art. 66) du Code de la sécurité dispose que « *I. Aux seules fins de prévenir la commission d'actes de terrorisme, si la visite révèle l'existence de documents ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée, il peut être procédé à leur saisie ainsi qu'à celle des données contenues dans tout système informatique ou équipement terminal présent sur les lieux de la visite soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la visite.* »

[2424] Code de la sécurité intérieure, Art. L 229-1 (Modifié par la loi n° 2019-222 du 23 mars 2019 - Art. 66)

[2425] M. QUÉMÉNER, « Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme », *Id.*, p. 657.

[2426] M. QUÉMÉNER, « Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme », *Ibid.*, p. 657.

[2427] Code de la sécurité intérieure, Art. L 228-3 (Modifié par la loi n° 2019-222 du 23 mars 2019 - Art. 69).

[2428] Code de procédure pénale, Art. 706-73 (Modifié par Modifié par l'Ordonnance n° 2020-1733 du 16 décembre 2020 - art. 11) et 706-73-1 (Modifié par la loi n° 2017-257 du 28 février 2017 - Art. 34 (V) et par l'Ordonnance n°2019-1015 du 2 octobre 2019 - Art. 34).

pas l'intervention d'un opérateur de communications électroniques, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs »[2429], créant finalement deux régimes d'interception distincts[2430]. La loi instaure, de plus, une base légale pour les interceptions de réseaux wifi où les données peuvent être interceptées dans le cadre du recours aux techniques de renseignement, ce qui comprend *ipso facto* l'interception des données émises ou reçues par les objets connectés[2431], sans oublier la possibilité, inscrite dans la loi depuis 2015, d'utiliser des « *dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé* »[2432].

En outre, par le biais de deux lois de 2015, l'une relative au renseignement[2433] l'autre aux mesures de surveillance des communications électroniques internationales[2434], de celle de 2017 en question, et de celle de 2018 relative à la programmation militaire susmentionnée, un régime d'accès administratif aux données de connexions assez étendu est dorénavant mis en œuvre[2435], y compris l'interception des flux de communications étrangères (émises ou reçues) passant par la France, et dans le cadre duquel les informations recueillies peuvent être mises à disposition de tous les services de renseignement concernés pour exploitation[2436].

Il est, par conséquent, possible d'évoquer une « banalisation de l'état d'exception » où face à la menace omniprésente, l'urgence commande l'inscription dans la loi d'un tel pouvoir : « *on*

[2429] Code de la sécurité intérieure, Art. L 852-2 (Créé par la loi n° 2017-1510 du 30 octobre 2017 - Art. 15 (V)) qui précise à son dernier alinéa « *L'autorisation mentionnée au premier alinéa du présent article vaut autorisation de recueil des informations ou documents mentionnés à l'article L. 851-1 associés à l'exécution de l'interception et à son exploitation* »

[2430] M. QUÉMÉNER, « Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme », *Id.*, p. 658 : « *La loi crée deux régimes d'interception, l'un pour les « correspondances échangées au sein d'un réseau privé de communications électroniques hertziennes », prévoyant une autorisation préalable du Premier ministre après avis de la CNCTR, le second pour les communications hertziennes échangées sur un réseau public, non soumis à un régime d'autorisation mais à un contrôle général de la CNCTR.* »

[2431] Code de la sécurité intérieure, Art. L 853-2 (Modifié par la loi n° 2021-998 du 30 juillet 2021 - Art. 11 et 18) « *I. - Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre, et permettant d'accéder à ces mêmes données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques.* »

[2432] Code de la sécurité intérieure, Art. L 853-1 (Modifié par la loi n° 2021-998 du 30 juillet 2021 - Art.18).

[2433] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF n° 0171 du 26 juillet 2015, p. 12735, texte n° 2.

[2434] Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, JORF n° 0278 du 1 décembre 2015, p. 22185, texte n° 1.

[2435] Code de la sécurité intérieure, Art. L 851-1 à L 851-6.

[2436] Code de la sécurité intérieure, Art. L 854-1 et L 854-2 ; et, Délégation parlementaire au renseignement, Rapport N° 4573/448 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016, *Id.,* p. 71-72.

peut voir dans les délits flous, les primes aux « collaborateurs » de la justice et les nombreux fichiers, le cheval de Troie de l'état d'exception dans le droit de punir. […]. Le danger est l'exception institutionnalisée comme l'est l'USA Patriot Act : face au mal radical, nous retrouvons l'état d'exception au sens d'une fusion entre droit et violence, démocratie et absolutisme. Au fond, libérée des contre-pouvoirs libéraux qui neutralisent sa puissance, l'action politique retrouve une souveraineté sans partage. Sous le masque de l'exception resurgit la strate théologique de l'État : le théâtre de la guerre contre le terrorisme devient celui de la lutte du Bien contre le Mal »[2437].

Cette multiplication accrue des dispositifs sécuritaires témoigne ainsi d'un changement dans le concept même de politique, et du renversement du processus de « politisation de la citoyenneté » amorcée en Grèce où l'exercice de la citoyenneté, la « *politeia* », la politique, représentait un critère de l'identité sociale[2438]. Les mesures de sécurité ont joué un rôle non négligeable dans ce processus de « dépolitisation » entraînant une passivité de la citoyenneté, une confusion entre l'action et l'inaction, le public et le privé, là où la politique est censée être l'opposé du privé, ce dernier étant celui qui, en général, recourait à la nécessité. Cependant, l'extension progressive des techniques d'identification à tous les citoyens[2439], jadis réservées aux seuls criminels, engendre un impact inévitable sur leur identité politique, aboutissant conséquemment à ce que l'identité ne représente plus la fonction sociale de la « personne », outil qui permet sa reconnaissance, mais plutôt les données biologiques et/ou biométriques et/ou numériques.

Là où le citoyen grec se définissait par l'opposition entre le privé et le public, la maison (siège de la vie reproductive) et la cité (lieu du politique), le citoyen moderne et postmoderne évolue pour sa part dans une zone d'indifférenciation, de confusion permanente, entre le public et le privé. Cette indifférenciation se matérialise par exemple à travers la vidéosurveillance, surnommée vidéoprotection qui « on le sait est une « technologie de surveillance » », pouvant désormais être mobile et non plus uniquement fixe et où « *la diversité des usages de la vidéoprotection mobile* […] témoigne] *de la nécessité de sécuriser rapidement des pratiques*

[2437] D. SALAS, *La volonté de punir, op. cit.,* p. 172.

[2438] G. AGAMBEN, « Comment l'obsession sécuritaire fait muter la démocratie », *Id.,* p. 23 : « *[…] citons le texte entier tiré de* [l'ouvrage de Meier] *: « il se créa ainsi une identité politique spécifiquement grecque, dans laquelle l'idée que des individus devaient se conduire comme des citoyens trouva une forme institutionnelle, écrit Meier. L'appartenance aux groupes constitués à partir des communautés économiques ou religieuse fut reléguée au second plan. Dans la mesure où les citoyens d'une démocratie se vouaient à la vie politique, ils se comprenaient eux-mêmes comme membres de la polis. Polis et politeia, cité et citoyenneté, se définissaient réciproquement. La citoyenneté devint ainsi une activité et une forme de vie par laquelle la polis, la cité, se constitua en un domaine clairement distinct de l'oikos, la maison. La politique devint un espace public libre, opposé en tant que tel à l'espace privé où régnait la nécessité ».* »

[2439] *Cf.* p. 59 et s.

entourées d'un certain flou juridique »[2440] ; procédé installé et employé dans quasiment la totalité des États contemporains. Ce dispositif de sécurité a ainsi connu le même destin que celui des empreintes : réservé principalement aux prisons, il a été progressivement étendu à tous les lieux publics, leur ôtant donc leur caractère public. L'image du panoptique de Bentham reprise par Foucault ou même de l'individu dangereux de Foucault ne sont pas loin, puisque l'alignement de l'identité sociale à l'identité corporelle s'est amorcé avec le souci d'identifier les criminels récidivistes et les individus dangereux. Dans ce contexte, il n'apparaît donc plus étonnant que la relation entre l'État et ses citoyens s'est profondément modifiée, les dispositifs étatiques ayant induit une relation où l'incertitude, le soupçon, le fichage, la surveillance et le contrôle priment et où les « réponses répressives classiques » sont complétées par des réponses préventives » de sorte qu'on assiste à une « mondialisation de la prévention »[2441].

Dans ses cours au Collège de France, Foucault avait analysé les transformations des modalités de l'exercice du pouvoir et avait élaboré, à partir de 1974, la notion de biopolitique[2442], notion qui fut reprise et développée dans sa dimension radicale dans la mesure où, poussée à l'extrême, la logique profonde de cette notion autorise, comme toute forme d'exercice du pouvoir, des dérives à l'image d'une implication sans limites du biopouvoir dans les moindres aspects de la vie des personnes ; la biopolitique ne pouvant se former qu'à partir de la population, « population qu'un gouvernement doit gérer »[2443]. Il est vrai que « *si la politique porte sur la vie, alors tout peut devenir biopolitique : chaque phénomène social trouve immédiatement sa traduction en phénomène vital* »[2444].

Dans le monde du XXI[e] Siècle, où « *la souveraineté numérique croise dans nos sociétés actuelles la plupart voire toutes les autres souverainetés* »[2445] générant une source importante de conflit public comme privé, l'État n'apparaît plus être celui de la discipline, mais plutôt un État de surveillance et de contrôle. *De facto*, celui-ci ne semble pas vouloir ordonner ou discipliner mais surveiller, prévenir, gérer, punir et contrôler ; ce qui a bien été exprimé par un fonctionnaire de la police italienne indiquant que le gouvernement italien ne demandait plus

---

[2440] O. RENAUDIE, « La vidéoprotection mobile à la recherche de son régime juridique », *In* F. Debove et O. Renaudie (Dir.), *Sécurité Intérieure : Les nouveaux défis*, *op. cit.*, p. 251-252.

[2441] E. LENOIR, « La prévention de la délinquance : un nouvel axe de la sécurité intérieure à la croisée des enjeux de la cohésion sociale », *In* F. Debove et O. Renaudie (Dir.), *Sécurité Intérieure : Les nouveaux défis*, *Id.*, p. 18.

[2442] *Cf.* p. 602.

[2443] M. FOUCAULT, *Naissance de la biopolitique*, Cours au collège de France 1978-1979, Coll. Hautes Études, EHESS, Ed. Gallimard – Seuil, 2004, Leçon du 10 janvier 1979 - p. 24.

[2444] F. KECK, « Les usages du biopolitique », *In* L'Homme, 187-188 | Juillet/Décembre 2008 : Miroirs transatlantiques, Ed. EHESS, p. 295 ; Disponible en ligne : https://journals.openedition.org/lhomme/29305

[2445] CERNA, « La souveraineté à l'ère du numérique : Rester maîtres de nos choix et de nos valeurs », *loc. cit.*, p. 27.

que la police maintienne l'ordre, mais plutôt de gérer le désordre, donnant lieu, lors du sommet du G8 en 2001 à Gênes, à une des manifestations de violence policière des plus sanglantes, « particulièrement graves pour les libertés démocratiques en Europe »[2446]. Quelques mois plus tard, des changements constitutionnels s'annonçaient aux États-Unis, déclenchés par le *USA Patriot Act* et la législation post 11 septembre se référant à « l'État de sécurité », le « *Security state* » ; et, en France, des stratégies de sécurité sont élaborées, des mesures et des techniques de lutte sont renforcées au nom de la sécurité nationale, et des lois pérennisant des dispositions applicables en état urgence - état d'exception sont promulguées.

Lors de la Révolution française alors que les gardes nationales devaient assurer la sécurité du peuple et du commerce[2447], la notion de sécurité renvoyait à l'idée de sûreté qui était liée à celle de police. Néanmoins, une distinction entre sûreté et police persistait, ce qui n'est plus le cas dans les législations actuelles au sein desquelles si une situation menaçant la sécurité survient, l'officier de police agit, non seulement avec une « marge d'appréciation » caractérisant ses actions, mais aussi en tant que souverain moyennant les autonomies décisionnelle et opérationnelle qui lui ont été accordées et renforcées, comme il a pu être observé avec les dernières orientations de la politique de sécurité et de défense adoptées ; cela ne lui permet pas, toutefois, de décider ou même de préparer le jugement qui sera prononcé par le juge au regard du fait que la décision du juge implique les causes, là où le policier gère les effets, donc l'indécidable. Et ce sont précisément ces effets, ou cette situation indécise et incertaine, qui constituent les « raisons de sécurité ».

Ainsi, en se plaçant sous le pavillon de la sécurité, l'État moderne sort de la politique pour rentrer dans un « *no man's land entre droit public et fait politique et entre l'ordre juridique et*

[2446] C. HEIMBER, « Gênes, Italie, G8. Résurgences des années noires », Mediapart, Blog : Chroniques pour mémoires, Genève, août 2001 : « *Les faits sanglants de Gênes, en juillet 2001, ont été particulièrement graves pour les libertés démocratiques en Europe. Le G8, le sommet des maîtres du monde, s'est déroulé en dépit de toutes les protestations populaires. Mais il n'a bien entendu abouti à aucun résultat concret pour la solidarité envers les plus démunis. Ce qui n'a fait que confirmer l'immense mépris des dominants à l'égard des besoins de l'humanité. En revanche, ce sommet de la honte a donné lieu à une explosion inouïe de la violence d'État qui a pris des proportions très inquiétantes, jusqu'à tuer un jeune manifestant. À Gênes, en effet, tout a été sciemment organisé pour criminaliser, et décourager à l'avenir, la moindre volonté de manifester contre les symboles du tout-libéral planétaire. Le spectacle de la violence, en fin de compte, a surtout permis au G8 de détourner l'attention et de ne pas trop donner à voir l'inanité de sa politique et de ses non-décisions. […]. Un jeune manifestant a donc été assassiné par un non moins jeune carabinier. De Carlo Giuliani, tout a été dit dans la presse : punk, toxicomane, repris de justice, zonard, etc. Mais il n'était rien de tout cela. Il n'était qu'un jeune étudiant génois, d'origine romaine, objecteur et sympathisant zapatiste, sans doute révolté par l'arrogance des autorités et l'incroyable militarisation du G8.* » : https://blogs.mediapart.fr/heimbergch/blog/200718/genes-italie-g8-en-2001-resurgences-des-annees-noires-pour-carlo-giuliani

[2447] Par ex. : L'histoire de France, « La Révolution française » : http://www.histoire-france.net/epoque/revolution-francaise

la vie »[2448] où la confusion règne « dès lors que l'état d'exception est devenu la règle »[2449], et où il apparaît de plus en plus difficile d'allier sécurité et liberté, mais beaucoup plus facile de combiner sécurité et défense : « *conformément à une tendance en acte dans toutes les démocraties occidentales, la déclaration de l'état d'exception est progressivement remplacée par une généralisation sans précédent du paradigme de la sécurité comme technique normale de gouvernement* »[2450].

D'ailleurs, déplore Agamben, « l'état d'exception a même atteint aujourd'hui son plus large déploiement planétaire. L'aspect normatif du droit peut être ainsi impunément oblitéré et contredit par une violence gouvernementale qui, en ignorant à l'extérieur le droit international et en produisant à l'intérieur un état d'exception permanent, prétend cependant appliquer encore le droit »[2451], caractérisant, par conséquent, l'illusion de sécurité et de liberté[2452] s'articulant principalement autour d'un art de la gouverne suivant les nécessités et tendances du moment gouvernemental.

Dans cette perspective, « *face à un tel État, il nous faut repenser les stratégies traditionnelles du conflit politique. Dans le paradigme sécuritaire, tout conflit et toute tentative plus ou moins violente de renverser le pouvoir fournissent à l'État l'occasion d'en gouverner les effets au profit d'intérêts qui lui sont propres. C'est ce que montre la dialectique qui associe étroitement terrorisme et réponse de l'État dans une spirale vicieuse. La tradition politique de la modernité a pensé les changements politiques radicaux sous la forme d'une révolution qui agit comme le pouvoir constituant d'un nouvel ordre constitué. Il faut abandonner ce modèle pour penser plutôt une puissance purement destituante, qui ne saurait être captée par le dispositif sécuritaire et précipitée dans la spirale vicieuse de la violence. Si l'on veut arrêter la dérive antidémocratique de l'État sécuritaire, le problème des formes et des moyens d'une telle puissance destituante constitue bien la question politique essentielle qu'il nous faudra penser au cours des années qui viennent* »[2453].

[2448] G. AGAMBEN, *État d'exception*, *Id.*, p. 10.
[2449] G. AGAMBEN, *État d'exception, Ibid.*, p. 18.
[2450] G. AGAMBEN, *État d'exception*, *Ibidem*, p. 29.
[2451] G. AGAMBEN, *État d'exception*, *Ibidem*, p. 146.
[2452] *Cf.* p. 487.
[2453] G. AGAMBEN, « Comment l'obsession sécuritaire fait muter la démocratie », *Id.,* p. 23

Chapitre II. Le traitement des identités numériques : Un changement de paradigme socioculturel

« *Le développement de la médecine, la médicalisation générale du comportement, des conduites, des discours, des désirs, tout cela se fait sur le front où viennent se rencontrer les deux nappes hétérogènes de la discipline et de la souveraineté. […]*
C'est ce que j'appellerais une « société de normalisation ». »[2454]

Dès les années 30, A. Huxley « *[…] qui construisit […] son récit dystopique sur le Brave New World en singeant les managers de la société fordienne et de l'« État mondial », affublé de la devise « Communauté, Identité, Stabilité »* »[2455] avait conçu et envisagé le changement de paradigme socioculturel pouvant, un jour, affecter la société de l'information et de contrôle social grâce à la révolution numérique.

Épistémologiquement, un paradigme indique une « *conception théorique dominante ayant cours à une certaine époque dans une communauté scientifique donnée, qui fonde les types d'explication envisageables, et les types de faits à découvrir dans une science donnée* », synonyme « de modèle, d'exemple »[2456]. Dans les sciences humaines et sociales, ce terme est utilisé dans deux sens différents : « *D'une part, il représente tout l'ensemble de croyances, de valeurs reconnues et de techniques qui sont communes aux membres d'un groupe donné. D'autre part, il dénote un élément isolé de cet ensemble : les solutions d'énigmes concrètes qui, employées comme modèles ou exemples, peuvent remplacer les règles explicites en tant que bases de solutions pour les énigmes qui subsistent dans la science normale* »[2457]. À l'ère du numérique et du traitement massif et généralisé des données et, par leur biais, des identités, cette conception scientifique du paradigme souligne les enjeux auxquels peuvent être confrontées les identités humaines au regard du traitement de leurs données suscitant, conséquemment, des nouvelles cultures et structures sociales, comme modèle, teintées de numérique. Une société de contrôle voit ainsi le jour, à côté de la société de l'information mise en œuvre, qui aspire vers une régulation sociale innovante, principalement *via* les nouvelles technologies développées, et en développement continu, et la revivification de certaines

[2454] J. REVEL, *Le vocabulaire de Foucault*, *op. cit.*, p. 46 ; et, M. FOUCAULT, *Il faut défendre la société*, *op. cit.*, Cours du 14 janvier 1976 - p. 34-35.
[2455] Cultures & Conflits, « Société de la connaissance, société de l'information, société de contrôle. Entretien avec Armand Mattelart », *In* Cultures & Conflits n° 64, Hiver 2006 (4/2006), (p. 167-183), p. 169, §10 ; disponible en ligne : https://doi.org/10.4000/conflits.2051
[2456] CNRTL, « Paradigme » : https://www.cnrtl.fr/definition/paradigme
[2457] T.S. KUHN, *La Structure des révolutions scientifiques*, Paris, Ed. Flammarion (Nouvelle Bibliothèque scientifique), 1992, trad. de la nouvelle éd., *The Structure of Scientific Revolutions*, publiée par The University of Chicago Press (1970), p. 207.

sciences et architectures dites de contrôle, comme la cybernétique, le panoptique ou la biopolitique.

Précisément, la société de contrôle *« est une société où se multiplient les mécanismes sociotechniques du contrôle flexible. Les vertus cardinales de ce mode de gestion – autonomie, créativité, réactivité, adaptabilité – se conjuguent avec les exigences de la « grille des objectifs » et de la « culture du résultat ». Le contrôle y est à court terme, à rotation rapide, mais continue et illimitée. Cette nouvelle feuille de route a l'arrière-goût de l'implication contrainte, de la servitude volontaire et de la précarité. Elle est en résonance avec le régime des nouvelles technologies informationnelles* »[2458].

Quels sont donc les effets du changement de paradigme socioculturel avéré ou initié par les nouvelles technologies et les nouvelles cultures numériques ? Autrement dit, de quelle manière le traitement des identités numériques constitue-t-il un changement de paradigmes et de cultures sociales ? et comment contribue-t-il, *vice versa*, à ce changement ?

Cette dernière analyse montre ainsi que les nouvelles opérations de traitements de l'information, générée du soi connecté, suscitent l'émergence de nouvelles formes et cultures de contrôle social (Section 1), provoquant, subséquemment, la question d'une éventuelle remise en cause des identités humaines (Section 2) qui s'avère être fondamentale pour l'avenir de l'humanité, telle qu'elle est vécue et perçue jusqu'à présent.

Section 1 – L'émergence de nouvelles cultures de contrôle social

Ces cultures de contrôle social ne sont pas nouvelles, mais imprègnent progressivement les sociétés du XXI^{e} Siècle grâce au développement d'internet et des outils et technologies de l'information et de la communication faisant, ainsi, émerger et raviver une culture de cybernétique (§1) tout en alimentant, parallèlement, une culture d'asservissement numérique (§2) subtilement ressentie et vécue.

§1. Une Culture de cybernétique

La cybernétique, citée notamment par la nouvelle politique de défense et de sécurité, représente d'une part une science, un art de la gouverne (A) et, d'autre part, une science de l'information et de la communication (B), composant la nouvelle culture émergente s'articulant autour de la science de la cybernétique.

[2458] Cultures & Conflits, « Société de la connaissance, société de l'information, société de contrôle. Entretien avec Armand Mattelart », *Id.*, p. 169-170, §11.

A. Science, art de la gouverne

Norbert Wiener, mathématicien et philosophe, fonde dans les années 1940 la « cybernétique », terme qu'il inventa afin de désigner le champ tout entier d'un complexe d'idées qu'il étudie et analyse, dérivant du mot grec « *Kubernëtës* », ou « *steersman* » « pilote », le même mot grec dont est tiré le mot « *governor* », « gouverneur »[2459]. Développée initialement dans son ouvrage de 1948, cette notion se réfère à la théorie du « contrôle et de la communication chez l'animal et la machine »[2460], une science du contrôle et de l'information qui vise la connaissance et le pilotage des systèmes, qu'ils soient vivants ou non-vivants.

Lorsqu'elle a vu le jour, le gouvernement américain voulait la classer en « secret-défense », mais à la suite de l'opposition de la part de son fondateur, qui devenait de plus en plus antimilitariste, la cybernétique a finalement été rendue publique ; sa diffusion étant toutefois limitée à un cercle restreint de spécialistes. Depuis, la cybernétique et ses concepts et méthodes étant largement interdisciplinaires, elle est devenue un terrain de recherche bien établi, impactant différents domaines d'études, comme les mathématiques, la biologie, la physique, la neurophysiologie, l'ingénierie, la mécanique, l'informatique, la philosophie, les sciences cognitives, la psychologie, portée par un cadre de chercheurs divers et variés qui y ont contribué, tels que J. Von Neumann, M. Mead, G. Bateson, W. Pitts, W. Weaver, C. Shannon, W. McCulloch ou encore A. Turing[2461]. Étymologiquement, le terme de cybernétique implique essentiellement une méthodologie de l'action, sous-tendant une action de manœuvrer, de piloter un vaisseau, de gouverner. Couffignal, un des pionniers français de la cybernétique, la définit comme « l'art d'assurer l'efficacité de l'action »[2462], qui se rapproche donc de la conception de la gouverne telle que perçue par Platon, le bon pilote étant celui dont l'action est la plus efficace dans la tempête, à cause de son art et de l'autorité qu'il a sur les matelots[2463].

Afin de bien saisir la cybernétique, il faut se resituer dans le contexte de guerre et de chaos qui prévalait pendant les années 1939-1945. Dans ces conditions, ce n'était pas d'abord en formant de bons chefs, avec l'aide de philosophes comme Platon ou Aristote, qu'il était certain d'assurer

---

[2459] N. WIENER, *The human use of human beings: Cybernetics and society*, Da Capo Press, (1950-1954 Houghton Mifflin), 1988, p. 15, où l'auteur précise "*Incidentally, I found later that the word has already been used by Ampère with reference to political science, and had been introduced in another context by a Polish scientist, both uses dating from the earlier part of the nineteenth century*."

[2460] N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, Martino Publishing, (1948-1961 The MIT Press), 2013.

[2461] N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *Id.*, p. 12-19.

[2462] L. COUFFIGNAL, *La cybernétique*, Presses universitaires de France, Coll. Que sais-je ?, n° 638, Paris, 1963.

[2463] Platon, *Œuvres de Platon,* t. 9ème, Paris, Rey et Gravier Libraires, 1833, La République, Livre 1er, p. 35 ; Disponible en ligne : http://remacle.org/bloodwolf/philosophes/platon/cousin/rep1.htm

la victoire de manière efficace ; c'était plutôt en étudiant, grâce à des méthodes appropriées, la façon dont l'information circule et s'organise, ce qui impliquait par conséquent, selon Wiener, l'étude de la théorie des messages qui comprend la science du contrôle : « *besides the electrical engineering theory of the transmission of messages, there is a larger field which includes not only the study of language but the study of messages as a means of controlling machinery and society, the development of computing machines and other such automata, certain reflections upon psychology and the nervous system, and a tentative new theory of scientific method* » ; cette théorie élargie des messages étant une théorie probabiliste, partie intrinsèque du mouvement qui doit son origine à W. Gibbs[2464].

La définition de la notion de cybernétique comprend à la fois les notions de communication et de contrôle qui sont assimilées, selon l'auteur, puisqu'en communiquant avec une autre personne, un message lui est transmis et quand cette personne communique à son tour, un message de même nature est retourné contenant des renseignements accessibles d'abord à elle et non à la personne réceptrice du message ; en contrôlant les actions d'une autre personne, un message lui est communiqué, et bien que ce message soit de nature impérative, la technique de communication ne diffère pas de celle d'un message relatif à des faits. De plus, pour que le contrôle soit efficace, effectif, une connaissance de tous les messages émanant de la personne (à contrôler) doit être mise en œuvre pouvant donc indiquer que l'ordre est compris et a été exécuté. C'est la thèse centrale de Wiener dans son ouvrage sur la cybernétique et la société, selon laquelle « *society can only be understood through a study of the messages and the communication facilities which belongs to it; and that in the future development of these messages and communication facilities, messages between man and machines, between machines and man, and between machine and machine, are destined to play an ever-increasing part* »[2465].

En effet, indique l'auteur, quand un ordre est donné à une machine, la situation ne diffère pas fondamentalement de celle qui se présente quand un ordre est donné à une personne en ce sens que, de manière consciente, il y a eu connaissance de l'ordre qui a été donné et du signal de conformité qui est revenu ; les étapes intermédiaires de transmission du signal, qu'il soit passé par une machine ou par une personne, étant sans importance et n'apportant aucune modification à la relation entretenue avec le signal reçu : « *thus the theory of control in engineering, whether human or animal or mechanical, is a chapter in the theory of messages* »[2466]. C'est alors

[2464] N. WIENER, *The human use of human beings*, *Id.*, p. 15.
[2465] N. WIENER, *The human use of human beings*, *Ibid.*, p. 16.
[2466] N. WIENER, *The human use of human beings*, *Ibid.*, p. 16-17.

l'objectif de la cybernétique, celui de développer un langage et des techniques permettant de s'attaquer effectivement au problème du contrôle et de la communication en général, mais aussi de trouver le répertoire approprié d'idées et de techniques pour classer leurs manifestations particulières sous certains concepts. Les commandes à travers lesquelles un contrôle est exercé sur un environnement donné constituent une sorte d'information qui lui a été communiquée, et comme toute forme d'information, ces commandes sont sujettes en transit à des désorganisations, des perturbations, parvenant en général avec moins de cohérence. Avec le contrôle et la communication, c'est une lutte perpétuelle, précise l'auteur, contre la tendance naturelle à dégrader, à détériorer l'organisé, l'ordonné, et à détruire le significatif, le compréhensible ; la tendance donc de l'entropie à s'accroître[2467], entendue comme la désorganisation, le chaos, la quantité de désordre dans un système : « *En effet, au cœur de la cybernétique telle que la conçoit Wiener repose la notion d'entropie, terme issu de la thermodynamique et désignant la « quantité de désordre » au sein d'un système isolé. L'observation montre un mouvement de l'organisation (l'état le moins probable) vers la désorganisation (l'état le plus probable) : un système donné a beaucoup plus de chances de perdre de l'ordre que d'en gagner* »[2468].

Par information, ce ne sont pas uniquement les renseignements qui sont visés, qui demeurent certes nécessaires dans une guerre, mais plutôt l'ensemble des messages, verbaux et non verbaux, conscients et inconscients, qui circulent aussi bien entre un pilote et son co-pilote qu'entre deux ordinateurs ou deux cellules d'un organisme. L'échange d'informations dans la vision de Wiener implique des êtres libres puisque, *in fine*, l'ensemble des informations émises et reçues par une personne sont combinées avec celles qui sont déjà accumulées par elle, influençant *ipso facto* son action et comportement futurs. En effet, l'information est un terme désignant le contenu de ce qui est échangé avec le monde extérieur à mesure que l'Homme s'y adapte et qu'il y fait ressentir, appliquer, son adaptation ; le processus de réception et d'utilisation de l'information représentant le processus de l'adaptation, de l'ajustement aux contingences de l'environnement externe et ambiant, et la possibilité de vivre efficacement dans ce milieu. Les besoins et la complexité de la vie moderne, indique l'auteur, rendent plus nécessaire que jamais ce processus d'information et la presse, les musées, les laboratoires

[2467] N. WIENER, *The human use of human beings*, *Ibidem*, p. 16-17.

[2468] B. LOVELUCK, *Réseaux, Libertés et Contrôle*, *op. cit.,* p. 36, et l'auteur indique que « *Pour Wiener l'univers, dans son ensemble, tend vers le chaos, malgré quelques enclaves organisées, locales et transitoires. Il désigne cet équilibre précaire sous le nom d' « homéostasie ». Par exemple, la substance de l'identité individuelle n'est qu'un agencement mouvant de cellules, et le « modèle » qui les organise permet à « la vie » d'atteindre à cette stabilité temporaire*. »

scientifiques, les universités, les bibliothèques ou les manuels sont tenus de satisfaire les besoins de ce processus, ou, sinon, n'atteignent pas leur but. Vivre efficacement, c'est vivre avec une information adéquate précise Wiener : « *thus, communication and control belong to the essence of man's inner life, even as they belong to his life in society* »[2469].

L'assimilation de la vie à la machine, que l'auteur opère dans ses développements, peut évoquer le matérialisme, mais c'est surtout le formalisme qui caractérise la cybernétique. Wiener, fortement inspiré par Leibniz sans pour autant suivre ses idéologies, a repris quelques-unes de ses aspirations, mais aussi celles d'autres chercheurs, qui sont dominées selon l'auteur par les idées de communication, notamment les machines à calculer et les automates, « *automata* », mais aussi le « *calculus raciocinator* », le calcul de logique[2470], en vue de mettre en place une théorie de l'information, comprenant le contrôle et la communication, applicable concomitamment aux organismes vivants, aux machines et à l'organisation sociale afin d'assurer, de manière efficace et autorégulée ou auto-organisée, une production de la connaissance, la gouverne des sociétés et la conduite des guerres.

Il est vrai que l'époque où ces idées se concrétisaient était une période de guerre dominée par la barbarie, le chaos et les camps de concentration, et où des personnalités comme Staline et Hitler représentaient l'image du chef traditionnel. Dès lors, il pouvait sembler plus raisonnable et plus logique de s'en remettre à des procédés automatiques et des machines à calculer, qui s'autorégulaient et s'auto-organisaient, plutôt que de former des chefs ; ses travaux furent, par conséquent, initialement orientés vers et financés par l'armée. Ayant d'abord travaillé pour la défense américaine, Wiener passa la fin de sa vie à militer pour la paix et pour l'humanité par le biais de ses travaux, de sorte que le pessimisme de la guerre soit corrigé ou doublé d'un optimisme technologique. Sa vision était celle d'imaginer toutes les manières par lesquelles l'Homme, en communiquant de façon efficace et donc en levant tous les obstacles au développement et à l'innovation dans tous les domaines de l'information, y compris les obstacles de droit tels que la propriété intellectuelle ou industrielle ou encore le secret-défense ou secret des affaires, pourrait étendre sa culture ou sa vie, voire lutter contre la guerre et le chaos, *in fine* contre l'entropie.

Son analyse, qualifiée parfois d' « anarchisme rationnel », supposait le dépérissement de l'État par l'autorégulation, l'autogouverne de l'organisation sociale. Dans ce cadre, il est utile de noter que Wiener, devenu antimilitariste et pacifiste, se distingue de Von Neumann, autre scientifique ayant largement contribué au développement de la cybernétique et qui mit également au point,

[2469] N. WIENER, *The human use of human beings*, *Id.*, p. 18.
[2470] N. WIENER, *The human use of human beings*, *Ibid.*, p. 19.

entre autres, la théorie des jeux et le calcul balistique. Porteuse d'une méthodologie interdisciplinaire et ayant la capacité d'être appliquée dans n'importe quel secteur de recherche, la cybernétique devint progressivement synonyme d'application des mathématiques et des méthodes de calcul à toutes les sciences, souvent orientée vers la planification et la gestion optimales de la société. C'est dans cette perspective que cette science évoque fondamentalement la notion de contrôle, en ce sens que la connaissance et la compréhension des systèmes permet à un agent extérieur, au pilote, d'orienter ceux-ci vers un but fixé au préalable et donc de réguler, de gouverner l'organisation sociale, technique, politique, scientifique ou encore militaire, caractérisant l'art de la gouverne, l'art du pilotage que constitue, en partie, la cybernétique.

E. Morin, percevant les dérives que la pensée cybernétique pouvait induire, indiquait que *« l'idée de cybernétique, art/science de la gouverne, peut s'intégrer et se transformer en cybernétique, art/science de piloter ensemble, où la communication n'est plus un outil de la commande, mais une forme symbolique complexe d'organisation* »[2471], évoquant en ce sens l'idée de la systémique ainsi que l'idée de Platon écrivant « *n'est-ce pas à la fois le pilote et les matelots, dont les sens s'unissent a l'intelligence du pilote, qui se sauvent eux-mêmes en même temps que le vaisseau ?* »[2472]. Dès lors, en élargissant le sens de la cybernétique et en essayant d'en extraire la notion de commande tout en gardant celle de l'information, Morin souhaitait clairement l'infléchir vers la démocratie et éviter les dérives totalitaires qu'il percevait. C'est une prudence élémentaire dans la mesure où s'il existe bien une science qui, par sa nature et son essence même, semble destinée à servir le totalitarisme, c'est bel et bien la cybernétique, mais au regard des politiques de sécurité dernièrement mises en œuvre, il est possible d'avancer que les dérives pressenties par Wiener et Morin se sont en quelque sorte réalisées, alors même que tous deux aspiraient à libérer l'humanité de celles-ci et des abus pouvant en découler.

Pour Couffignal, les organes cybernétiques remplacent l'Homme dans l'exécution d'opérations mentales : ce sont des « machines à penser »[2473] évoquant l'idée, déjà amorcée par Wiener, que la place de l'Homme dans ses rapports avec la technique et l'ingénierie s'est transformée, induisant une convergence entre l'homme et la machine et la possibilité de classer et de hiérarchiser. La classification pouvait désormais inclure les automates et les créations techniques de l'Homme compte tenu du fait que l'échelle s'est déplacée : « *c'est la « complexité » des différents systèmes informationnels en présence, entendu comme leur*

[2471] E. MORIN, *La méthode 1. La nature de la nature*, t. I, Ed. du Seuil, 1977, p. 356-357.
[2472] PLATON, *Les Lois – Livres VII à XII*, Ed. Flammarion, 2006, Livre XII, Chap. X, p. 337.
[2473] L. COUFFIGNAL, *Les machines à penser*, Les Éditions de Minuit, 2ème Ed., Paris, 1964.

capacité à apprendre, qui permettrait dorénavant d'ordonner et de hiérarchiser le monde – indépendamment de leur nature humaine, animale ou artificielle. L'homme est ainsi présenté comme un « être-pour-la-communication », dont les caractéristiques individuelles importent moins que ses rapports informationnels avec le monde – y compris le monde technique des êtres artificiels »[2474].

Conscient de l'impact que les applications de la cybernétique pouvaient éventuellement avoir sur la société, Wiener prévoyait la fin du travail humain, remplacé par des machines intelligentes, et met en garde les responsables politiques contre les conséquences d'une utilisation de la cybernétique qui ne serait pas accompagnée d'une évolution « post-industrielle » ou d'une « seconde révolution industrielle » de la société et de ses structures, au sein de laquelle l'homme pourrait être libéré du travail. Ainsi, selon l'auteur, « *it has long been clear to me that the modern ultra-rapid computing machine was in principle an ideal central nervous system to an apparatus for automatic control; […]. With the aid of strain gauges or similar agencies to read the performance of these motor organs and to report, to "feed back", to the central control system as an artificial kinesthetic sense, we are already in a position to construct artificial machines of almost any degree of performance. […]. I have said that this new development has unbounded possibilities for good and for evil*[2475]*. […]. Of course, just as the skilled carpenter, the skilled mechanic, the skilled dressmaker, have in some degree survived the first industrial revolution, so the skilled scientist and the skilled administrator may survive the second. However, taking the second revolution as accomplished, the average human being of mediocre attainments or less has nothing to sell that it is worth anyone's money to buy. The answer of course is to have a society based on human values other than buying or selling* »[2476].

En outre, il prévenait que si cette évolution fait défaut, un développement excessif du chômage et de l'exclusion sociale, voire du contrôle social, verrait le jour, ce qui, à terme, pourrait

---

[2474] B. LOVELUCK, *Réseaux, Libertés et Contrôle, Id.*, p. 32

[2475] "*For one thing, it makes the metaphorical dominance of the machine, as imagined by Samuel Butler, a most immediate and non-metaphorical problem. It gives the human race a new most effective collection of mechanical slaves to perform its labor. Such mechanical labor has most of the economic properties of slave labor, although, unlike slave labor, it does not involve the direct demoralizing effects of human cruelty. However, any labor that accepts the conditions of competition with slave labor accepts the conditions of slave labor, and is essentially slave labor. The key word of this statement is* ***competition****. It may very well be a good thing for humanity to have the machine remove from it the need of menial and disagreeable tasks, or it may not. I do not know. It cannot be good for these new potentialities to be assessed in the terms of the market, of the money they save; and it is precisely the terms of the open market, the "fifth freedom" that have become the shibboleth of the sector […]*": N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *Id.*, p. 27.

[2476] N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *Id.*, p. 27-28.

conduire au dépérissement de la démocratie et à la création d'une société de contrôle. Wiener indiquait ainsi très consciencieusement que « *those of us who have contributed to the new science of cybernetics thus stand in a moral position which is, to say the least, not very comfortable. We have contributed to the initiation of a new science which, as I have said, embraces technical developments with great possibilities for good and for evil. We can only hand it over into the world that exists about us, and this is the world of Belsen and Hiroshima. We do not even have the choice of suppressing these new technical developments. They belong to the age, and the most any of us can do by suppression is to put the development of the subject into the hands of the most irresponsible and most venal of our engineers. The best we can do is to see that a large public understands the trend and the bearing of the present work, and to confine our personal efforts to those fields, such as physiology and psychology, most remote from war and exploitation. As we have seen, there are those who hope that the good of a better understanding of man and society which is offered by this new field of work may anticipate and outweigh the incidental contribution we are making to the concentration of power (which is always concentrated, by its very conditions of existence, in the hands of the most unscrupulous). I write in 1947, and I am compelled to say that it is a very slight hope* »[2477]. Toutefois, envisagé sous un autre angle et dans une perspective plus humaine et éthique, la cybernétique peut également constituer une source d'inspiration positive et féconde, aboutissant à l'invention d'une sorte de « capitalisme à visage humain », conciliant l'Homme, l'économie (non-monétaire) et l'environnement.

Le monde est intégralement constitué de systèmes, vivants ou non-vivants, imbriqués, dynamiques et en interaction continue, caractérisant des systèmes complexes[2478]. Dans cette perspective, une société, une économie, un réseau d'ordinateurs, une entreprise, un cerveau, ou même un individu peuvent être considérés comme formant un « système ». Les ordinateurs et toutes les machines ou technologies intelligentes, telles qu'elles se présentent aujourd'hui, sont des applications de la cybernétique. Cette dernière a également fourni des méthodes et des "armes silencieuses" puissantes permettant de contrôler deux systèmes majeurs : la société et

[2477] N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *Ibid.*, p. 28-29.
[2478] « *Un système complexe peut être défini comme un système composé de nombreux éléments interagissant de manière dynamique. Ces systèmes font émerger des propriétés nouvelles, émergeantes, non observables au niveau des éléments constitutifs, par une dynamique difficilement prédictible et rendent vaine toute analyse en termes de réduction et de simplification d'un quelconque système dit complexe…* » : D. BOURCIER, R. BOULET et P. MAZZEGA, « La gouvernance des systèmes complexes : Réflexions et recherches sur les politiques publiques aujourd'hui », *In* D. Bourcier, R. Boulet & P. Mazzega (éd.), *Politiques publiques – Systèmes complexes*, Ed. Hermann, 2012, p. 9.

l'économie[2479]. D'autre part, le réseau internet ayant pris forme dans le cadre d'un projet au Pentagone, il était logique que, née dans un contexte militaire, la cybernétique finisse par y trouver son premier champ d'application ; un champ d'application finalement érigé par la politique de sécurité française, notamment la nouvelle loi de programmation militaire, en « axe d'effort prioritaire » qu'il faut absolument développer et exploiter afin de garantir le propre fonctionnement et la résilience du Ministère des Armées, « tout en contribuant à la continuité

[2479] « Silent weapons for quiet wars - Armes silencieuses pour guerres tranquilles/sans bruit », An introductory programming manual, Operations Research, Technical Manual, TM-SW7905.1 – Le document suivant, daté de Mai 1979, a été trouvé le 7 Juillet 1986 dans un photocopieur IBM acheté à une vente de surplus militaire, et fut publié en annexe du livre "*Behold a pale horse*" de William Cooper, Light Technology Publishing, 1991 : « *Il est manifestement impossible de parler d'engineering social, ou d'automatisation d'une société (engineering des systèmes d'automatisation sociale ou "armes silencieuses") sur une échelle nationale ou internationale sans impliquer de vastes objectifs de contrôle social et de destruction de la vie humaine (c'est à dire d'esclavage et de génocide). Ce manuel est en lui-même une déclaration d'intention de ce type. Un tel écrit doit être tenu à l'abri du regard du public. Autrement, il pourrait être reconnu comme une déclaration formelle et technique de guerre intérieure. De plus, dans le cas où une personne ou un groupe de personnes dans une position de pouvoir importante utiliseraient une telle connaissance et une telle méthodologie pour la conquête économique, il doit être compris qu'un état de guerre intérieure existe alors entre ce groupe de personnes et le public. La solution aux problèmes de notre époque requiert une approche impitoyablement franche, sans s'embarrasser de valeurs religieuses, morales, ou culturelles. […]. La technologie des armes silencieuses a évolué à partir d'Operations Research (O.R.), une méthodologie stratégique et tactique développée par l'état-major militaire en Angleterre durant la Seconde Guerre Mondiale. Le but original d'Operations Research était d'étudier les problèmes stratégiques et tactiques de défense aérienne et terrestre avec pour objectif l'utilisation effective de ressources limitées contre des ennemis étrangers. Il fut bientôt reconnu par ceux en position de pouvoir que les mêmes méthodes pouvaient être utiles pour contrôler totalement une société. Mais de meilleurs outils étaient nécessaires. L'engineering social (l'analyse et l'automatisation d'une société) requièrent la mise en relation d'une grande quantité d'informations économiques toujours changeantes, si bien qu'un système ultra-rapide de traitement de l'information était nécessaire pour prendre de vitesse la société, et prédire quand celle-ci sera parvenue à sa capitulation. […]. La Guerre Tranquille fut tranquillement déclarée par l'Elite Internationale lors d'une rencontre tenue en 1954. […].*
Tout ce qui est attendu d'une arme ordinaire est attendu d'une arme silencieuse par ses créateurs, mais seulement dans sa manière de fonctionner. Elle tire des situations, au lieu de balles ; propulsées par le traitement des données, au lieu d'une réaction chimique ; tirant leur origine d'octets d'informations, au lieu de grains de poudre ; à partir d'un ordinateur, au lieu d'un fusil ; manipulée par un programmeur d'ordinateur au lieu d'un tireur d'élite, sous les ordres d'un banquier au lieu d'un général d'armée. Elle ne produit pas de bruit d'explosion évident, ne cause pas de dommages physiques ou mentaux évidents, et n'interfère pas de façon évidente avec la vie quotidienne sociale de chacun. Elle produit pourtant un immanquable "bruit", cause d'immanquables dommages physiques et mentaux, et interfère de façon immanquable avec la vie sociale quotidienne ; ou plutôt, immanquable pour un observateur entraîné, pour celui qui sait quoi regarder. Le public ne peut pas comprendre cette arme, et donc ne peut pas croire qu'il est attaqué et soumis par une arme. Le public peut instinctivement sentir que quelque chose ne va pas, mais en raison de la nature technique de l'arme silencieuse, il ne peut pas exprimer son sentiment d'une façon rationnelle, ou prendre en main le problème avec intelligence. Par conséquent, il ne sait pas comment crier à l'aide, et ne sait pas comment s'associer avec d'autres pour se défendre. Lorsqu'une arme silencieuse est appliquée graduellement, les gens s'ajustent, s'adaptent à sa présence, et apprennent à tolérer ses répercussions sur leurs vies jusqu'à ce que la pression (psychologique via économique) devienne trop grande et qu'ils s'effondrent. En conséquence, l'arme silencieuse est un type d'arme biologique. Elle attaque la vitalité, les options, et la mobilité des individus d'une société, en connaissant, comprenant, manipulant, et attaquant leurs sources d'énergie sociales et naturelles, ainsi que leur forces et faiblesses physiques, mentales, et émotionnelles. » : https://www.syti.net/SilentWeapons.html ; http://carthoris.free.fr/Biblioth%E8que/Armes%20silencieuses%20pour%20guerres%20tranquilles.pdf ; http://dimsung.free.fr/doc/armesilencieuse.pdf ; https://archive.org/stream/SilentWeaponsForQuietWars_201701/SilentWeaponsForQuietWars_TruthTalkNewsWithHowardNema1_djvu.txt

des grandes fonctions vitales de la Nation »[2480]. Comme le préconisait Wiener, « *[…] the most fruitful areas for the growth of the sciences were those which had been neglected as a no man's land*[2481] *between the various established fields* »[2482].

L'ère de la révolution numérique, ère de l'information, de la communication et des systèmes complexes, offre à la cybernétique une place particulièrement déterminante permettant son développement exponentiel. Le Livre blanc de 2013 n'y échappe pas et indique en ce sens que « les opérations ciblées et les frappes à distance ou cybernétiques « *pourraient devenir plus fréquentes, compte tenu de leur souplesse d'emploi dans un contexte où les interventions classiques continueront d'être politiquement plus difficiles et parfois moins efficaces* »[2483], et affirme que *« le développement rapide des infrastructures numériques ne s'est pas toujours accompagné d'un effort parallèle de protection, de sorte que les agressions de nature cybernétique sont relativement faciles à mettre en œuvre et peu coûteuses. Leur furtivité complique l'identification de leurs auteurs qui peuvent être aussi bien étatiques que non-étatiques* »[2484].

Dès lors, afin d'y faire face efficacement, une connaissance anticipée et détaillée de la cible visée est désormais prévue, « *connaissance qui peut s'acquérir par des attaques préalables de moindre ampleur destinées à tester la cible, ou par des renseignements obtenus par d'autres moyens* »[2485]. En outre, dans le cadre de la loi de programmation de 2018, il est prévu qu' « *en matière de sécurité cybernétique, l'organisation informatique et la sécurisation des réseaux seront optimisées, tandis que les moyens de lutte informatique défensive seront développés* »[2486], mais surtout que la période fixée par ladite loi, à savoir 2019-2025, « *sera aussi mise à profit pour étudier l'élargissement des contextes opérationnels d'emploi de l'arme cybernétique* »[2487].

Sous couvert de « défense totale », l'impératif de sécurité appliqué au traitement de l'information soulève de nombreux enjeux relatifs à l'exercice du pouvoir dans des sociétés définies comme démocratiques, caractérisant par là même une dichotomie qui se forme entre société de l'information et société de contrôle, tout en concrétisant, « avant tout, une nouvelle

---

[2480] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 2.1.2.2. *La protection*
[2481] *Cf.* p. 540.
[2482] N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *Id.*, p. 2.
[2483] Livre blanc sur la défense et la sécurité nationale 2013, Chap. 3, § A. *Ruptures et évolutions*, p. 30.
[2484] Livre blanc sur la défense et la sécurité nationale 2013, Chap. 3, § D. *Les menaces et les risques amplifiés par la mondialisation*, p. 44-45.
[2485] Livre blanc sur la défense et la sécurité nationale 2013, Chap. 3, § D., *Id.*, p. 45.
[2486] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.1.1.3. *Sécurité-Protection et résilience*
[2487] Loi du 13 juillet 2018 relative à la programmation militaire - Rapport annexé, § 3.3.3.1. *Une structuration volontariste de l'action du ministère dans l'espace numérique*

étape dans la rationalisation de l'organisation et du contrôle des sociétés humaines » dont les résultats peuvent être décrits à travers « *l'expression de « technologies intellectuelles » – définies comme une substitution des jugements intuitifs par des algorithmes (en tant que règles permettant de résoudre un problème), et incarnées dans des machines, des programmes informatiques et toutes les formes de procédures décisionnelles. C'est donc un processus de long terme, que Beniger appelle la « révolution du contrôle », qui donne sa cohérence à la trajectoire menant de la révolution industrielle à la « société de l'information », et dont l'ordinateur peut être perçu comme l'un des principaux aboutissements. Par ailleurs, il montre que cette vision de l'organisation sociale est modelée sur celle de l'organisme biologique, et se présente comme un vaste problème de programmation* »[2488], alors même que le fondateur de la cybernétique avait activement tenté d'exclure toute forme d'exploitation de l'information.

B. Science de l'information et de la communication

L'information, définie par F. Varela comme ressemblant « *à un phlogistique moderne qui expliquerait la structure de la connaissance en s'appuyant sur un ordre des choses préexistant […]* »[2489], est, selon l'approche cybernétique, commune aux machines ainsi qu'aux organismes vivants. Définie de la sorte, il apparaît que les organismes vivants sont assimilés aux machines, or, indique Wiener, « *when I compare the living organism with such a machine, I do not for a moment mean that the specific physical, chemical, and spiritual processes of life as we ordinarily know it are the same as those of life-imitating machines. I mean simply that they both can exemplify locally anti-entropic processes, which perhaps may also be exemplified in many other ways which we should naturally term neither biological nor mechanical* »[2490].

D'où l'importance de l'information et de la théorie des messages aux yeux du père de la cybernétique, inspiré par la philosophie de Saint-Augustin sur le mal (« Le mal, affirmait Saint-Augustin, n'est pas en lui-même une puissance, mais la mesure même de notre faiblesse »), voulant remédier à l'imperfection humaine et éviter le chaos et la désorganisation, qui explique à cet égard que les messages sont eux-mêmes une forme de « pattern », de « modèle », et d' « organisation » : « *indeed, it is possible to treat sets of messages as having an entropy like sets of states of the external world. Just as entropy is a measure of disorganisation, the*

[2488] B. LOVELUCK, *Réseaux, Libertés et Contrôle, Id.*, p. 34-35.
[2489] F. J. VARELA, *Invitation aux sciences cognitives*, *op. cit*., p. 12-13, et l'auteur explique que le phlogistique est le « *nom désignant le fluide imaginé au dix-huitième siècle comme la substance même de la chaleur pour expliquer certains phénomènes physiques dont rend compte aujourd'hui la thermodynamique, avec des modèles fort différents* » (note de bas de p. n°1).
[2490] N. WIENER, *The human use of human beings*, *op. cit.*, p. 32.

information carried by a set of messages is a measure of organization. In fact, it is possible to interpret the information carried by a message as essentially the negative of its entropy, and the negative logarithm of its probability. That is, the more probable the message, the less information it gives. Clichés, for example, are less illuminating than great poems »[2491].

Un des effets de la pensée cybernétique est celle la rupture des distinctions admises entre l'artificiel et le vivant, l'âme et le corps, la machine et l'esprit en ce sens que la logique de raisonnement est indifférente à la matérialité des supports dans la mesure où ce n'est pas le matériel, le hardware, qui qualifie les phénomènes mais plutôt la structure des événements ou des comportements. Wiener se penche ainsi sur les veilles tentatives des anciennes machines développées aspirant à fabriquer des automates mais qui opéraient, entre autres, sur la base d'un mécanisme « d'horlogerie fermée », « *closed clockwork basis* », et souligne que les machines automatiques modernes, telles que les technologies de missiles contrôlés, les détonateurs de proximité, « *proximity fuse* », le mécanisme d'ouverture automatique des portes, l'appareillage de commande d'une usine de produits chimiques et le reste de l'arsenal moderne des machines automatiques remplissant des fonctions militaires ou industrielles, sont dotées d'organes sensoriels, à savoir des récepteurs pour les messages venant de l'extérieur[2492]. Chaque instrument dans le répertoire du fabricant d'instruments scientifiques est, selon l'auteur, un organe sensoriel possible et peut être constitué pour enregistrer à distance ses lectures et observations par l'intervention d'appareils électriques appropriés : « *thus the machine which is conditioned by its relation to the external world, and by the things happening in the external world, is with us and has been with us for some time. The machine which acts on the external world by means of messages is also familiar* »[2493].

Par conséquent, les différentes étapes entre la mise en action d'une machine de ce type par des organes sensoriels et son exécution d'une tâche peuvent être aussi simples que dans le cas d'une porte électrique, ou peuvent être de tout degré de complexité souhaité dans les limites des techniques d'ingénierie développées. Une action complexe, explique l'auteur, est une action dans laquelle les données introduites, nommées « input », pour obtenir un effet sur le monde extérieur, nommé « output », peuvent impliquer un grand nombre de combinaisons : « *these are combinations, both of the data put in at the moment and of the records taken from the past stored data which we call the memory. These are recorded in the machine. The most complicated machines yet made which transform input data into output data are the high-speed*

[2491] N. WIENER, *The human use of human beings*, *Id.*, p. 21.
[2492] N. WIENER, *The human use of human beings*, *Id.*, p. 22-23.
[2493] N. WIENER, *The human use of human beings*, *Ibid.*, p. 23.

electrical computing machines, […] »[2494]. En outre, rappelant que l'homme et l'animal ont un sens kinesthésique, par lequel ils enregistrent la position et les tensions de leurs muscles, l'auteur avance ainsi que « *for any machine subject to a varied external environment to act effectively it is necessary that information concerning the results of its own actions furnished to it as part of the information which it must continue to act. […]. This control of a machine on the basis of its actual performance rather than its expected performance is known as feedback, and involved sensory members which are actuated by motor members as perform the function of tell-tales or monitors – that is, of elements which indicate a performance* » ; et c'est bien la fonction de ces mécanismes, de contrôler et de réguler la tendance mécanique à la désorganisation, « *in other words, to produce a temporary and local reversal of the normal direction of entropy* »[2495].

L'approche cybernétique d'un « système » consiste, donc, en une analyse globale de tous les éléments composants ledit système, mais surtout, en une analyse de leurs interactions, de leurs échanges, *in fine*, de leur relation ; le but final étant de réguler la « boucle de feedback » par l'analyse de l'information. En effet, l'action d'un élément sur un autre génère, en retour, une réponse du second élément vers le premier ; c'est le « feedback », la rétroaction, le retour d'information. Par conséquent, ces deux éléments ayant entraîné une réponse sont dits liés par une « boucle de feedback », et ce feedback, précise Wiener, « *is a method of controlling a system by reinserting into it the results of its past performance* »[2496] ou, autrement dit, « *the property of being able to adjust future conduct by past performance. Feedback may be as simple as that of a common reflex, or it may be a higher order feedback, in which past experience is used not only to regulate specific movements, but also whole policies of behavior* »[2497]. De ce fait, un système fondé sur la cybernétique, étant donné qu'il a pour but de s'autoréguler et de s'auto-organiser, s'appuie sur un équilibre entre les boucles positives (qui amplifient une tendance) et les boucles négatives (qui diminuent une tendance) ; c'est donc un système qui tend à une stabilité, à un équilibre et à éviter le dérèglement ou le chaos[2498].

[2494] N. WIENER, *The human use of human beings*, *Ibid.*, p. 23-24.
[2495] N. WIENER, *The human use of human beings*, *Ibidem*, p. 24-25.
[2496] N. WIENER, *The human use of human beings*, *Ibidem*, p. 61.
[2497] N. WIENER, *The human use of human beings*, *Ibidem*, p. 33, et l'auteur indique à cet égard, "*such a policy-feedback may, and often does, appear to be what we know under one aspect as a conditioned reflex, and under another as learning*."
[2498] Un exemple de système cybernétique rudimentaire est un radiateur électrique. Celui-ci possède deux éléments, une résistance et un thermostat, liés par une boucle rétroactive : ainsi, l'augmentation de la chaleur déclenche d'elle-même la coupure du thermostat, provoquant en retour la baisse de la température, qui produira à son tour le ré-actionnement, la réouverture du thermostat.

Des systèmes issus de la nature, tel qu'un écosystème ou une cellule, représentent, à ce titre, des exemples parfaits de systèmes autorégulés. Un accent doit être mis sur les notions d'interaction et de relation dans la mesure où, du point de vue de la connaissance comme de l'existence, la relation et l'interaction priment sur le contenu d'un phénomène, d'une machine ou d'un organisme vivant, contenu qualifié parfois par l'auteur de « boîte noire »[2499], inscrutable qu'en termes d'entrée et de sortie, d'*input – output*.

La méthode cybernétique consiste alors en une méthode d'étude comportementale examinant les objets ou les sujets sous l'angle de l'information, et centrée sur la communication afin de la maîtriser en vue d'assurer une autorégulation, une auto-organisation, voire une autogouverne, efficace. Selon Wiener, « *it is my thesis that the physical functioning of the living individual and the operation of some of the newer communication machines are precisely parallel in their analogous attempts to control entropy through feed-back. Both of them have sensory receptors as one stage in their cycle of operation: that is, in both of them there exists a special apparatus for collecting information from the outer world at low energy levels, and for making it available in the operation of the individual or of the machine. In both cases these external messages are not taken neat, but through the internal transforming powers of the apparatus, whether it be alive or dead. The information is then turned into a new form available for the future stages of performance. In both the animal and the machine this performance is made to be effective on the outer world. In both of them, their performed action on the outer world, and not merely their intended action, is reported back to the central regulatory apparatus. This complex of behavior is ignored by the average man, and in particular does not play the role that it should in our habitual analysis of society; for just as individual physical responses may be seen from this point of view, so may the organic responses of society itself. I do not mean that the sociologist is unaware of the existence and complex nature of communications in society, but until recently he has tended to overlook the extent to which they are the cement which binds its fabric together* »[2500] ; dans l'état actuel de la science, le vide induit par cette omission est comblé.

[2499] « *I shall understand by a black box a piece of apparatus, such as four-terminal networks with two input and two output terminals, which performs a definite operation on the present and past of the input potential but for which we do not necessarily have any information of the structure by which this operation is performed* »: N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *op. cit.*, p. xi (note de bas de p. n°1); *Cf.* p. 205, 336, 345, 363, 438, 444 et 451.
[2500] N. WIENER, *The human use of human beings*, *Id.*, p. 26-27.

Ainsi, pour éviter le chaos, l'entropie, ce qui importe c'est le message dans sa capacité d'être transmis en vue d'assurer une bonne communication et l'intégrité des canaux de communication, essentielle au bien-être de la société[2501], et donc une organisation sociale efficace par le biais de l'information elle-même efficace ; le transport de l'information étant, *in fine*, plus important que le transport physique[2502]. Selon le cybernéticien, les problèmes de « control engineering » et de « communication engineering » sont finalement inséparables en ce sens qu'ils sont tous deux centrés autour de la notion fondamentale de « message », qu'il définit comme « *a discrete or continuous sequence of measurable events distributed in time – precisely what is called a time series by the statisticians. The prediction of the future of a message is done by some sort of operator on its past, whether this operator is realized by a scheme of mathematical computation, or by a mechanical or electrical apparatus* »[2503].

Tout organisme peut être, selon l'auteur, perçu comme message en ce sens que certains, tel que l'homme, tendent pendant un moment à se maintenir et souvent même à accroître leur niveau d'organisation : la vie représentant « an island here and now in a dying world », le processus par lequel les êtres vivants résistent à ce courant général de corruption et de désintégration, de pourriture, est connu sous le terme d' « homéostasie »[2504]. Et c'est bien le modèle, le *pattern*, maintenu par cette homéostasie qui constitue la pierre angulaire de l'identité personnelle de l'homme, eu égard au fait que les êtres humains ne sont pas des choses qui se conforment, mais plutôt des *patterns*, des modèles qui se perpétuent. Wiener précise ainsi « *a pattern is a message, and may be transmitted as a message* »[2505], d'où l'importance de la communication et de la transmission de l'information : « *even now the transportation of messages serves to forward an extension of man's senses and his capabilities of action from one end of the world to another* »[2506].

Cela soulève alors la question de l'individualité humaine, selon l'auteur, qui met l'accent sur l'importance fondamentale d'une circulation libre, efficace et éclairée de l'information tout en

---

[2501] N. WIENER, *The human use of human beings*, *Ibid.*, p. 131.
[2502] N. WIENER, *The human use of human beings*, *Ibid.*, p. 97, et l'auteur donne l'exemple d'un architecte gérant la construction à distance et indique "*In short, the bodily transmission of the architect and his documents may be replaced very effectively by the message-transmission of communications which do not entail the moving of a particle of matter from one end of the line to the other.*", p. 98.
[2503] N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *op. cit.*, p. 8-9.
[2504] N. WIENER, *The human use of human beings*, *Id.*, p. 95, l'auteur précise ainsi "*The oxygen and carbon dioxide and salt in our blood, the hormones flowing from our ductless glands, are all regulated by mechanisms which tend to resist any untoward changed in their levels. These mechanisms constitute what is known as homeostasis, and are negative feedback mechanisms of a type that we may find exemplified in mechanical automata.*", p. 96
[2505] N. WIENER, *The human use of human beings*, *Id.*, p. 96.
[2506] N. WIENER, *The human use of human beings*, *Ibid.*, p. 98.

mettant en garde contre les dérives de la théorie de la prédiction, accompagnant la théorie des messages, dont les principes et techniques ont été développés en période de guerre, scellés sous secret-défense et orientés vers la sécurité. Néanmoins, et Wiener le reconnaît, « *the principles proved to be sound and practical, and have been used by government for smoothing purposes, and in several fields of related work*. […] thus] *the end of the war saw the ideas of prediction theory and of the statistical approach to communication engineering already familiar to a large part of the statisticians and communication engineers of the United States and Great Britain* »[2507].

Dans les pays industrialisés actuels, le type de société qui émerge découle principalement de différentes applications de la cybernétique et de ses méthodes et techniques, comme le processus de robotisation et d'automaticité de la production, les réseaux financiers mondialisés, les nouvelles méthodes de gestion et d'organisation de l'entreprise, les nouvelles méthodes de marketing, les réseaux informatiques et de communications, le développement de l'intelligence artificielle, et ainsi de suite. En effet, la phase cybernétique, qui s'était passagèrement éteinte en 1956, a finalement produit un « incroyable éventail de multiples résultats concrets » : « *le choix largement répandu de la logique mathématique pour décrire le fonctionnement du système nerveux et du raisonnement humain ; l'instauration comme « méta » discipline de la théorie des systèmes, qui cherche à formuler les principes généraux gouvernant tout système complexe. Cette approche comparative abstraite a eu un impact important sur bien des domaines scientifiques, comme le génie (analyse de système, théorie du contrôle), la biologie (physiologie régulatoire, écologie), les sciences sociales (thérapie familiale, anthropologie structurale, gestion, urbanisme) et l'économie (théorie des jeux) ; l'avènement de la théorie de l'information comme une théorie statistique du signal et des canaux de communication, aujourd'hui encore à la base de bien des développements en technologie de la communication ; les premiers exemples de robots partiellement autonomes, les premiers systèmes incorporant une auto-organisation partielle* »[2508] ; et ce, sans compter le développement de la surveillance comme arme ou moyen cybernétique[2509], tel que perçu par les gouvernements et les entreprises, allant dans le sens du panoptique de Foucault[2510], alors même que Wiener prônait une transparence totale, une liberté de circulation de l'information éclairée, des messages non

[2507] N. WIENER, *Cybernetics or, Control and Communication in the Animal and the Machine*, *Id.*, p. 15-16.
[2508] F. J. VARELA, *Invitation aux sciences cognitives*, *op. cit.*, p. 32-33.
[2509] Pour plus d'informations : W. ERNST, "Beyond the rhetoric of panopticism: surveillance as cybernetics" *In* T.Y. Levin, U. Frohne and P. Weibel (eds.), *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*, ZKM Centre for Art and Media: Karlsruhe, The MIT Press, 2002, p. 460-463.
[2510] *Cf.* p. 592.

brouillés, la levée de tout bluff et la levée totale de toute secret, « *the compulsion of scientific warfare* […] *driving us pell-mell, head over heels into the ocean of our own destruction* […rushing] *quickly to our own subjection and annihilation* »[2511].

Le noyau même de la cybernétique trouve aujourd'hui une de ses places principales dans le cyberespace et la numérisation, développant progressivement, « de façon continue et conséquente, des moyens techniques qui permettaient à l'information de circuler indépendamment de ses supports physiques et des objets sur lesquels elle porte », de sorte que « les mouvements de communication ont acquis une vitesse différentes et rendent, « aussi bien en théorie qu'en pratique, l'information instantanément disponible à travers le monde »[2512]. Ce monde numérique donne souvent l'impression que « les hommes naissent et demeurent libres et égaux », et que toute personne dispose de sa liberté d'expression à volonté ; mais la réalité, de manière pragmatique et comme il a été vu tout au long de cette étude, est bien différente.
En effet, indique Bauman, au côté de l'espace « fabriqué » moderne, qui « *a subi un processus de « centralisation », d' « organisation » et de « normalisation »* […où] *ce furent les pouvoirs de la technique, la vitesse de son action et son coût qui se mirent dès lors à « organiser l'espace* » […et dans lequel] *la totalité sociale était faite d'espaces locaux de plus en plus grands, de plus en plus englobants, avec, perchée au sommet, l'autorité supra-locale de l'État surveillant l'ensemble, tout en se protégeant des regards* », existe désormais un autre espace, imposé par « l'avènement du réseau mondial de l'information », l' « espace cybernétique », et,

---

[2511] N. WIENER, *The human use of human beings*, *Id.*, p. 128-130, citons le texte entier qui est d'une grande utilité: "*The whole technique of secrecy, message jamming, and bluff, is concerned with insuring that one's own side can make use of the forces and agencies of communication more effectively than the other side. In this combative use of information, it is quite as important to keep one's own message channels open as to obstruct the other side in the use of the channels available to it. An overall policy in matters of secrecy almost always involve the consideration of many more things than secrecy itself. […]. I have already said the dissemination of any scientific secret whatever is merely a matter of time, that in this game a decade is a long time, and that in the long run, there is no distinction between arming ourselves and arming our enemies. […]. Like so many Gadarene swine, we have taken unto us the devils of the age, and the compulsion of scientific warfare is driving us pell-mell, head over heels into the ocean of our own destruction. Or perhaps we may say that among the gentlemen who have made it their business to be our mentors, and who administer the new program of science, many are nothing more than apprentice sorcerers, fascinated with the incantation which starts a devilment that they are totally unable to stop. Even the new psychology of advertising and salesmanship becomes in their hands a way for obliterating the conscientious scruples of the working scientists, and for destroying such inhibitions as they may having against rowing into this maelstrom. Let these wise men who have summoned a demoniac sanction for their own private purposes remember that in the natural course of events, a conscience which has been bought once will be bought twice. The loyalty to humanity which can be subverted by a skillful distribution of the administrative sugar plums will be followed by a loyalty to official superiors lasting just so long as we have the bigger sugar plums to distribute. The day may well come when it constitutes the biggest potential threat to our own security. In that moment in which some other power, be it fascist or communist, is in the position to offer the greater rewards, our good friends who have rushed to our defense per account rendered will rush as quickly to our subjection and annihilation.*".
[2512] Z. BAUMAN, *Le coût humain de la mondialisation*, *op. cit.*, p. 27-28.

à cet égard, l'auteur note que « l'interface des terminaux d'ordinateurs a des effets variables sur le sort des différents types de personnes et de population et il existe toujours des gens qui sont, comme autrefois, séparés par des obstacles physiques ou par des distances temporelles (il suffit de penser à une population en période de guerre ou d'attentats) mais cette séparation est encore plus douloureuse qu'auparavant, elle a des retentissements psychologiques encore plus profonds »[2513].

En outre, cette séparation peut également s'opérer dans le monde du tout numérique, notamment dans le monde d'internet, créant, comme il a été vu, des communautés différentes et discriminantes, des fichiers sur les personnes suspectées, des bulles de boucle d'information médiatique fermée voire des *fake news*, des atteintes à la réputation ou à la notoriété, ayant tous un retentissement psychologique et/ou matériel sur la vie réelle des personnes, et « *internet tel que nous le connaissons aujourd'hui est « la machine cybernétique ultime », qui combine à la fois la liberté et le contrôle, et mêle ensemble les êtres humains et les machines à partir d'un idéal de libre circulation de l'information* »[2514].

Aujourd'hui, l'information qui circule dans cet espace « libéré », simulateur sans équivoque d'un espace de liberté, permet à certains, « l'élite en mouvement, maîtresse de la mobilité », d'accéder ainsi littéralement « à la désincarnation, à la nouvelle légèreté du pouvoir » totalement délocalisé et dématérialisé, leur pouvoir « n'étant plus de ce monde » indique Bauman : « *c'est cette expérience de la nouvelle élite, expérience d'un pouvoir non localisé – avec son mélange inquiétant et impressionnant d'impalpabilité et d'omnipotence, de désincarnation et de capacité de transformation du réel – que l'on célèbre communément en vantant « la nouvelle liberté » représentée par le « cyberespace » électronique* », dont une présentation remarquable se retrouve dans « l'analogie entre le cyberespace et la conception chrétienne du Paradis » proposée par M. Wertheim[2515].

Comme le souligne Bauman, il est pragmatiquement évident que dorénavant, « *dans le cyberespace, les corps ne comptent plus, mais le cyberespace compte de manière décisive et irrévocable dans l'existence des corps. Les verdicts prononcés dans le paradis du cyberespace sont sans appel, et leur autorité ne peut en aucun cas être contestée par ce qui se passe sur terre. S'étant assurés d'un lieu, le cyberespace, où ils peuvent tranquillement dicter leurs verdicts, les corps des puissants n'ont pas besoin d'être munis d'armes puissantes ; bien plus,*

[2513] Z. BAUMAN, *Le coût humain de la mondialisation*, *Id.*, p. 31-32, et l'auteur précise « *on peut formuler les choses ainsi : loin d'entraîner une homogénéisation des modes de vie, l'annulation des distances spatio-temporelles a pour conséquence de les opposer.* »
[2514] B. LOVELUCK, *Réseaux, Libertés et Contrôle, op. cit.*, p. 44.
[2515] Z. BAUMAN, *Le coût humain de la mondialisation*, *Id.*, p. 33-34.

contrairement au géant Antée, ils n'ont pas besoin d'un contact avec la terre pour asseoir, fonder ou manifester leur pouvoir »[2516].

Or, le père de la cybernétique voulait justement éviter l'avènement de ces pratiques et techniques et malgré toutes ses mises en garde et sa vision humaniste, la cybernétique, pouvant « être mobilisée à des fins diverses – et parfois opposées », a les capacités « de libérer ou au contraire de mieux assujettir l'individu », mais également « des moyens efficaces pour étendre et automatiser le contrôle social » ; il semble qu'à l'heure actuelle le choix est en quelque sorte tranché[2517].

Dans cette perspective, « *we are in a life in which the world as a whole obeys the second law of thermodynamics : confusions increases and order decreases* »[2518] ; les élites, les gouvernements et les entreprises du monde actuel, tel qu'il a été agencé, voulant à tout prix accroître l'ordre et la commande, tout en maintenant l'accroissement de la confusion, au nom de la sécurité (nationale ou informatique), de la protection (défense nationale ou contre une attaque informatique). L'existence de ce monde implique nécessairement la surveillance, la connaissance, l'anticipation et la prédiction, le tout moyennant les informations et les messages, menant *in fine* à la mise en œuvre simultanée d'une culture cybernétique et d'une culture d'asservissement numérique.

§2. Une Culture d'asservissement numérique

Cette culture de l'asservissement invisible et non tangible, qui découle notamment du pouvoir de la surveillance et de la computation, se traduit principalement par une économie développée autour de l'accès, de l'attention et de la contribution au sein du cyberespace (A) ainsi que par la mise au point d'une surveillance productive et participative (B).

A. L'économie de l'attention et de la contribution

Le monde numérique, avec le web, les réseaux sociaux et le développement exponentiel des algorithmes et technologies de l'information et de la communication, ont libéré l'homme de plusieurs contraintes et fournissent divers moyens et services ainsi qu'une large quantité d'informations parmi lesquels les personnes peuvent choisir : choix d'utiliser ce service au lieu d'un autre, de faire une recherche sur Google au lieu de DuckDuckGo par exemple, choix de

[2516] Z. BAUMAN, *Le coût humain de la mondialisation*, *Ibid.*, p. 35 ; *Cf.* document « Silent weapons for quiet wars - Armes silencieuses pour guerres tranquilles/sans bruit », *loc. cit.*
[2517] B. LOVELUCK, *Réseaux, Libertés et Contrôle, Id.*, p. 42.
[2518] N. WIENER, *The human use of human beings*, *Id.*, p. 36.

lire ou de partager telle information au telle autre, choix dans les moyens et les méthodes de construction, d'accroissement et/ou d'amélioration de sa réputation et de sa notoriété et ainsi de suite. En effet, les concepteurs de ce monde « *partagent l'idée que les informations ne doivent pas être choisies par les journalistes, que les publicités ne peuvent pas être les mêmes pour tous, que les catégories d'appartenance traditionnelles ne représentent pas les individus et que chacun doit pouvoir choisir librement ses « contenus » sans subir le paternalisme des prescripteurs* »[2519], et font la promotion de la vision libérale du cyberespace.

De nombreux sujets ou produits font ainsi chaque jour l'objet d'une attention particulière, que ce soit dans le domaine politique, médical, social, sportif, médiatique, esthétique, intellectuel ou autre ; une attention qui peut devenir virale et générer un buzz autour du sujet du moment choisi, comme les propos d'une célébrité ou d'une personnalité politique, le succès d'une série, d'un film ou d'un jeu vidéo, ou, plus essentiel encore, le harcèlement moral ou sexuel, les ravages ayant affecté la cathédrale Notre-Dame de Paris ou encore la sclérose latérale amyotrophique (SLA). D'apparence, cela n'a que des bénéfices pour la société en ce sens qu'il est possible d'orienter l'attention d'un grand nombre de personnes vers un sujet donné, de les sensibiliser, voire de récolter des dons afin de contribuer au sujet choisi, tout en leur laissant le choix de le faire ; or, « *choice occurs within parameters. Some of these parameters, such as the fact that we need gravity to walk and oxygen to breathe, are relatively fixed. Others, such as the design of legal institutions and technological tools, are slightly more malleable; they are, in other words, themselves the subject of choices* »[2520].

Chacun de ces divers sujets a fait l'objet d'une attention majeure pendant un certain moment et à une période donnée, de sorte qu'il est possible de s'interroger sur la raison pour laquelle tel moment particulier a été dédié à tel sujet particulier ; autrement dit, le bâtiment et les poutres de Notre-Dame devaient depuis longtemps être modifiés et renouvelés mais n'ont fait l'objet d'attention qu'avec le mouvement initié sur les réseaux lorsque le feu est survenu ; les cas de harcèlements ont depuis longtemps été recensés et dénoncés mais n'ont fait l'objet d'une véritable attention qu'avec le mouvement *#MeToo* ; la sclérose latérale amyotrophique est une maladie certes récurrente depuis longtemps mais n'a fait l'objet d'attention particulière qu'avec

[2519] D. CARDON, *À quoi rêvent les algorithmes, op. cit.,* p. 89.

[2520] J. E. COHEN, « Examined Lives: Informational Privacy and the Subject as Object », *loc. cit.,* p. 1393, et l'auteur relève que "[…]. *The debate about privacy and freedom of choice is, in fact, two debates—one about the conditions of choice within a given set of institutions or parameters (here, the evolving, relatively unregulated market for personally-identified data), and one about the parameters themselves. And if "freedom of choice" includes the freedom of self-determination writ large, then it necessarily includes the freedom to use nonmarket means to change the parameters within which markets operate. The question is whether it would be desirable to do so*."

le mouvement du « *Ice bucket challenge* » lancé en 2014. Qu'en est-il alors des autres sujets d'importance égale mais ne générant aucune attention particulière sinon minime, et pourquoi certains sujets ont-ils été sélectionnés au détriment des autres, mais aussi, quelle est la raison pour laquelle des dons ont été récoltés pour certaines causes touchant la société alors qu'il existe un budget public de la recherche ?

Les fonds collectés par le mouvement du *Ice bucket challenge* d'un montant total de 98,2 millions de dollars en 2014 correspondait-il à une augmentation particulière de la maladie ou du taux de mortalité dû à celle-ci, ou découle-t-il simplement de l'attention qui lui a été portée par le bais de ce mouvement qui consistait à défier des personnes à se jeter un seau de glaces et/ou faire un don à l'association SLA, grandement véhiculé par Facebook et ses nombreuses applications. Ce mouvement a certes permis de récolter des fonds pour les recherches et les traitements de cette maladie, des fonds d'ailleurs bien nécessaires pour ce faire, mais il n'en demeure pas moins qu'un dollar versé au fonds des donations SLA est un dollar refusé à la prévention du paludisme, à la recherche sur le cancer, au traitement et à la prévention du VIH, ou encore à la recherche sur les maladies cardiaques, qui à terme finissent par être subventionnés par les grandes industries pharmaceutiques ; le financement public de la recherche va se rétrécissant particulièrement face au budget de la défense toujours croissant, les sources privées profitant de ce déséquilibre et prévoyant des financements pour la recherche. C'est en fin de compte la publicité et ses nouveaux pouvoirs qui font toute la différence et qui orientent l'attention des individus, en s'appuyant notamment sur le récit de ceux qui souffrent tout en procurant l'espoir que le mouvement et les contributions apportées pourraient pousser la recherche à son point culminant et « sauver » (des vies, un bâtiment, une communauté, etc.). À l'heure actuelle, il semble bien que la cause qui produit la campagne publicitaire la plus accrocheuse, la plus mignonne, la plus amusante ou la plus intelligente est celle qui génère le plus de soutien financier grâce à l'attention qui lui est accordée. Dans le cas du mouvement ayant généré des sommes astronomiques pour l'association américaine traitant de la SLA, aucune des vidéos postées, malgré toutes les bonnes intentions, n'expliquait les raisons pour lesquelles cette maladie était si affaiblissante et mortelle ni même pour quels bénéfices, ou quelles raisons, l'argent donné sera dépensé[2521]. La société, dans son ensemble, n'a finalement pas discuté des impératifs ayant poussé à choisir ce sujet en particulier parmi tant d'autres, elle a juste suivi le mouvement et sa popularité. La plupart des vidéos partagées ne faisaient même aucune mention du sujet ayant initialement porté ce mouvement, et devinrent ainsi des

[2521] S. VAIDHYANATHAN, *Anti-social media, op. cit.*, p. 78-79.

spectacles pour le plaisir du spectacle : « *it was just the most fun to think about – even though the thinking remained at the level of watching a person get soaked in cold water* » caractérisant le fait que « *attention is the only currency that matters* »[2522].

Le web, perçu généralement comme un espace libre et ouvert où la plupart des services sont gratuits, porte la promesse d'un élargissement de l'offre d'information mais aussi de l'offre de consommation par la panoplie d'informations, de services, de techniques et de produits mise à la disposition des personnes. Or, *in concreto*, tout tend à montrer plutôt qu'il existe une surconcentration de l'attention autour de certaines informations particulières, gagnant une immense et soudaine popularité largement facilitée par les techniques de marketing, de ciblages publicitaires et de coordinations virales qui, finalement, orientent insidieusement le public vers certains produits, certaines informations, certains sujets ou certains services en fonction de leurs préférences, leurs habitudes et leurs comportements, révélant *in fine*, l'importance de l'aspect comportemental et le fétichisme entourant les données[2523]. Les mesures d'audience, les compteurs de nombre de vues ou de nombre de partage ou de nombres de commentaires ou encore de nombre de « like » participent pleinement à ce mouvement de coordination virale de l'attention, contribuant à la production des « pics d'attention » et à la fabrication de la popularité.

L'attention représente une chose rare, limitée par le temps, mais facile à détourner ou à "voler" : un mouvement, un flash, un bruit, le passage d'une mouche dans la périphérie du champ de vision pouvant facilement distraire un individu et détourner son attention. Or, l'attention nourrit la pensée humaine, pensée qui fonctionne en flux, suivant un même courant d'idées ; et si le flux de la pensée est rompu, le pouvoir de cette dernière diminue. Cependant, dans le monde numérique, il apparaît que l'attention est aussi précieuse et porteuse de valeur ajoutée, ou peut-être surtout, quand elle est brève et peu profonde. En effet, les individus sont plus susceptibles d'être convaincus de cliquer sur un lien sur une page web, une application ou un courriel si leur attention est superficielle et de courte durée. Les annonceurs savent que pour vendre quelque chose, ils doivent attirer l'attention des personnes ne serait-ce que pendant un court moment, tout en sachant que pendant qu'ils la détiennent, d'autres essayent de la détourner et de distraire les personnes concernées pour les attirer vers leurs propres produits ou services.

Ainsi, un écosystème médiatique devenant plus pollué et plus fracturé se met en œuvre au sein duquel chaque acteur expérimente avec de nouvelles conceptions et de nouveaux designs, des stratégies de ciblage et de marketing, et des stimuli pour attirer l'attention et la retenir assez

[2522] S. VAIDHYANATHAN, *Anti-social media, Id.*, p. 79.
[2523] *Cf.* p. 380 et 402.

longtemps pour convaincre le client potentiel de passer à l'action et consommer, en achetant, en partageant, en « likant » ou en commentant, mais, en ce qui concerne Google et Facebook, entités dominantes dans cet écosystème, il y a beaucoup moins de tentatives de persuasion puisque « the game is all about matching » ; à terme, cet écosystème devient déshumanisant : « *the unrelenting drive to surveil and tag complex consumers and then demand slivers of their attention in hopes that they engage in a series of transactions is more than distracting and exhausting. It's dehumanizing. It treats us each as a means to a sale rather than as ends in ourselves* »[2524].

Autant l'attention est rare, dans la société et l'économie de l'information actuelles, autant l'information est abondante ; en conséquence, la gestion et le filtrage d'informations sont devenus des fonctions importantes et précieuses porteuses de grandes valorisations. Ainsi, Google, Facebook et les autres géants du web aident les personnes quotidiennement à gérer la masse d'information à leur disposition en accomplissant la tâche de décider ce qui est précieux, a de la valeur ou est intéressant pour tout individu concerné, processus accompli en surveillant et en collectant une masse de données concernant les comportements, habitudes et préférences de celles-ci « *to ensure we see ads* [… messages and information that] *algorithms judge to be "relevant" to us* »[2525], puis de leur laisser « le choix » dans les propositions affichées, générant *ipso facto* le développement de l'économie de l'attention et celui d'industries entièrement dévouées à la capture de l'attention, les « attention brokers » et l' « attention market »[2526]. En effet, « *lorsque l'offre d'information abonde, c'est désormais l'attention des publics qui constitue un bien rare et convoité* »[2527]. Paradoxalement, c'est le fait de monétiser l'attention captée par ces géants, notamment Google et Facebook, qui paie pour la main-d'œuvre et les technologies leur permettant de filtrer si efficacement le flux massif d'informations.

En outre, la plupart des services et des produits (en termes de création) et des informations proposées sur le web, depuis son avènement, suivaient l'idée de liberté que celui-ci promettait

---

[2524] S. VAIDHYANATHAN, *Anti-social media, Id.*, p. 87.
[2525] S. VAIDHYANATHAN, *Anti-social media, Ibid.*, p. 84.
[2526] T. WU, « Attention Brokers », NYU Law, septembre 2015, p. 2 "*The Attention Broker (sometimes called an Attention Merchant) is a reseller of human attention. It attracts attention by offering something to the public (entertainment, news, free services and so on), and then reselling that attention to advertisers for cash. Examples of pure attention brokers include television networks, some web companies, and some newspapers – entities sometimes referred to as "advertising supported media." The broker is a specialized form of a two-sided market intermediary, […]. Its activities are critical to the operation of attention markets, for it is its business model that creates much of the competition for attention […]. Attention Brokers are not the only intermediary. Publishers are businesses that sell consumers entertainment products, for money, that consume attention as well (film studios and book publishers are two examples).*": http://www.law.nyu.edu/sites/default/files/upload_documents/Tim%20Wu%20-%20Attention%20Brokers.pdf
[2527] D. CARDON, *À quoi rêvent les algorithmes, Id.,* p. 93.

en les proposant « gratuitement », étant donné que « *"free" meant digital content could be cost-free and able to circulate unfettered* »[2528]. Le gratuit ne pouvant payer pour les services, les technologies et la main-d'œuvre, la publicité apparut comme source de revenus, créant l'industrie des publicités ciblées et des techniques de marketing personnalisées et poussant, parallèlement, les industries classiques, qui dépendaient depuis leur mise en place des ventes unitaires ou des prix d'admission, à réduire leurs prix et à chercher d'autres sources de revenus et d'autres moyens de rester compétitifs sur le marché, « *thus competing against each other not only for the marginal cash in a family's entertainment budget but also for their scarce free time* »[2529].

L'économie de l'attention a également entraîné le mouvement du *personal branding* susmentionné et de l'importance rattachée à la e-réputation ou à la e-notoriété, que ce soit celle d'une entreprise, d'une association, d'une université, d'un produit, d'un service, d'une célébrité, d'une personnalité politique ou publique, ou encore d'un individu[2530]. Et l'ensemble de ces industries, comme il a été vu pendant cette étude, fonctionne pour survivre et avoir une place sur le marché par le biais des études comportementales, du profilage et des dossiers numériques unifiés[2531], ayant pour socle les données à caractère personnel.

La vie privée, entendue dans son sens le plus large comprenant les données personnelles, la dignité, l'auto-détermination ou encore l'attention par exemple, devient progressivement une valeur échangeable, ce qui est, selon les promoteurs de ces industries, en première ligne les GAFAM, nécessaire pour pouvoir offrir une large gamme de choix aux consommateurs. Comme le souligne la Professeure Cohen, « *the "attention economy," we are told, demands personal profiling as a survival tactic. Vendors that are unable to exploit consumer profiles to target their products and services effectively will be forced, instead, to discontinue narrowly-targeted product offerings and/or charge higher prices for continued offerings. The effects, we are told, will be especially stark where targeted advertising has traditionally supported free or near-free content—e.g., in the news and broadcast industries. Yet all other things being equal, a prohibition on individualized profiling (or on nonconsensual profiling) will not change the fact that businesses compete to provide products and services that consumers prefer, and that digital networks and search tools reduce the costs of niche competition* »[2532] ; ce qui devrait

[2528] S. VAIDHYANATHAN, *Anti-social media, Id*., p. 81.
[2529] S. VAIDHYANATHAN, *Anti-social media, Ibid*., p. 81.
[2530] *Cf.* p. 120 et s.
[2531] *Cf.* p. 390 et 430.
[2532] J. E. COHEN, « Examined Lives: Informational Privacy and the Subject as Object », *Id.,* p. 1400.

alors justifier la capture de l'attention, la compétition pour ce faire, et l'échange monétaire qu'elle induit ; le tout reposant largement sur les masses de données et le pouvoir des calculs.

Par ailleurs, l'idéologie qui se trouve à la base de cette économie de l'attention et de la contribution est celle qui structure également les expériences individuelles et les attentes culturelles constamment en quête de buzz et de popularité. Il suffit de penser à l'influence des différentes célébrités ou micro-célébrités, qui représentent une minorité, sur la vie quotidienne des individus, qui sont une majorité : des humoristes sur les chaînes YouTube, des discours politiques partagés sur les réseaux, des blagues ou des défis (tel que le *Ice bucket challenge*) improbables, versatiles et flottants, des promotions de produits de beauté sur les réseaux, par exemple ; l'ensemble générant un impact indéniable sur les individus-spectateurs et leurs quotidiens.

En effet, ces célébrités, qu'elles soient issues du monde de la politique, du sport, des médias, du commerce, de la science, du divertissement ou du spectacle, « *ont pour rôle de manifester leur univers, dont le caractère essentiel consiste précisément à être regardé, à être regardé par beaucoup de gens, partout dans le monde […]. Quel que soit le sujet dont elles parlent, elles transmettent un message, celui d'une certaine façon de vivre. Leur vie, leur mode de vie* »[2533] qui, souvent, fait la promotion d'un certain sujet, service ou produit particulier. Les effets de ces messages sont manifestes de nos jours sur leurs spectateurs, ces derniers voulant continuellement gagner en popularité et en notoriété, suivre les mouvements viraux et les dernières tendances du moment par peur de manquer quelque chose, le fameux FOMO (*Fear Of Missing Out*) qui se met en place, ou par peur d'être exclu, stigmatisé, rejeté ou discriminé ou de tout autre conséquence pouvant en découler. La fabrication de la popularité, notamment numérique, privilégie ainsi « *la synchronisation, le mimétisme et l'obsolescence programmée* », et alimente la nécessité primordiale d'avoir un « *appareillage de supervision et de mesure […] introduit de plus en plus profondément dans la conception des informations et des messages* »[2534].

Par conséquent, les individus se comportent de plus en plus comme des « marques », améliorant leurs réputation et notoriété numériques ainsi que leur valorisation de soi[2535], moyennant les techniques et dispositifs précités, en vue de se promouvoir, constamment et exhaustivement, à travers, entre autres, Facebook, Twitter, YouTube ou Instagram. Pourtant, « *tous les individus ne disposent pas des mêmes ressources sociales pour profiter des espaces de valorisation de*

[2533] Z. BAUMAN, *Le coût humain de la mondialisation, op. cit.,* p. 85.
[2534] D. CARDON, *À quoi rêvent les algorithmes, Id.,* p. 92.
[2535] *Cf.* p. 120 et s.

soi. La « bulle » dans laquelle Facebook enferme ses utilisateurs censure moins des contenus selon les convictions des utilisateurs qu'elle n'oppose les « individus par excès », « individus individualisés » qui font feu de tout bois pour faire briller leur réputation, et les « individus par défaut », qui se trouvent relégués à distance des informations d'actualité »[2536].

Cela dit, les contextes sociaux actuels indiquent et signalent continuellement à la population, et particulièrement à la jeune génération, l'importance de se promouvoir et de gagner en popularité, pour devenir, dans leur contexte social, une micro-célébrité et, par la suite, une macro-célébrité et atteindre la richesse, le pouvoir et la célébrité, et donc le bonheur et une bonne vie ; les personnes non célèbres étant rarement citées comme des « success stories », des champions, ou des entrepreneurs de renommés. Un des summum de la lutte pour l'attention, prometteurs de richesse et de gloire, notamment dans les pays anglo-saxons, se manifeste dernièrement avec les TED Talk : « *purposely informal and limited to eighteen minutes, these punchy, pithy talks are meant to inspire and entertain. They don't invite deliberation or debate. They don't demand immersion or even background reading. They are capsules of knowledge. To deliver a TED Talk, however, is the apex of self-branding. And, not coincidentally, one of the major ways people discover TED Talks and other self-promotional videos is through Facebook* »[2537].

Finalement, cela aboutit à la multiplication d'espaces (numériques ou physiques), tous quémandant l'attention, où il n'existe plus vraiment de marqueurs permettant de distinguer si les éléments destinés à persuader – les services, produits, publicités, personnalités ou sujets – sont destinés à convaincre à faire quelque chose, tel que voter, acheter, faire un don ou jouer, ou plutôt à divertir ou à informer ; peu d'espaces échappant actuellement aux demandes d'attention, que ce soit dans le cyberespace, dans les écoles, dans les métros ou panneaux d'affichage par exemple. Et, paradoxalement, ces mêmes espaces imposent une vision sociale et des attentes culturelles, exerçant une pression sociale sur les individus qui finissent par choisir une certaine performance plutôt qu'une autre pour construire leur identité, représentation et affiliation, menant à ce que chaque "profil" soit constamment soigné et peaufiné pour se faire une bonne publicité, avoir une bonne e-réputation et gagner en popularité, « l'attention attirant l'attention »[2538].

Une des techniques les plus employées à l'heure actuelle se traduit par le raffinement des profils Instagram mais surtout des profils Facebook : « *Facebook profiles are advertisements for*

[2536] D. CARDON, *À quoi rêvent les algorithmes, Ibid.,* p. 99.
[2537] S. VAIDHYANATHAN, *Anti-social media, Id.*, p. 82.
[2538] D. CARDON, *À quoi rêvent les algorithmes, Id.,* p. 93.

ourselves. Facebook sorts users' profiles by affiliation and interest, and then more dynamically based on interactions and the flow of "engagement". And user's feed clues into Facebook's algorithms that amplify the process further, creating a constantly churning lattice of affiliations » ; par conséquent, « *the more time we spend grooming our self-presentation and declaring our tribal affiliations, the more we grow acculturated to this habit. It becomes a cultural norm. It assumes the soft power of ideology. Companies that desire to break through the flows and distractions all around us find it necessary to detect and play to those affiliations* »[2539]. Ce qui concrétise par là même le pouvoir des algorithmes, du calcul, des traitements, des corrélations, des interconnexions, des études comportementales, du profilage et des pratiques computationnelles de plus en plus autonomes de façon générale, le tout facilité et véhiculé par la surveillance généralisée, ainsi que le succès des nombreuses industries centrées sur les personnes fonctionnant par le biais de ces moyens, techniques et pouvoirs, et concrétise de surcroît la nouvelle norme culturelle et l'économie émergentes construites autour de l'accès, de l'attention et de la contribution ; l'ensemble donnant l'impression de concrétiser la liberté de choix, la liberté de construction personnelle et la liberté d'expression.

En effet, comme le note le Professeur Cardon, « *les calculateurs prétendent libérer la société de la « tyrannie du centre ». Pourtant, cette émancipation, par l'intermédiaire de mesures qui s'exercent sous la tutelle des intérêts économiques, continue de produire des effets de centralité d'autant plus forts qu'ils se sont largement émancipés des cadres nationaux pour devenir globaux. Le paradoxe de la société des calculs est qu'elle amplifie les phénomènes de coordination de l'attention et de hiérarchisation du mérite, tout en permettant aux individus de se sentir de plus en plus libres de leurs choix. En fait les calculateurs donnent à la société les moyens de reproduire d'elle-même les inégalités et les hiérarchies qui l'habitent* »[2540].

La « vision libertarienne »[2541] qui accompagne le cyberespace, offrant la liberté de choix aux individus mais aussi une sélection de techniques et de moyens pour accroître leur réputation, leur notoriété ou leur niveau de célébrité, orientés vers une multitude de tendances dans des secteurs aussi divers que variés, a permis de mettre l'accent sur l'importance des « clicks », augmentant la popularité d'une personne, d'un service, d'un produit ou d'un sujet, et donc sur l'importance de l'attention afin de générer ce click, like, nombres de vues, de partages, voire de commentaires ; or, « *[…] like "property," "choice" has become a category with a specific,*

[2539] S. VAIDHYANATHAN, *Anti-social media, Id.*, p. 93.
[2540] D. CARDON, *À quoi rêvent les algorithmes, Id.,* p. 91.
[2541] D. CARDON, *À quoi rêvent les algorithmes, Ibid.,* p. 90.

culturally determined meaning. "Freedom of choice" means "choice in markets", and means only that »[2542].

En outre, cette vision du monde numérique, fournit *de facto* à la société l'impression de s'auto-organiser moyennant les biens et les services numériques et les technologies de l'information et de la communication qui se fondent, comme il a été vu, sur des pratiques et des méthodes issues de la cybernétique[2543]. Dans ce contexte, « *en alignant leurs calculs personnalisés sur les comportements des internautes, les plateformes ajustent leurs intérêts économiques à la satisfaction de l'utilisateur. Sans doute est-ce à travers cette manière d'entériner l'ordre social en reconduisant les individus vers leurs comportements passés que le calcul algorithmique exerce sa domination. Il prétend leur donner les moyens de se gouverner eux-mêmes ; mais, réduits à leur seule conduite, les individus sont assignés à la reproduction automatique de la société et d'eux-mêmes. Le probable préempte le possible. Paradoxalement, c'est au moment où les internautes s'attachent, par leurs représentations, leurs ambitions et leurs projets, à se penser comme des sujets autonomes et libérés des injonctions des prescripteurs traditionnels que les calculs algorithmiques les rattrapent, par en dessous si l'on peut dire, en ajustant leurs désirs sur la régularité de leurs pratiques* »[2544].

B. La surveillance productive et participative

De façon générale, toute époque produit de "nouvelles" technologies, comme ce fut le cas avec les imprimeries, les boussoles ou les vaccins par exemple, mais la nouveauté de cette dernière époque, celle du développement exponentiel du web, des données et des technologies de l'information et de la communication notamment, réside dans l'accélération surprenante des innovations et le renouvellement constant des représentations et des modalités d'interactions, bouleversant promptement, et de manière également innovante, l'organisation sociale. Inscrites dans une optique libérale, ces nouvelles technologies proposent la libération de l'information des frontières politiques ou médiatiques en permettant à tout citoyen de communiquer de manière instantanée sur n'importe quel sujet, y compris des informations ayant la capacité de

[2542] J. E. COHEN, « Examined Lives: Informational Privacy and the Subject as Object », *Id.,* p. 1399, et l'auteur indique que "*In a provocative essay on the evolution of governance structures, Larry Lessig observes that we have lost faith in other, more traditional institutions of governance. But it seems to me that the phenomenon is cognitive as much as existential: We conceive of "freedom" in literal, almost physical terms, as a function of direct or subjective constraints on behavior. Law, of course, does not directly constrain in most instances; nor, I would argue, does it constrain more directly than price in many cases. Yet law operates in terms of prohibition, while markets operate in terms of possibility. And so liberty has come to mean freedom from laws (other than economic ones) rather than freedom that laws might guarantee. It was not always thus*."

[2543] *Cf.* p. 557 et s.

[2544] D. CARDON, *À quoi rêvent les algorithmes, Id.,* p. 88.

remettre en cause le pouvoir politique ; il suffit de penser aux mouvements ayant eu lieu lors du « printemps arabe » et leur propagation vers d'autres pays et d'autres causes[2545]. Quelles qu'en soient les conséquences, ces technologies « *peuvent ainsi nourrir des formes inédites d'émancipation démocratique, mais elles alimentent aussi le souverainisme sécuritaire, en contribuant à la surveillance numérique* »[2546].

Les nouvelles technologies de l'information et de la communication, porteuses de promesses d'émancipation et de liberté, semblent ainsi avoir libérer l'homme de nombreuses contraintes, qu'elles soient liées au travail, au transport, au logement, à la liberté d'expression et de communication, à l'interaction et au partage instantanés, technologies véhiculées par les plateformes et interfaces numériques en développement constant. Des plateformes telles que Uber, Deliveroo, Blablacar ou encore Airbnb, fonctionnant principalement sur l'offre de services innovants mais surtout à la demande des utilisateurs-consommateurs, en fournissent une parfaite illustration et participent à ce qui est désormais connu comme « l'économie à la demande » ou « économie de la consommation » en ce sens que, avec ces nouvelles technologies et les moyens et outils qu'elles fournissent comme la personnalisation et l'immédiateté, il y a beaucoup plus de valeur à extraire de la consommation que de la production en elle-même, cette nouvelle économie modifiant et renouvelant par conséquent l'équilibre dynamique entre l'offre et la demande, qui fonctionnait auparavant sur la solvabilité de la demande[2547]. Comme le souligne le Professeur Pasquale, « *the firms that order the Internet and*

[2545] « *Les soulèvements arabes, communément appelés Printemps arabe (al-Thawrat al-Arabiyyah) consistent en des processus complexes […] : La première vague de révoltes antigouvernementales dans les pays arabes a éclaté en décembre 2010 en Tunisie, puis une deuxième est apparue en Égypte deux mois plus tard. Elles se sont ensuite propagées dans les sociétés arabo-musulmanes d'Afrique du Nord et du Moyen-Orient. […]. La rapidité de la diffusion des soulèvements arabes* [ayant été entre autres] *le résultat de l'usage des technologies de communication moderne en ligne par la jeunesse. […]. Ces révolutions démocratiques qui ont eu lieu dans les pays du Moyen-Orient et d'Afrique du Nord ont souligné l'incroyable courage et le sens de la dignité des jeunes qui en ont pris la tête. Il s'agissait de révoltes spontanées impliquant toutes les classes sociales. Elles ont inspiré divers mouvements dans d'autres pays, comme celui des Indignados en Espagne (2011-2012), les manifestations portugaises et grecques ou le mouvement Occupy Wall Street aux États-Unis. Bien que ces mouvements ne reposent pas exactement sur les mêmes demandes, on peut néanmoins noter des parallèles quant aux formes de mobilisation sociale, l'utilisation de technologies modernes comme les médias sociaux et dans les méthodes de protestation pacifique (al-Mouthawara al Silmiyya). Cependant, les slogans étaient différents : les révoltes arabes ciblaient des régimes considérés comme autoritaires, répressifs et corrompus, là où les Indignados réclament plus d'équité sociale, d'efficience gouvernementale et d'opportunités. […]* » : E. GELABERT, « Le Printemps arabe en perspective », *In* Cahiers de l'action Vol. 39, N° 2, 2013, p. 11-17.

[2546] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, op. cit.,* p. 83.

[2547] G. RENOUARD, « Comment l'économie à la demande remodèle la société », L'Atelier BNP Paribas, Archive, Mars 2016 : « *Désignant une activité où des entreprises utilisent les nouvelles technologies pour apporter aux consommateurs des biens ou services de manière quasi-immédiate, l'économie à la demande connaît des taux de croissances fulgurants* » : https://atelier.bnpparibas/smart-city/article/economie-demande-remodele-societe ; A. FILEV, « L'économie à la demande : un défi pour l'efficacité opérationnelle », Journal Du Net, publié le 07/12/2017 : « *L'économie à la demande est en effet au croisement de quatre tendances ou transformations majeures :- L'ultra connectivité permanente, facilitée par l'explosion des usages mobiles,- Le développement rapide des technologies logistiques de proximité, des logiciels de support client et de l'ultra*

direct the flow of capital have outsized influence in Washington. For better or worse, they also increasingly determine the value and visibility of labor, companies, and investments. But they do all this in the shadows »[2548].

Pour fonctionner et produire de la valeur, ces applications à la demande dépendent de la collecte ou de l'extraction, de la circulation et du traitement d'une large quantité de données, ravivant *de facto* de nombreux enjeux relatifs à la protection des données, ou celle de la vie privée, « *avec toutes leurs implications potentielles de surveillance et de contrôle algorithmique sur les producteurs de valeur* »[2549]. En effet, la surveillance et la collecte des données des usagers sont au cœur du fonctionnement de ces plateformes numériques, une surveillance qui finalement « *conduit tout autant à remettre en cause la « liberté » qu'elle affirment leur garantir* »[2550], et les informations recueillies représentent le socle de la captation et de la création de valeur.

Ces informations peuvent être également monétisées à d'autres fins, telle que le ciblage publicitaire, contribuant à l'augmentation de la valeur captée et au capital de l'entreprise gérant l'application en question ; l'ensemble de ces informations étant produites par les usagers mêmes, chauffeurs et passagers, livreurs et clients, propriétaires et locataires, devenant des usagers-travailleurs et participant volontairement, de manière consensuelle, à cette surveillance. Or, « *participatory surveillance may be consensual and may downplay coercion, but it is in the end about discipline and integration, not about rebellion or resistance. And differentiation and fragmentation serve precisely these purposes* »[2551].

Le fonctionnement de ces plateformes concrétise ainsi l' « *algorithmic and data-driven management* »[2552], une méthode de gestion du travail fondée sur les données et les algorithmes

---

personnalisation des offres,- Le développement du cloud, la simplification des paiements électroniques et l'essor du travail indépendant facilitant la décentralisation des activités,- La demande croissante des consommateurs pour une nouvelle génération de services rapides, efficaces et pratiques. Ces évolutions bouleversent violemment tous les secteurs économiques, à commencer par les acteurs traditionnels, même les plus gros. […] » : https://www.journaldunet.com/management/expert/68119/l-economie-a-la-demande---un-defi-pour-l-efficacite-operationnelle.shtml

[2548] F. PASQUALE, *The black box society, op. cit.*, p. 217.

[2549] A. A. CASILLI, *En attendant les robots : Enquête sur le travail du clic*, Ed. du Seuil, Coll. La couleur des idées, 2019, p. 106.

[2550] A. A. CASILLI, *En attendant les robots, Id.*, p. 259, où l'auteur indique « *L'application Xora, par exemple, organise l'emploi du temps et les trajets des « travailleurs mobiles » qui l'utilisent. Mais elle enregistre aussi leurs déplacements et habitudes à tout moment de la journée, à tel point qu'elle a pu être comparée à un bracelet électronique.* »

[2551] R. WHITAKER, *The end of privacy, op. cit.*, p. 150.

[2552] M. K. LEE, D. KUSBIT, E. METSKY et L. DABBISH, "Working with machines: The impact of algorithmic and data-driven management on human workers", *In* B. Begole et J. Kim (dir.), *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, New York, ACM, 2015, p. 1603-1612: "*We call software algorithms that assume managerial functions and surrounding institutional devices that support algorithms in practice algorithmic management. Algorithmic management allows companies to oversee myriads of workers in an optimized manner at a large scale, […]".*

qui surveillent, dirigent et contrôlent le travail ; l'application Uber, par exemple, en représente une incarnation parfaite et démontre son succès. Précisément, la surveillance et le contrôle de leurs usagers-travailleurs constituent deux des fonctions principales de cette application dans le but de coordonner et gérer ses services et ses effectifs décentralisés, en évaluant la vitesse et la performance des véhicules de transport, en localisant les chauffeurs, leurs véhicules et les demandes clientèles, en déterminant et en démarquant les chauffeurs travaillant pour des services concurrents de ceux exclusifs, ou encore en attribuant les trajets selon des critères bien définis certes, non explicités toutefois auprès des conducteurs ou des passagers. *In fine*, plusieurs facteurs et critères jouent dans le fonctionnement du service mais demeurent finement et intensément surveillés, gérés et contrôlés par les algorithmes qui sont, aux yeux de leurs utilisateurs-travailleurs, opaques.

Cette opacité, néanmoins, ne diminue aucunement les tâches de participation, d'attention et de contribution requises pour le fonctionnement de ces interfaces à la demande ; l'ensemble de ces tâches produisant des données récoltées, surveillées et contrôlées, même lorsque l'usager-travailleur n'utilise pas directement le service en question. En effet, ces applications surveillent et collectent continuellement les données de leurs usagers (chauffeurs, livreurs, propriétaires et clients) afin de les utiliser de différentes manières : ces données et les analyses comportementales qu'elles permettent et les connaissances qu'elle produisent peuvent alors être monétisées ou partagées avec d'autres plateformes, utilisées pour améliorer les offres, produits et services, ou encore employées à des fins d'automation pour développer de nouvelles solutions ou améliorer la performance de leurs algorithmes et systèmes moyennant de nombreuses mises à jour ; le tout caractérisant l'aspect productif de la surveillance omniprésente de ces applications.

De plus, une autre finalité bien spécifique à Uber réside dans l'emploi des données pour déterminer l'équilibre entre offre de service par les conducteurs et demande par les passagers, qui requiert un algorithme de tarification dynamique, aussi connu comme le « *surge*

pricing »[2553], dont se vante Uber qui en est propriétaire[2554], illustrant également la surveillance productive et participative qui s'agence.

Par ailleurs, comme c'est le cas avec tous les usages numériques actuels, l'aspect social et les dynamiques réputationnelles sont d'une grande importance et d'une grande influence pour ces plateformes, étant donné que pour avoir du succès, les usagers-travailleurs de celles-ci doivent continuellement soigner leurs profils, images et présentations de soi, maintenir de bonnes relations, une bonne conduite et des comportements corrects pour la bonne gestion du score de réputation et de la performance (les *likes*, évaluations, étoiles, notations, nombre de *followers*, de courses, de partages, de vues, de contacts, etc.), permettant par là même de s'autoévaluer et de s'autoréguler. Ce sont donc des métriques de performance qui quantifient l'effort productif des usagers-travailleurs, et qui sont souvent associées à des mécanismes de compétition ou de ludification, dit aussi de gamification[2555], caractérisant les méthodes de contrôle de ces

---

[2553] Uber, « How surge pricing works »: "*[…] surge pricing helps quickly connect each person who needs a ride with a driver to help them get to their destinations*.": https://www.uber.com/en-FR/drive/partner-app/how-surge-works/ ; U. M. DHOLAKIA, "Uber's Surge Pricing: 4 Reasons Why Everyone Hates It", government technology, 27/01/2016 & "Why Do Consumers Hate Uber's Surge Pricing?", Rice-Kinder Institution for Urban Research, The Urban Edge, 27/01/2016: *"The controversial practice of surge pricing used by high-profile rideshare company Uber is based on this logic of fairness. The idea behind surge pricing is to adjust prices of rides to match driver supply to rider demand at any given time. During periods of excessive demand when there are many more riders than drivers, or when there aren't enough drivers on the road and customer wait times are long, Uber increases its normal fares. They do this with a "multiplier" whose value depends on scarcity of available drivers. On a Friday night in midtown Houston for example, the surge fare may be twice the normal fare (in which case the multiplier is two). When surge pricing is in effect, Uber's riders are informed that their fares will be higher, and they have to agree to pay the amount. Only then is a driver dispatched to pick them up*.": https://www.govtech.com/applications/Ubers-Surge-Pricing-4-Reasons-Why-Everyone-Hates-It.html & https://kinder.rice.edu/2016/01/27/uberhatesurgepricing/#.Vqkf5_krLct

[2554] A. A. CASILLI, *En attendant les robots, Id.*, p. 109.

[2555] M. BONENFANT et S. GENVO « Une approche située et critique du concept de gamification », *In* Revue Sciences du jeu, *Questionner les mises en forme ludiques du web : gamification, ludification et ludicisation*, N° 2, 2014, points 1-4 : « *Dans la recherche académique anglophone, dans le milieu du markéting et dans les pratiques professionnelles de conception de jeux, le concept de gamification s'est rapidement diffusé. Parfois traduit en français par le terme de « ludification », il est défini par Zichermann et Cunningham (2011) comme un processus qui consiste à user de l'état d'esprit et de la mécanique du jeu pour résoudre des problèmes et faire participer les usagers, les principes de base du design de jeu étant appliqués dans différents contextes. […]. Un des premiers contextes dans lequel l'expression gamification a fait son apparition est celui du markéting alors qu'elle y est présentée comme une « solution miracle » pour les compagnies. Il faut ainsi comprendre qu'au cœur de la gamification se trouve la question de la motivation et de « l'engagement » d'un individu dans diverses activités qui reposent sur l'emploi « des structures de récompense, des renforcements positifs et boucles de feedback subtiles en même temps que des mécanismes comme des points, des médailles, des niveaux, des challenges et des tableaux de leaders ». Il faut cependant mentionner que Gabe Zichermann et Chistopher Cunningham donnent un sens particulier à la notion d'engagement dans leur définition de la gamification, ce qui permet parallèlement d'en saisir certaines finalités : « le terme "engagement", dans un sens "business", indique la connexion entre un consommateur et un produit ou un service […]. Plutôt que l'idée antique de pousser le consommateur à "acheter plus", engager l'utilisateur afin de générer des revenus est le modèle markéting du futur. Dit plus simplement, l'engagement ne suit pas les revenus. À la place, après l'engagement, les revenus suivent ». Dans ce contexte, l'engagement ne concerne pas l'individu ou le citoyen, mais bien le consommateur qui (s')investit auprès d'une entreprise par le biais de stratégies ludiques. Initialement, il s'agit essentiellement de développer à travers le concept de gamification de nouvelles techniques de commercialisation pour renforcer la fidélisation des consommateurs/utilisateurs/joueurs. […]. Or, si la gamification est particulièrement présente dans le markéting, elle apparaît dans d'autres domaines. […] tout*

plateformes. Ce qui peut, en outre, entraîner des impacts ou des sanctions sur ces utilisateurs-travailleurs, un usager ayant une mauvaise note, un mauvais score ou une mauvaise réputation pouvant être recalé ou refusé, voire exclu de l'application. Par conséquent, à travers les méthodes de surveillance et de contrôle employées sur leurs usagers, les dispositifs algorithmiques de ces plateformes semblent bien exercer, également, « *un pouvoir de discipline d'autant plus efficace que leur productivité est contrôlée en temps réel* »[2556].

Ce contexte peut, de fait, produire des nouvelles formes de discriminations, la discrimination numérique[2557], ces applications reposant sur l'extraction et la mise en relation d'informations qui portent non seulement sur les produits, mais aussi sur les individus qui les vendent et qui les utilisent, et engendre, particulièrement, l'asservissement des utilisateurs, « *la subordination des usagers-travailleurs des plateformes* [qui] *ne s'exprime pas seulement par les sollicitations incessantes qu'ils reçoivent, mais aussi par l'enregistrement et l'évaluation constante de leurs comportements* »[2558], voire « *une subordination à la seconde près, via un contrôle permanent et en temps réel grâce aux TIC, d'autant plus efficace qu'il est invisible et automatisé. Une sorte de « sur-subordination » avec des obligations de résultats* »[2559].
De même, le contexte de ces plateformes et de leurs fonctionnements, basés fondamentalement sur la surveillance qui permet le contrôle et la gestion souhaitée, mène à un processus de « négociation collective itérative et dialectique » entre les données relevant du privé ou du public, créant un nouveau paradigme au sein duquel la vie privée n'est plus une prérogative individuelle mais une négociation collective[2560] qui semble résulter « *d'un aménagement relationnel, qui prend en compte des éléments intersubjectifs et se modèle selon les impulsions venant des personnes avec lesquelles un individu interagit* »[2561] ; mais, de façon pragmatique, c'est plutôt une négociation collective sur la vie privée de chaque individu-utilisateur « *dont l'issue dépend des rapports de force qui opposent les usagers-travailleurs aux plateformes* »[2562]. Plus encore, la captation des données émises par les applications mobiles, les

contexte serait potentiellement adapté à la gamification, puisque ce sont les « mécanismes » du jeu – et non son thème – qui vont procurer du « fun ». » ; Disponible en ligne : https://journals.openedition.org/sdj/286
[2556] A. A. CASILLI, *En attendant les robots, Id.*, p. 260.
[2557] A. A. CASILLI, *En attendant les robots, Ibid.*, p. 105.
[2558] A. A. CASILLI, *En attendant les robots, Ibidem*, p. 259.
[2559] D. PENNEL, *Travailler pour soi : Quel avenir pour le travail à l'heure de la révolution individualiste ?*, Ed. du Seuil, Coll. H.C. ESSAIS, 2013, p. 37.
[2560] *Cf.* p. 390.
[2561] A. A. CASILLI, « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *op. cit.*, p. 431, où l'auteur indique que « *La spécificité de la vie privée dans le web social et des relations équipées par les technologies mobiles est un processus décentralisé, complexe et multidirectionnelle*. »
[2562] A. A. CASILLI, *En attendant les robots, Id.*, p. 261.

plateformes, les réseaux sociaux, les compteurs, les électroménagers et meubles « intelligents », ainsi que par les moyens de transport et par d'autres éléments ambiants des infrastructures urbaines (capteurs, caméras de vidéoprotection, etc.) « *est déjà une partie de notre réalité, mais est destinée à atteindre un seuil critique dans lequel ni les droits individuels, ni les mesures de protection de la propriété privée des informations personnelles pourraient suffire pour contrer les formes d'aliénation et de l'expropriation de plus en plus forte auxquelles les citoyens seraient exposés* »[2563].

Cet ensemble est facilité par les capacités de surveillance et de contrôle de ces plateformes prometteuses de liberté « parfaite », et contribue dès lors au concept de « capitalisme de surveillance » susmentionné[2564], que certains nomment le « complexe de surveillance-innovation »[2565]. Dans cette perspective, il paraît utile de savoir s'il s'agit d'une « liberté parfaite » ou d'un « contrôle parfait », question « déjà posée il y a douze ans » et qui est restée « sans réponse tout simplement parce que les deux faces sont indissociables » : le « surcroît d'information, qui renforce la liberté, va de pair avec un surcroît de surveillance qui tend au contrôle généralisé »[2566]. De ce fait, indique Delmas-Marty, *« en multipliant les flux d'information dans un espace sans frontières et en stockant un nombre croissant de données traitées en temps réel, les TIC sont un moyen sans équivalent dans l'histoire de partager et de croiser les savoirs, mais aussi de suivre la trace des êtres humains comme on suit des produits ou des animaux dangereux, voire de construire des robots de plus en plus autonomes, […]* »[2567], alors même que les individus deviennent de plus en plus dépendants.

In fine, avec les différents usages numériques innovants, la surveillance est non seulement devenue généralisée et ubiquitaire mais prend aujourd'hui de nombreuses formes et natures : elle s'avère être non seulement productive, captant et créant de la valeur, mais également participative, requérant des individus une contribution et une participation qui peuvent, à leur tour, être soit passives, « en profitant des services gratuits qui leur sont offerts sans se plaindre d'une atteinte à leur vie privée », soit actives fondées sur un dévoilement réciproque et « en participant à la surveillance du réseau »[2568]. Cette surveillance participative est essentiellement définie comme « *une surveillance mutuelle et horizontale basée sur le dévoilement volontaire*

[2563] A. A. CASILLI, « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *Id.*, p. 434.
[2564] *Cf.* p. 371, 380 et 444 et s.
[2565] J. E. COHEN, « The surveillance-innovation complex: The irony of the participatory turn », *In* D. Barney, G. Coleman, C. Ross, J. Sterne et T. Tembeck (dir.), *The participatory condition in the digital age*, University of Minnesota Press, 2016, p. 207-226.
[2566] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 92.
[2567] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Ibid.,* p. 92.
[2568] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Ibidem,* p. 94.

et agonistique des données personnelles par les utilisateurs eux-mêmes des services numériques, applications mobiles, plateformes web. Elle s'accompagne d'une perte de contrôle sur les conditions d'usage des plateformes et services web sur lesquels les données personnelles sont sauvegardées et mises en circulation »[2569].

La structure de surveillance n'est donc plus uniquement monodirectionnelle mais se trouve être continuellement nourrie et élargie par les objets mêmes de cette surveillance, inscrits dans un contexte social prônant la participation basée sur le dévoilement permettant d'investir dans le capital social de soi en ligne ; objets qui représentent les individus mais aussi les objets connectés ou les « choses », « celles qu'ils possèdent et celles avec lesquelles ils sont en contact », celles-ci paradoxalement devenant plus autonomes et plus intelligentes[2570]. Et les individus, dans le cadre de cette « surveillance douce », auto-imposée et réalisée de manière coopérative, ne voient pas leur volonté écrasée ou abolie ; cette dernière étant bien au contraire grandement sollicitée et chargée de conduire les opérations nécessaires à sa mise en œuvre[2571].

Cette nouvelle forme de surveillance semble alors capturer le flux de communications des usagers « *par une architecture de la participation passant par la production de traces qui personnalisent les usages, documentent les passages et la présence dans les environnements numériques* », menant à ce que l'ordre de priorités entre protection de la vie privée et personnalisation de l'expérience numérique soit inversé « *face à ces traces dont la pérennité et les utilisations secondaires (autant à des fins commerciales que sécuritaires) échappent aux utilisateurs* »[2572] ; traces qui finalement font l'objet de calcul, où la « *collection disparate de traces d'activités sont décousues révélant de façon kaléidoscopique des micro-facettes identitaires* », mais aussi, le fait que l'individu est calculé et constitue un flux : « *il est à la fois transparent et expulsé de ses propres traces* »[2573].

Dès lors, non seulement se diffuse « *une « culture de la surveillance » qui renvoie au modèle pré-étatique des « sociétés du regard permanent »* », modèle qui semble être à la fois libertaire et totalitaire et qui revient cette fois-ci « à l'échelle planétaire »[2574], mais il s'avère, de surcroît,

---

[2569] A. A. CASILLI, « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *Id.*, p. 424, et l'auteur précise « *La surveillance est participative dans la mesure où elle est mutuelle, passant par une généralisation des mécanismes de modération par le bas et d'application communautaire de normes en vigueur sur les plateformes sociales.* »

[2570] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 94.

[2571] A. A. CASILLI, *En attendant les robots, Id.*, p. 263.

[2572] A. A. CASILLI, « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *Id.,* p. 425.

[2573] D. CARDON, *À quoi rêvent les algorithmes, op. cit.,* p. 87-88.

[2574] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 94-95.

que « *la surveillance participative réinvente […] entièrement l'architecture panoptique* »[2575] ; l'ensemble caractérisant les nouvelles cultures de contrôle sociale émergentes.

Section 2 – Vers une remise en cause des identités humaines ?

L'essor et la mise au point des différentes cultures de contrôle social largement facilités par l'assise manifestée du capitalisme de surveillance semblent, alors, tendre vers l'instauration de nouvelles architectures sociétales (§1) permettant, de concert, d'observer l'émergence progressive d'un humain devenu réductible (§2) ; ce qui souligne, *ipso facto*, une question fondamentale : la société du XXI[e] Siècle s'oriente-t-elle vers une remise en cause des identités humaines ?

§1. Vers l'instauration de nouvelles architectures sociétales

Les nouvelles architectures sociétales qui se mettent en place aspirent à une meilleure gestion de la société et se traduisent, d'une part, par la manifestation d'un panoptique renouvelé et innovant (A), et d'autre part, par la revivification d'une biopolitique également renouvelée et innovante (B).

A. Un panoptique renouvelé et innovant

Conçu par Bentham dans les années 1780[2576], puis repris et analysé par Foucault dans les années 1970[2577], le concept du panoptique demeure toujours d'actualité pour décrire la société et l'organisation sociale ainsi que pour représenter la métaphore du pouvoir et ses mécanismes, mais aussi l'exercice de la surveillance dans les sociétés contemporaines. L'idée initiale du Panopticon, telle que conçue par Bentham, était celle de l'architecture d'une prison où l'inspecteur avait la capacité de surveiller tous les prisonniers alors que ces derniers ne pouvaient jamais voir l'inspecteur, ni vérifier s'ils étaient véritablement surveillés grâce à l'appareillage d'une architecture entièrement opaque[2578]. Le panoptique correspond donc à un

---

[2575] A. A. CASILLI, *En attendant les robots, Id.*, p. 263, et l'auteur en conclue que « *Loin de libérer le travail, le digital labor s'impose en définitive comme un « bénévolat forcé » ou une « servitude volontaire ».* »
[2576] J. BENTHAM, *The panopticon writings*, Verso Ed., 1995.
[2577] M. FOUCAULT, *Surveiller et punir : Naissance de la prison*, Ed. Gallimard, Coll. Tel, 1975.
[2578] M. FOUCAULT, *Surveiller et punir, Id.,* p. 233 : « *Tous les mécanismes de pouvoir qui, de nos jours encore, se disposent autour de l'anormal, pour le marquer comme pour le modifier, composent ces deux formes dont elles dérivent de loin. Le Panopticon de Bentham est la figure architecturale de cette composition. On en connaît le principe : à la périphérie un bâtiment en anneau ; au centre, une tour ; celle-ci est percée de larges fenêtres qui ouvrent sur la face intérieure de l'anneau ; le bâtiment périphérique est divisé en cellules, dont chacune traverse toute l'épaisseur du bâtiment ; elles ont deux fenêtres, l'une vers l'intérieur, correspondant aux fenêtres de la tour ; l'autre, donnant sur l'extérieur, permet à la lumière de traverser la cellule de part en part. il suffit*

théâtre : *« autant de cages, autant de petits théâtres, où chaque acteur est seul, parfaitement individualisé et constamment visible. Le dispositif panoptique aménage des unités spatiales qui permettent de voir sans arrêt et de reconnaître aussitôt* »[2579] ; le but principal étant la discipline ou la formation dans la vision de Bentham, et l'objectif plus large celui de la réforme morale de la société à travers le spectacle édifiant de la discipline *via* la surveillance constante.

La conception de Bentham n'a finalement jamais été concrètement réalisée, mais en tant que métaphore sur le pouvoir de la surveillance, elle est sans précédent, et c'est bien ce qui a intéressé Foucault. L'architecture panoptique sert en soi comme garantie de l'ordre où chacun est bien enfermé à sa place dans une cellule d'où il est constamment vu par le surveillant, mais où les murs l'empêchent d'être en contact avec les autres, « *il est vu, mais il ne voit pas ; objet d'une information, jamais sujet dans une communication* »[2580]. C'est bien l'effet majeur du panoptique, précise Foucault, celui d'induire « *un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir. Faire que la surveillance soit permanente dans ses effets, même si elle est discontinue dans son action ; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice ; que cet appareil architectural soit une machine à créer et à soutenir un rapport de pouvoir indépendant de celui qui l'exerce ; bref que les détenus soient pris dans une situation de pouvoir dont ils sont eux-mêmes les porteurs* »[2581].

Dans la vision de Bentham, existe un principe clé selon lequel le pouvoir devait être visible mais invérifiable, créant ainsi un contexte dans lequel les sujets n'ont pour alternative que de croire que l'apparence correspond bien à la réalité ; la clé ultime étant la surveillance dans une perspective de miroir sans tain. Le Panopticon constitue ainsi une machine, un dispositif d'une importance inégalée étant donné qu'il dissocie « le couple voir-être vu » et « automatise et désindividualise le pouvoir », une « *machine merveilleuse qui, à partir des désirs les plus différents, fabrique des effets homogènes de pouvoir. Un assujettissement réel naît d'une relation fictive* [puisque] *celui qui est soumis à un champ de visibilité, et qui le sait, reprend à son compte les contraintes du pouvoir ; […] ; il inscrit en soi le rapport de pouvoir dans lequel il joue simultanément les deux rôles ; il devient le principe de son propre assujettissement* »[2582].

La vision de Bentham possède une logique irréfutable révélant le pouvoir de la surveillance comme garant de la conformité, représentant par conséquent un outil efficace pour le contrôle

---

alors de placer un surveillant dans la tour centrale, et dans chaque cellule d'enfermer un fou, un malade, un condamné, un ouvrier ou un écolier. Par l'effet du contre-jour, on peut saisir de la tour, se découpant exactement sur la lumière, les petites silhouettes captives dans les cellules de la périphérie […]. »

[2579] M. FOUCAULT, *Surveiller et punir, Id.,* p. 233.

[2580] M. FOUCAULT, *Surveiller et punir, Ibid.,* p. 234.

[2581] M. FOUCAULT, *Surveiller et punir, Ibid.,* p. 234-235.

[2582] M. FOUCAULT, *Surveiller et punir, Ibidem,* p. 235-236.

social. L'histoire de la surveillance dans le monde occidental des XIX^e^ et XX^e^ Siècles se conforme à la logique Benthamienne du panoptique et, simultanément, la reflète, tout en s'en écartant ; les sujets du contrôle panoptique ayant souvent résisté, notamment eu égard à ces pouvoirs de coercition et de sanction[2583]. Il n'empêche que, comme le souligne Bauman, « *nous sommes naturellement portés à reconnaître dans les dispositifs contemporains de pouvoir une version nouvelle et améliorée des veilles techniques panoptiques qui n'auraient au fond nullement changé. […]. Nous avons également tendance à oublier les défis particuliers que devait relever le processus de modernisation, et qui rendirent les stratégies panoptiques à la fois séduisantes et applicables* »[2584].

Ce qui a intéressé Foucault, dans son travail sur la naissance de la prison, c'est bien cette « intensité imaginaire » que le panoptique a pu porter pendant deux siècles ; il précise que le panoptique doit être compris « *comme un modèle généralisable de fonctionnement ; une manière de définir les rapports du pouvoir avec la vie quotidienne des hommes. […]. Mais le Panopticon ne doit pas être compris comme un édifice onirique : c'est le diagramme d'un mécanisme de pouvoir ramené à sa forme idéale ; son fonctionnement, abstrait de tout obstacle, résistance ou frottement, peut bien être représenté comme un pur système architectural et optique : c'est en fait une figure de technologie politique qu'on peut et qu'on doit détacher de tout usage spécifique. Il est polyvalent dans ses applications* »[2585]. C'est bien un dispositif d'implantation, de distribution, d'organisation hiérarchique, de modes d'intervention qui peuvent être appliqués dans les écoles, les hôpitaux, les ateliers, les prisons, donc à chaque fois qu'il existe une multitude d'individus auxquels il faudrait imposer une tâche ou une conduite particulière. Dans ce contexte, « *le schéma panoptique, sans s'effacer ni perdre aucune de ses propriétés, est destiné à se diffuser dans le corps social* » ayant pour vocation d'y devenir « une fonction généralisée »[2586].

L'agencement panoptique tel que conçu par Bentham permettait, en théorie, de mettre en place une institution disciplinaire parfaite avec un réseau de dispositifs présents partout et parcourant l'ensemble de la société sans lacune ni interruption, un agencement donc « *qui programme, au niveau d'un mécanisme élémentaire et facilement transférable, le fonctionnement de base d'une société toute traversée et pénétrée de mécanismes disciplinaires* »[2587]. En distinguant les deux images de discipline que promet le schéma panoptique, Foucault a ainsi pu observer et analyser

[2583] R. WHITAKER, *The end of privacy, op. cit.*, p. 36.
[2584] Z. BAUMAN, *Le coût humain de la mondialisation*, *op. cit.*, p. 79.
[2585] M. FOUCAULT, *Surveiller et punir, Id.,* p. 239.
[2586] M. FOUCAULT, *Surveiller et punir, Id.,* p. 242.
[2587] M. FOUCAULT, *Surveiller et punir, Ibid.,* p. 243.

le mouvement qui va d'un extrême à l'autre, « d'un schéma de la discipline d'exception à celui d'une surveillance généralisée » dit-il, tout au long des XVII[e] et XVIII[e] Siècles et qui repose, selon le Professeur, sur une transformation historique, celle de l'extension progressive des dispositifs de discipline tout au long de ces deux siècles, « *leur multiplication à travers tout le corps social, la formation de ce qu'on pourrait appeler en gros la société disciplinaire* »[2588].

Mais il serait inexact de penser que les fonctions disciplinaires ont été absorbées une fois pour toute par un appareil d'État, cela s'est passé graduellement explique Foucault, la technologie panoptique s'est finement répandue vers une multitude d'applications différentes, allant des institutions « spécialisées » aux instances « préexistantes », aux appareils et autorités administratives jusqu'aux aux « appareils étatiques » ayant pour fonction « non pas exclusive mais majeure de faire régner la discipline à l'échelle d'une société (la police) » : « *on peut donc parler au total de la formation d'une société disciplinaire dans ce mouvement qui va des disciplines fermées, sorte de « quarantaine » sociale, jusqu'au mécanisme indéfiniment généralisable du « panoptisme ». Non pas que la modalité disciplinaire du pouvoir ait remplacé toutes les autres mais parce qu'elle s'est infiltrée parmi les autres, les disqualifiant parfois, mais leur servant d'intermédiaire, les reliant entre eux, les prolongeant, et surtout permettant de conduire les effets de pouvoir jusqu'aux éléments les plus ténus et les plus lointains. Elle assure une distribution infinitésimale des rapports de pouvoir* »[2589].

Depuis cette époque, il semble que les temps modernes et postmodernes ont continué la propagation de l'agencement panoptique quitte à devenir une fabrique de panoptiques, caractérisant le brillant usage qu'en a fait Foucault : « *une métaphore de la transformation moderne, du redéploiement et de la redistribution des pouvoirs à l'époque moderne* »[2590]. Le développement de l'État-nation moderne a été lié à la croissance de la surveillance en tant que mécanisme fondamental de contrôle administratif. Or, s'est aussi mis en place le capitalisme qui a vocation à dissocier l'économique du politique et qui a établi les compartiments distincts, bien qu'interdépendants, du secteur privé et du secteur public. En outre, comme l'a si bien suggéré Foucault, les principes du panoptique se répandent par le biais de l'infiltration, l'État et le capitalisme n'y échappant pas. Précisément, à la suite de la révolution industrielle, l'usine est devenue le principal site d'innovation en matière de surveillance et de discipline, sous

---

[2588] M. FOUCAULT, *Surveiller et punir, Ibidem,* p. 244, où l'auteur indique « *Toute une généralisation disciplinaire, dont la physique benthamienne du pouvoir représente le constat, s'est opéré au cours de l'âge classique. La multiplication des institutions de discipline en témoigne, avec leur réseau qui commence à couvrir une surface de plus en plus large, et à occuper surtout une place de moins en moins marginale […]* »

[2589] M. FOUCAULT, *Surveiller et punir, Ibidem,* p. 251-252.

[2590] Z. BAUMAN, *Le coût humain de la mondialisation*, *Id.*, p. 77.

l'impulsion des pressions du marché, pour améliorer l'efficacité et l'économie dans le processus productif.

Les théories du management, de la gestion scientifique, ont ainsi vu le jour, remplacées ultérieurement par l'école de gestion des relations humaines nécessitant des techniques de surveillance et de discipline afin d'assurer une gestion efficace. Quant aux activités étatiques, elles ont eu recours aux techniques de recensement et de statistique pour gérer efficacement et adéquatement leurs institutions, leurs administrations et leur population, ce qui requiert également la surveillance, outil essentiel pour les études et analyses statistiques ; l'objectif étant de construire une compréhension, une connaissance du monde social en vue de le changer ou le contrôler, et les informations statistiques sont une source idéale pour assurer la gestion et la régulation de la société et son bon fonctionnement. Il est, à ce titre, utile de noter que « *whether as political projects launched for state action or as social science schools of interpretation, knowledge is not analytically distinct from the control that knowledge promises. This remains true whether the motive is one of reform or of conservatism; changing or reproducing the social order are both problems of manipulation, intervention, and control. Both require a statistical base* »[2591].

S'est développé alors l'appareil administratif rationnel, une bureaucratie moderne, équivalente à la vision de Weber, dans laquelle, pour assurer une gestion administrative efficace, l'inspecteur ou le surveillant, devenu le bureaucrate, parcourt les sujets, devenus la société dans son ensemble, rendus aussi transparents que possible à son regard. Cependant, comme il a été vu dans cette étude, cette transparence n'est pas bidirectionnelle, l'État étant constamment protégé par le secret d'État[2592]. En effet, « *l' « idéal-type » du Panopticon ne laisse aucune place pour l'espace privé ; en tout cas pour un espace privé opaque, un espace privé sans surveillance ou, ce qui est pire, échappant encore à la surveillance* »[2593]. Dans ce cadre, se mit en place l'appareil de surveillance étatique récoltant une vaste quantité d'informations fonctionnant de pair avec l'appareil bureaucratique Weberien, dans la mesure où une organisation hiérarchique des fonctions et des institutions était nécessaire pour faciliter la mise en commun rationnelle de l'information. Parallèlement, et conformément à la vision disciplinaire de Bentham *via* l'agencement panoptique, qui certes servait à sanctionner les contrevenants, mais servait surtout à exercer un contrôle préventif par le biais des mécanismes disciplinaires, un contrôle préventif commençait à voir le jour, que ce soit du côté de l'État ou

[2591] R. WHITAKER, *The end of privacy, Id.*, p. 42.
[2592] *Cf.* p. 345.
[2593] Z. BAUMAN, *Le coût humain de la mondialisation*, *Id.*, p. 78.

de celui des entreprises, nécessitant des études de statistique et de probabilité sur les risques qui permettaient de déterminer la probabilité qu'une personne ou une catégorie de personnes allait enfreindre à la règle.

Il est évident que le développement du web et des données ainsi que du cadre de définition des facteurs de risque constituent des éléments du schéma panoptique en ce sens que les risques doivent être gérés et maîtrisés, la prévention étant toujours plus rentable et moins perturbatrice sur le plan social que la punition après coup : « *the panoptic state is thus increasingly future-oriented and concerned about the predictive power of the information it gathers, just as the capitalist corporation is oriented toward the future return on its investments. Both become in effect hostages to uncertainty and eagerly, if not greedily, scan and store as much information as possible to reduce the level of uncertainty* »[2594]. Avec le développement des nouvelles technologies de l'information et de la communication permettant la collecte, le traitement, la corrélation, l'agrégation, le stockage ou encore l'extraction, les tendances panoptiques gagnent, de façon incommensurable, en portée et en efficacité.

In fine, le panoptique contemporain, avec l'avènement du XXI[e] Siècle, du cyberespace et du Big data, est remarquablement différent. C'est principalement un agencement panoptique de consommation fondé sur des avantages positifs où la pire sanction est l'exclusion. En effet, le nouveau Panopticon se distingue de son ancêtre sur deux points importants : il est décentré et est principalement consensuel. Les nouvelles technologies de l'information offrent un potentiel d'omniscience réel, plutôt que simulé, tout en remplaçant le surveillant avec plusieurs surveillants pouvant agir parfois de concert et parfois en concurrence. Plus particulièrement, les nouvelles technologies rendent les individus visibles, d'une manière que Bentham n'aurait pu concevoir ou même imaginer, mais ils sont visibles à de multiples regards venant de plusieurs directions : « *each time you make a purchase or engage in a financial transaction, each time you take any action that is recorded, somewhere (and fewer and fewer actions are not recorded somewhere) you are briefly illuminated by the now ubiquitous, decentered Panopticon* »[2595]. La force même de ce panoptique innovant est que les personnes ont tendance à y participer volontairement, justement parce qu'elles voient les avantages positifs de la participation, et sont moins susceptibles de percevoir les désavantages ou les menaces que ce dispositif panoptique renouvelé peut induire. Autrement dit, « *nos corps sont emprisonnés dans les réseaux, les banques de données, les autoroutes de l'information – de sorte que tous ces*

[2594] R. WHITAKER, *The end of privacy, Id.*, p. 45.
[2595] R. WHITAKER, *The end of privacy, Id.*, p. 140.

sites de stockage de l'information dans lesquels nos corps sont, pour ainsi dire, « pris électroniquement », ne fournissent plus une protection contre l'observation […]. Le stockage de grandes quantités de données, qui croissent avec chaque utilisation d'une carte de crédit et virtuellement avec chaque achat, conduit, […], à la mise en place d'un « superpanopticon », avec une différence par rapport au Panopticon « classique » : les surveillés, qui fournissent les données en question, sont les premiers acteurs – des acteurs volontaires – de la surveillance »[2596].

Le panoptique participatif, complément de la surveillance participative et productive susvisée[2597], déploie son regard de manière séduisante quoiqu'insidieusement, le tout dans le but, affiché, d'accroître les commodités, les bénéfices et le confort des individus en les libérant des contraintes de la vie quotidienne. Il suffit de penser aux développements des cartes de crédit permettant d'effectuer des achats, que ce soit physiquement, en ligne ou par téléphone, sans avoir à se soucier de la disponibilité de l'argent à portée de main ; ou encore de la mise en place des caméras de "vidéoprotection" pour la sécurité du public puisque des quartiers, des villes, des bâtiments ou n'importe quel espace, constamment surveillées verraient raisonnablement le taux de criminalité se réduire, par peur de sanction, et les délinquants développer une tendance à se retirer de ces espaces surveillés. Ces caractéristiques panoptiques facilitent finalement la vie quotidienne, augmentent la sécurité et accordent plus de pouvoir aux consommateurs, de telle sorte qu'ils ne s'y opposeront pas s'ils voient leurs besoins et leurs désirs mieux servis en conséquence : « *think of it as a christmas wish list that enables santa to serve you better. The consumer Panopticon rewards participation* »[2598].

Cela dit, il y a toujours un prix à payer, comme il a pu être observé à travers cette étude, et il existe toujours un côté sombre qui demeure invisible et opaque pour l'utilisateur quotidien de ces services et bénéfices. *In concreto*, la capacité d'accorder un crédit à une personne solvable est rendue possible par la capacité d'identifier et d'exclure la personne à risque ; la même surveillance détaillée qui personnalise les prestations, cible celles qui en seront exclues ; l'attention accordée à un sujet en particulier, en exclut un autre d'importance égale[2599]. De plus, et à ce stade la séduction est pragmatiquement trompeuse, « *consumers are being disciplined by consumption itself to obey the rules, to be "good" not because it is morally preferable to*

[2596] Z. BAUMAN, *Le coût humain de la mondialisation*, *Id.*, p. 80, où l'auteur cite Mark Poster qui « *se demande avec étonnement pourquoi « la crainte portant sur les bases de données n'est pas encore devenue une question politique de premier plan au niveau national ».* »
[2597] *Cf.* p. 584.
[2598] R. WHITAKER, *The end of privacy, Id.*, p. 141.
[2599] *Cf.* p. 575.

being "bad" but because there is no conceivable alternative to being good, other than being put outside the reach of benefits »[2600].

C'est bien une manifestation de la transformation radicale du pouvoir panoptique où, dans la pratique de ce pouvoir, « la surveillance a finalement remplacé le spectacle » conduisant à l'émergence d'un autre mécanisme de pouvoir baptisé « Synopticon », qui est « par nature, global »[2601]. En effet, « *le Synopticon n'a pas besoin d'utiliser la coercition : il opère par la séduction, qui amène* [les individus] *à devenir spectateurs* » de la toute petite minorité qui est « soigneusement sélectionnée » dans les médias, ce « médium interactif à sens unique » précise Bauman[2602]. Selon l'auteur, que ce soit dans le contexte du cyberespace ou des médias, « *même ceux qui y ont accès n'ont le droit de faire leur choix que dans un cadre déterminé par les fournisseurs, qui les incite à perdre de l'argent en passant beaucoup de temps à faire un choix parmi toutes les possibilités qui leur sont offertes* »[2603].

De façon ingénieuse, des criminologues ont utilisé le monde de Disney World comme incarnation de la puissance panoptique. Un grand nombre de personnes visitent chaque jour les parcs de Disney où il y a souvent de longues et pénibles files d'attente et de longs, voire excessivement longs, délais pendant lesquels des familles ou des groupes d'individus attendent l'entrée à des expositions particulières ou à des jeux particuliers ; pourtant, un comportement pacifique ordonné est maintenu d'une manière apparemment homogène et transparente, sans signes visibles de coercition. Cela est rendu possible grâce à la volonté commune de la direction et des clients de faciliter la consommation des produits, productions et spectacles de Disney : « *within Disney World control is embedded, preventative, subtle, cooperative and apparently non-coercive and consensual. […]. Its order is instrumental and determined by the interests of Disney Productions rather than moral and absolute. […]. Surveillance is pervasive but it is the antithesis of the blatant control of the Orwellian State: its source is not government, and its vehicle is not Big Brother. The order of instrumental discipline is not the unitary order of a central State but diffuse and separate orders defined by private authorities responsible for the*

[2600] R. WHITAKER, *The end of privacy, Id.*, p. 142.
[2601] Z. BAUMAN, *Le coût humain de la mondialisation*, *Id.*, p. 82-83.
[2602] Z. BAUMAN, *Le coût humain de la mondialisation*, *Ibid.*, p. 83-84.
[2603] Z. BAUMAN, *Le coût humain de la mondialisation*, *Ibidem*, p. 84 ; ainsi, explique l'auteur, « *Dans le Synopticon, les locaux regardent les mondiaux. Ce qui confère de l'autorité à ces derniers, c'est leur éloignement même ; […] ils sont à la fois inaccessibles et visibles, éthérés et charnels, infiniment supérieurs tout en donnant à tous les inférieurs un brillant exemple à suivre ou à rêver de suivre ; admirés et convoités en même temps – un pouvoir royal qui guide au lieu de gouverner. Bien que séparés sur terre, les locaux rencontrent les mondiaux au cours d'émissions de télévision quotidiennement retransmises depuis le paradis* [le cyberespace]. *Les échos de cette rencontre résonnent à l'échelle mondiale, recouvrant tous les bruits locaux, se répercutant sur les murs locaux, ce qui révèle et renforce d'autant plus la solidité infranchissable de ces murs, solides comme ceux d'une prison.* », p. 85-86.

feudal-like domains of Disney World, condominium estates, commercial complexes and the like. Within contemporary discipline, control is as fine-grained as Orwell imagined but its features are very different. […] people are today seduced to conform by the pleasures of consuming the goods that corporate power has to offer »[2604].

C'est bien une des caractéristiques de ce panoptique renouvelé et décentré, celui d'être à la fois unifié et fragmenté en même temps, où la culture de la consommation prime, et où le partage ou l'acquisition des données par une minorité, de nos jours l'État-entreprise et les GAFAM notamment, sont pratique courante afin d'exercer encore plus de pouvoir, de contrôle et de gestion efficaces, tout en incitant subtilement les individus à la consommation et à la conformité pour pouvoir se faire. Avec l'individualisation en consommateur-sujet, que les nouvelles technologies et les nouvelles techniques de marketing opèrent, l'agencement panoptique, innovant et renouvelé, a les capacités d'aborder ou d'interpeller les sujets en vue de comprendre leurs besoins et de servir leurs désirs ; ce système étant si souple que plusieurs entreprises et/ou plateformes se font concurrence pour attirer l'attention et l'argent du consommateur libre et souverain. Avec la mondialisation et la globalisation économique, la double identité du Panopticon, à la fois compétitive et unifiée, s'avère être ainsi un grand pouvoir dans la mesure où la concurrence constitue le mécanisme d'infiltration de nouveaux marchés pendant qu'elle porte en soi l'acceptation universelle de la culture de consommation[2605].

De nos jours, « *in Europe, North America, and much of the rest of the world, governments and businesses achieve their ends in almost the opposite way from that of the Panopticon: not through the subjection of the individual to the gaze of a single, centralized authority, but through the surveillance of the individual by all (in theory, though in fact by many). I call this the Cryptopticon: an inscrutable information ecosystem of massive corporate and state*

[2604] C. D. SHEARING et P. C. STENNING, "From the Panopticon to Disney World: The development of discipline", *In* A. N. Doob et E. L. Greenspan (éds.), *Perspectives in Criminal Law: Essays in Honour of John Ll. J. Edwards,* Canada Law Books, Toronto, 1984, p. 347, et les auteurs rajoutent "*The contrasts between morally based justice and instrumental control, carceral punishment and corporate control, the Panopticon and Disney World and Orwell's and Huxley's visions are succinctly captured by the novelist Beryl Bainbridge's (1984) observations about a recent journey she made retracing J.B. Priestley's (1934) celebrated trip around Britain. She notes how during his travels in 1933 the center of the cities and towns he visited were defined by either a church or a center of government (depicting the coalition between Church and State in the production of order that characterizes morally based regimes). During her more recent trip, one of the changes that struck her most forcibly was the transformation that had taken place in the center of cities and towns. These were now identified not by churches or town halls, but by shopping centers; often vaulted glass-roofed structures that she found reminiscent of the cathedrals they had replaced both in their awe-inspiring architecture and in the hush that she found they sometimes created. What was worshipped in these contemporary cathedrals, she noted, was not an absolute moral order but something much more mundane: people were "worshipping shopping" and through it, we would add, the private authorities, the order and corporate power their worship makes possible.*"

[2605] R. WHITAKER, *The end of privacy, Id.*, p. 146-151.

surveillance »[2606]. À la différence du panoptique de Bentham, le Cryptopticon n'est pas censé être évident ; son échelle, son ubiquité, voire son existence même, sont supposés être cachés de la vue et demeurer invisibles. Précisément, « *the Cryptopticon relies on browser cookies, data streams retained by telecommunication firms, satellite imagery, global positioning system traces, covert voice surveillance, store discount cards, e-book readers, and mobile applications. Each of these techniques masks its real purpose: to gather or provide data and to track the behavior of millions of people with stunning precision. Beguilingly, though, each technique offers something valuable and convenient – often "for free"* »[2607].

À la différence des prisonniers de Bentham, les individus de ce nouveau monde ne savent pas, ou ne peuvent savoir, tous les moyens par lesquels ils sont surveillés ou profilés et ne régulent donc pas leurs comportements sous la surveillance généralisée quotidienne ; bien au contraire, ils semblent même ne pas s'en soucier, voire s'en moquer. Pourtant, « *the workings of the Cryptopticon are cryptic, hidden, scrambled and mysterious. One can never be sure who is watching whom and for what purpose. Surveillance is so pervasive and much of it is seemingly benign ("for your safety and security") that it's almost impossible for the object of surveillance to assess how she is manipulated or threatened by powerful institutions gathering and using the record of surveillance* »[2608]. La menace de ce nouveau schéma panoptique n'est pas que l'expression ou l'expérimentation sera annulée ou disciplinée, comme elles sont supposées l'être sous le panoptique benthamien, mais plutôt que les sujets deviennent « *inured to and comfortable with the networked status quo that they will gladly sort themselves into "niches" that enable effective profiling and behavioral prediction* »[2609], perdant à terme leur faisceau d'identité et leur autonomie dans la construction de soi.

Le Cryptopticon est intimement lié au Big data et la relation dynamique entre ces deux concepts caractérise la nécessité de comprendre les deux à la fois par rapport au commerce, à l'État et, plus généralement, à la société et son architecture actuelle. Finalement, dans ce dispositif panoptique innovant, que ce soit du côté des entreprises ou du côté des États, les deux souhaitent que les individus soient eux-mêmes, se comportent librement et souverainement, dévoilent toutes leurs passions et excentricités, toutes leurs habitudes et connections ou affiliations sociales, révélant, *in fine*, autant que possible l'ensemble de leur faisceau d'identité au complet et tel qu'il est individuellement perçu, vécu et représenté[2610]. En effet, « *in the liberal state of*

[2606] S. VAIDHYANATHAN, *Anti-social media, op. cit*., p. 67.
[2607] S. VAIDHYANATHAN, *Anti-social media, Id*., p. 67.
[2608] S. VAIDHYANATHAN, *Anti-social media, Ibid*., p. 67.
[2609] S. VAIDHYANATHAN, *Anti-social media, Ibidem*, p. 68.
[2610] *Cf.* p. 42 et s., 87 et s.

the twenty-first century, domination does not demand social or cultural conformity. The state, like every private firm that employs a sophisticated method of marketing, wants us to express ourselves – to choose – because mere expression of difference is usually unthreatening, yet remarkably useful to the powerful »[2611].

La société, son organisation et sa gestion semblent être ainsi passées du Panopticon, au Synopticon arrivant au Cryptopticon, tout en manifestant concomitamment l'idée, initialement et brillamment perçue par Foucault dans son analyse sur la machine panoptique, selon laquelle « *le Panopticon est un lieu privilégié pour rendre possible l'expérimentation sur les hommes, et pour analyser en toute certitude les transformations qu'on peut obtenir sur eux. Le panoptique peut même constituer un appareil de contrôle sur ses propres mécanismes*. [… il] *fonctionne comme une sorte de laboratoire de pouvoir. Grace à ces mécanismes d'observation, il gagne en efficacité et en capacité de pénétration dans le comportement des hommes ; un accroissement de savoir vient s'établir sur toutes les avancées du pouvoir, et découvre des objets à connaître avec toutes les surfaces où celui-ci vient s'exercer* »[2612].

B. Une biopolitique renouvelée et innovante

Malgré la mondialisation, la globalisation et les nombreuses puissances qui en émergent tendant à remettre en cause la souveraineté des États, le besoin de sécurité réclamé par la société a permis une sorte de repli sur soi étatique, se traduisant notamment par la réaffirmation des principes de souveraineté ainsi que de primauté de la territorialité et de la sécurité nationale, parallèlement à la politique d'ouverture, de liberté de circulation et de coopération avec les autres États, en particulier, européens[2613]. Ce repli sur soi ou retrait étatique vise principalement à assurer et à renforcer la sécurité nationale et celle de la population, confrontée à des risques et menaces divers et variés, en réaménageant les modes d'exercice du pouvoir, suivant la conception foucaldienne de la biopolitique. La transformation graduelle de l'exercice du

[2611] S. VAIDHYANATHAN, *Anti-social media, Id.*, p. 68-69, et l'auteur indique ainsi que "*Companies such as Google and Facebook put Big data collection and analysis at the heart of their revenue-generating functions, always described by company officials as enhancements to the "user experience". The line between state and commercial surveillance hardly matters anymore, as state security services regularly receive significant data sets on people's movement and habits just by asking for or by licensing the data on the open market. Data collected by one institution are easily transferred, mined, used, and abused by another. So one company might purchase consumer data from a supermarket or big-box retailer and then sell them to direct-mail marketers, political parties, and even local law enforcement. Data firms also collect state records such as voter registrations, deeds, car titles, and liens to sell consumer profiles to direct-marketing firms. Given the many possible abuses of Big data, including the long-term tarnishing of personal and professional reputations, citizens need to be fully aware of the flows of information between private firms, governments, and any other institutions that might have an interest in using such data.*"

[2612] M. FOUCAULT, *Surveiller et punir, Id.,* p. 238-239.

[2613] *Cf.* p. 464 et s., 498 et s.

pouvoir et de ses techniques, semblant remettre en cause le principe de souveraineté étatique, caractérise le passage de la politique à la biopolitique, à savoir le passage d'un gouvernement dédié à la préservation de l'intégrité territoriale et de la continuité du fonctionnement politique, à un gouvernement dont le but fondamental est d'assurer la protection de la société civile et ses conditions de survie.

C'est une transformation « des plus massives du droit politique du XIX^e^ Siècle » qui a consisté non « à substituer mais à compléter » le « vieux droit de souveraineté », celui de « faire mourir ou laisser vivre », par « *un autre droit nouveau, qui ne va pas effacer le premier, mais qui va le pénétrer, le traverser, le modifier, et qui va être un droit, ou plutôt un pouvoir exactement inverse : pouvoir de « faire » vivre et de « laisser » mourir. Le droit de souveraineté, c'est donc celui de faire mourir ou de laisser vivre. Et puis, c'est ce nouveau droit qui s'installe : le droit de faire vivre et de laisser mourir* » ; ce nouveau droit qui se réfère à la biopolitique représente ainsi une forme de pouvoir sur la vie, une « technologie de pouvoir » indique Foucault, « qui n'exclut pas la technique disciplinaire »[2614]. Trois formes principales de techniques de pouvoir peuvent donc être distinguées selon le Professeur, le pouvoir souverain, le pouvoir disciplinaire et la biopolitique, pouvoir sur la vie, ces techniques ayant coexisté au cours de l'histoire, les unes n'excluant pas les autres, mais s'ajustant et s'articulant ensemble plutôt. Apparue pendant la seconde moitié du XVIII^e^ Siècle, cette autre technologie de pouvoir intègre et modifie partiellement le pouvoir disciplinaire, sans l'exclure ou le discréditer ; elle va, cependant, surtout « l'utiliser en s'implantant en quelque sorte en lui », et s'incruster effectivement « grâce à cette technique disciplinaire préalable »[2615].

À la différence de la discipline qui s'adresse « au corps », cette nouvelle technique de pouvoir non disciplinaire s'applique « *à la vie des hommes, ou encore, si vous le voulez, elle s'adresse non pas à l'homme-corps, mais à l'homme vivant, à l'homme être vivant ; à la limite, […], à l'homme-espèce* »[2616]. En effet, la discipline aspire à régir la multiplicité des hommes comme une multiplicité qui « peut et doit » se résoudre en corps individuels, en individus à « surveiller, à dresser, à utiliser, éventuellement à punir », alors que la nouvelle technologie de pouvoir émergente vise la « multiplicité des hommes » perçus comme une « masse globale » et non comme des corps différents, « *une multiplicité d'individus qui sont et qui n'existent que profondément, essentiellement, biologiquement liés à la matérialité à l'intérieur de laquelle ils*

[2614] M. FOUCAULT, *Il faut défendre la société*, *op. cit.*, Cours du 17 mars 1976 - p. 214-215.
[2615] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 216.
[2616] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 216.

existent »[2617], affectée « de processus d'ensemble qui sont propres à la vie », des processus comme la naissance, la mort, la production ou la santé[2618]. Ainsi, précise Foucault, « *après une première prise de pouvoir sur le corps qui s'est faite sur le mode de l'individualisation, on a une seconde prise de pouvoir qui, elle, n'est pas individualisante mais qui est massifiante, […], qui se fait en direction non pas de l'homme-corps, mais de l'homme-espèce* »[2619].

La discipline des corps ou l' « anatomo-politique » du corps humain, apparue vers la fin du XVIII[e] début du XIX[e] Siècle comme toute technique de discipline, vise à rendre les corps dociles, utiles et malléables par le biais d'une intériorisation progressive de la norme par les personnes ; un pouvoir qui se caractérise donc par « *un certain nombre de techniques de coercition qui s'exercent selon un quadrillage systématique du temps, de l'espace et du mouvement des individus, et investissent particulièrement les attitudes, les gestes et les corps* »[2620]. La norme est, à cet égard, préférée à la loi pour discipliner les corps humains, cette dernière manifestant souvent l'interdit là où la première caractérise une règle disciplinaire qui va être intériorisée et qui détermine la conduite à adopter ; l'objectif ultime étant la normalisation des comportements et la mise en place d'une « société de normalisation »[2621]. Dès lors, « *après l'anatomo-politique du corps humain, mise en place au cours du XVIII[e] siècle, on voit apparaître, à la fin de ce même siècle, quelque chose qui n'est plus une anatomo-politique du corps humain, mais que j'appellerai une « biopolitique » de l'espèce humaine* »[2622].

Un biopouvoir, expression pratique de la logique biopolitique, s'installe alors visant un ensemble de processus variés relatifs à la vie, tels que la proportion des naissances ou la proportion des décès, le taux de reproduction ou la fécondité d'une population, processus qui finalement ont constitué « les premiers objets de savoir et les premières cibles de contrôle de cette biopolitique » nécessitant *de facto* la mise en œuvre de « la mesure statistique » pour évaluer ces phénomènes[2623]. Cette nouvelle technologie de pouvoir ayant fondamentalement pour objet la vie des individus, représente, selon la conception du Professeur, un droit positif ayant pour vocation de gouverner les individus et les phénomènes de la population, et donc d'intervenir dans les problèmes de la vie de l'espèce humaine, problèmes de fécondité, de

---

[2617] M. FOUCAULT, *Sécurité, Territoire, Population*, *op. cit.*, Leçon du 11 janvier 1978 - p. 23.
[2618] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 216.
[2619] M. FOUCAULT, *Il faut défendre la société*, *Ibid.*, Cours du 17 mars 1976 - p. 216.
[2620] J. REVEL, *Le vocabulaire de Foucault*, Ed. Ellipses Marketing, Coll. Vocabulaire de…, 2002, p. 20.
[2621] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 225, où l'auteur indique que « *La société de normalisation, c'est une société où se croisent, selon une articulation orthogonale, la norme de la discipline et la norme de la régulation.* »
[2622] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 216.
[2623] M. FOUCAULT, *Il faut défendre la société*, *Ibid.*, Cours du 17 mars 1976 - p. 216-217.

natalité, de morbidité, « *en gros de ce qu'on pourrait appeler les endémies, c'est-à-dire la forme, la nature, l'extension, la durée, l'intensité des maladies régnantes dans une population* »[2624]. Néanmoins, ces phénomènes ne sont pas envisagés en tant qu'épidémies pouvant causer des morts de façon plus fréquente, mais sont plutôt perçus comme « *des facteurs permanents – et c'est comme cela qu'on les traite – de soustraction des forces, diminution du temps de travail, baisse d'énergies, coûts économiques, tant à cause du manque de produire que des soins qu'elles peuvent coûter* »[2625].

Puis, au moment de l'industrialisation, le champ d'intervention de la biopolitique s'étend à « tout un ensemble de phénomènes, dont les uns sont universels et dont les autres sont accidentels », entraînant des conséquences analogues d'incapacité, de mise hors-circuit des individus, de vieillissement, ou de neutralisation, mais aussi, relativement à l'accidentel, des infirmités ou des anomalies diverses[2626]. En conséquence, la biopolitique met en place, aux côtés des institutions d'assistance qui existaient depuis un moment, « des mécanismes beaucoup plus subtils, économiquement beaucoup plus rationnels que la grosse assistance, à la fois massive et lacunaire » ; des mécanismes donc d'assurance, d'épargne individuelle et collective, ou de sécurité.

Un autre domaine d'intervention privilégié de la biopolitique est l'environnement, le milieu d'existence des êtres vivants, « espace dans lequel se déroulent des séries d'éléments aléatoires », espace propre à la sécurité donc, et qui désigne « ce qui est nécessaire pour rendre compte de l'action à distance d'un corps sur un autre ; c'est donc bien le support et l'élément d'une action »[2627]. Autrement dit, « *le milieu, c'est un ensemble de données naturelles, fleuves, marécages, collines, c'est un ensemble de données artificielles, agglomération d'individus, agglomérations de maisons, etc. Le milieu, c'est un certain nombre d'effets qui sont des effets de masse portant sur tous ceux qui y résident. C'est un élément à l'intérieur duquel se fait un bouclage circulaire des effets et des causes, puisque ce qui est effet d'un côté va devenir cause de l'autre. […]. Et enfin le milieu apparaît comme un champ d'intervention où, au lieu d'atteindre les individus comme un ensemble de sujets de droit capables d'actions volontaires – ce qui était le cas de la souveraineté –, au lieu de les atteindre comme une multiplicité*

[2624] M. FOUCAULT, *Il faut défendre la société*, *Ibid.*, Cours du 17 mars 1976 - p. 217.
[2625] M. FOUCAULT, *Il faut défendre la société*, *Ibidem*, Cours du 17 mars 1976 - p. 217, et l'auteur indique « *Ce sont ces phénomènes-là qu'on commence à prendre en compte à la fin du XVIII^e siècle et qui amène la mise en place d'une médecine qui va avoir, maintenant, la fonction majeure de l'hygiène publique, avec des organismes de coordination des soins médicaux, de centralisation de l'information, de normalisation du savoir, et qui prend aussi l'allure de campagne d'apprentissage de l'hygiène et de médicalisation de la population.* »
[2626] M. FOUCAULT, *Il faut défendre la société*, *Ibidem*, Cours du 17 mars 1976 - p. 217-218.
[2627] M. FOUCAULT, *Sécurité, Territoire, Population*, *Id.*, Leçon du 11 janvier 1978 - p. 22.

d'organismes, de corps susceptibles de performance, et de performances requises comme dans la discipline, on va essayer d'atteindre, précisément, une population »[2628].

C'est principalement sur ces domaines et champs d'intervention que s'est constituée la biopolitique, ses pratiques et dispositifs, et c'est de ceux-là, et de bien d'autres encore, que cette biopolitique va également prélever son savoir et définir les multiples champs d'intervention de son pouvoir. Ce qui, selon Foucault, marque l'apparition d'un élément nouveau, « qu'au fond ni la théorie du droit ni la pratique disciplinaire ne connaissent », la notion de « population » intrinsèquement liée à la biopolitique en ce sens que celle-ci « a affaire à la population » ; population apparue comme « problème politique, comme problème à la fois scientifique et politique, comme problème biologique et comme problème de pouvoir »[2629]. En outre, la biopolitique prend en compte la nature des phénomènes qui sont des phénomènes collectifs, de masse, aléatoires et imprévisibles, se déroulant dans la durée ; en somme, ce à quoi va s'adresser la biopolitique ce sont les « évènements aléatoires qui se produisent dans une population prise dans sa durée »[2630].

De plus, cette nouvelle technologie de pouvoir met en place de nombreux mécanismes, distincts des mécanismes disciplinaires mais qui, de façon générale, leur ressemblent : « *il va s'agir d'abord, bien sûr, de prévisions, d'estimations statistiques, de mesures globales ; il va s'agir, également, non pas de modifier tel phénomène en particulier, non pas tellement tel individu, mais, essentiellement, d'intervenir au niveau de ce que sont les déterminations de ces phénomènes généraux, de ces phénomènes dans ce qu'ils ont de global. […]. Et il s'agit surtout d'établir des mécanismes régulateurs qui, dans cette population globale avec son champ aléatoire, vont pouvoir fixer un équilibre, maintenir une moyenne, établir une sorte d'homéostasie, assurer des compensations ; bref, d'installer des mécanismes de sécurité autour de cet aléatoire qui est inhérent à une population d'êtres vivants, d'optimaliser, […], un état de vie* »[2631].

Précisément, à la différence du dressage individuel qu'opèrent les mécanismes disciplinaires, dans ceux de la biopolitique il s'agit de prendre l'individu par « des mécanismes globaux, d'agir de telle manière qu'on obtienne des états globaux d'équilibration, de régularité ; bref, de prendre en compte la vie, les processus biologiques de l'homme-espèce, et d'assurer sur eux une régularisation »[2632]. Dès lors, indique Foucault, en deçà du pouvoir de souveraineté, voilà

[2628] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibid.*, Leçon du 11 janvier 1978 - p. 23.
[2629] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 218-219.
[2630] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 219.
[2631] M. FOUCAULT, *Il faut défendre la société*, *Ibid.*, Cours du 17 mars 1976 - p. 219.
[2632] M. FOUCAULT, *Il faut défendre la société*, *Ibidem*, Cours du 17 mars 1976 - p. 220.

qu'apparaît avec cette technologie de biopouvoir, un pouvoir « continu, savant », le pouvoir de « régularisation ». Deux technologies de pouvoir superposées, s'articulant l'une à l'autre, se mettent ainsi en place, d'un côté, la « technologie disciplinaire » centrée sur le corps, produisant des effets individualisants et manipulant le corps comme « foyer de force qu'il faut à la fois rendre utiles et dociles », et de l'autre, la « technologie régularisatrice » centrée sur la vie, regroupant les effets de masse propre à une population, cherchant à contrôler les évènements hasardeux qui peuvent se produire, une technologie qui « cherche à en contrôler (éventuellement à en modifier) la probabilité, en tout cas à en compenser les effets », une technologie qui aspire donc à quelque chose comme l'homéostasie[2633] : « la sécurité de l'ensemble par rapport à ses dangers internes » ; *in fine*, deux technologies de pouvoir qui, dans les deux cas, représentent bien une « technologie du corps » mais à des degrés différents[2634].

Selon Foucault, c'est bien la mutation de ces techniques et modalités d'exercice du pouvoir qui a transformé le pouvoir de souveraineté, schéma organisateur initial qui s'était trouvé « inopérant pour régir le corps économique et politique d'une société en voie, à la fois, d'explosion démographique et d'industrialisation »[2635]. C'est aussi cette transformation de l'exercice de la souveraineté qui a permis au capitalisme et à la rationalité libérale de s'imposer à travers le monde marquant le passage de la souveraineté traditionnelle, essentiellement répressive et sombre, à une souveraineté moderne s'appuyant sur une gouvernementalité, un « pouvoir qui s'est exercé depuis la fin du XVI^{e} Siècle à travers les dispositifs et les technologies de la raison d'État et de la « police » », plus souple dont l'objet principal est la population[2636]. En effet, explique l'auteur, « *il faut bien comprendre les choses non pas du tout comme le remplacement d'une société de souveraineté par une société de discipline, puis d'une société de discipline par une société, disons, de gouvernement. On a, en fait, un triangle : souveraineté, discipline et gestion gouvernementale, une gestion gouvernementale dont la cible*

[2633] *Cf.* p. 567 et 571.
[2634] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 222-223.
[2635] M. FOUCAULT, *Il faut défendre la société*, *Ibid.*, Cours du 17 mars 1976 - p. 222-223, et l'auteur explique alors : « *Si bien qu'à la veille mécanique du pouvoir de souveraineté beaucoup trop de choses échappaient, à la fois par en bas et par en haut, au niveau du détail et au niveau de la masse. C'est pour rattraper le détail qu'une première accommodation a eu lieu : accommodation des mécanismes de pouvoir sur le corps individuel, avec surveillance et dressage – cela a été la discipline. Bien sûr, cela a été l'accommodation la plus facile, la plus commode à réaliser. C'est pourquoi elle s'est réalisée le plus tôt – dès le XVII^{e}, début du XVIII^{e} – à un niveau local, dans des formes intuitives, empiriques, fractionnées, et dans le cadre limité d'institutions comme l'école, l'hôpital, la caserne, l'atelier, etc. Et puis vous avez ensuite, à la fin du XVIII^{e} siècle, une seconde accommodation, sur les phénomènes globaux, sur les phénomènes de la population, avec les processus biologiques ou bio-sociologiques des masses humaines. Accommodation plus difficile car, bien entendu, elle impliquait des organes complexes de coordination et de centralisation.* »
[2636] M. FOUCAULT, *Il faut défendre la société*, *Ibidem*, Situation du Cours - p. 247.

principale est la population et dont les mécanismes essentiels sont les dispositifs de sécurité »[2637].

D'après Foucault, il existe ainsi « *un lien historique profond entre le mouvement qui fait basculer les constantes de la souveraineté derrière le problème maintenant majeur des bons choix de gouvernement, le mouvement qui fait apparaître la population comme une donnée, comme un champ d'intervention, comme la fin des techniques de gouvernement, le mouvement enfin qui isole l'économie comme domaine spécifique de réalité et l'économie politique à la fois comme science et comme technique d'intervention du gouvernement dans ce champ de réalité* »[2638].

Dès lors, les techniques disciplinaires s'articulant aux techniques régularisatrices constituent le biopouvoir qui caractérise, *in fine*, une technologie de sécurité que Foucault, dans son analyse, oppose aux mécanismes par lesquels le souverain, jusqu'à l'âge classique, s'efforçait d'assurer la sécurité de son territoire[2639]. À travers l'histoire des technologies de sécurité, le Professeur tente alors de repérer s'il est désormais possible de parler de société de sécurité, et formule une interrogation assez pertinente à notre époque contemporaine : « *peut-on dire que dans nos sociétés l'économie générale de pouvoir est en train de devenir de l'ordre de la sécurité ?* »[2640]. Par conséquent, à partir d'exemples tirés du XVII^{e} et du XVIII^{e} Siècles, le Professeur souligne les rapports entre une population et son « milieu », lie la question de la population à l'économie libérale en notant que la question du libéralisme se manifeste comme « nouvelle rationalité gouvernementale », et traite enfin du passage de la forme de normalisation spécifique à la sécurité tout en distinguant entre normalisation disciplinaire et normalisation au sens strict ; ce qui lui permet, *ipso facto*, de révéler la « corrélation » qui existe entre « la technique de sécurité et la population »[2641]. L'émergence de la notion de population, en tant qu'idée et réalité, n'est pas seulement cruciale au niveau politique, indique Foucault, elle a également une signification décisive au plan épistémologique : « *[…] la thématique de l'homme à travers les "sciences humaines" qui l'analysent comme être vivant, individu travaillant, sujet parlant, il faut la comprendre à partir de l'émergence de la population comme corrélatif de pouvoir et comme objet de savoir. L'homme, ce n'est, après tout, rien d'autre, tel qu'il a été pensé, défini à partir*

[2637] M. FOUCAULT, *Sécurité, Territoire, Population*, *Id.*, Leçon du 1er février 1978 - p. 111.
[2638] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibid.*, Leçon du 1er février 1978 - p. 111.
[2639] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibid.*, Leçon du 25 janvier 1978 - p. 66-67.
[2640] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibid.*, Leçon du 11 janvier 1978 - p. 12.
[2641] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibidem*, Leçon du 11 janvier 1978 - p. 13, et Leçon du 25 janvier 1978, p. 77-80.

des sciences dites humaines du XIX^e siècle et tel qu'il a été réfléchi dans l'humanisme du XIX^e siècle, cet homme ce n'est rien d'autre, finalement, qu'une figure de la population »[2642].

En outre, c'est à travers l'analyse des dispositifs de sécurité relatifs à la population que se met en relief le concept de « gouvernementalité », concept qui subit également une mutation, passant de son sens traditionnel d'autorité publique ou d'exercice de la souveraineté à une « valeur discriminante », à la faveur du concept physiocratique de « gouvernement économique », désignant les techniques spécifiques de gestion des populations. Dans ce contexte, le « gouvernement » prend alors le sens étroit « d'art d'exercer le pouvoir dans la forme de l'économie », et le libéralisme économique se présente comme un « art de gouverner »[2643].

Le nouveau triangle émergent, « gouvernement, population, économie politique », formant une série « solide » indissociable, même aujourd'hui, a révélé, selon Foucault, l'importance de la notion de gouvernementalité, notion qui perdure jusqu'à l'époque actuelle : « *par « gouvernementalité », j'entends l'ensemble constitué par les institutions, les procédures, analyses et réflexions, les calculs et les tactiques qui permettent d'exercer cette forme bien spécifique, quoique très complexe, de pouvoir qui a pour cible principale la population, pour forme majeure de savoir l'économie politique, pour instrument technique essentiel les dispositifs de sécurité. Deuxièmement, par « gouvernementalité », j'entends la tendance, la ligne de force qui, dans tout l'Occident, n'a pas cessé de conduire, et depuis fort longtemps, vers la prééminence de ce type de pouvoir qu'on peut appeler le « gouvernement » sur tous les autres : souveraineté, discipline, et qui a amené, d'une part, le développement de toute une série d'appareils spécifiques de gouvernement et, d'autre part, le développement de toute une série de savoirs. Enfin, par « gouvernementalité », […] il faudrait entendre le processus, ou plutôt le résultat du processus par lequel l'État de justice du Moyen Âge, devenu au XV^e et XVI^e siècles État administratif, s'est trouvé petit à petit « gouvernementalisé ». […]. Et il est vraisemblable que si l'État existe tel qu'il existe maintenant, c'est grâce, précisément, à cette gouvernementalité qui est à la fois extérieure et intérieure à l'État, puisque ce sont les tactiques de gouvernement qui, à chaque instant, permettent de définir ce qui doit relever de l'État et ce qui ne doit pas en relever, ce qui est public et ce qui est privé, ce qui est étatique et ce qui est*

[2642] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibidem*, Leçon du 25 janvier 1978, p. 81, et l'auteur rajoute : « *Ou disons encore, s'il est vrai que, tant que le problème du pouvoir se formulait dans la théorie de la souveraineté, en face de la souveraineté ne pouvait pas exister l'homme, mais seulement la notion juridique de sujet de droit.* »

[2643] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibidem*, Leçon du 1er février 1978 - p. 99-101.

non étatique. Donc, […], l'État dans sa survie et l'État dans ses limites ne doivent se comprendre qu'à partir des tactiques générales de la gouvernementalité »[2644].
Se forme ainsi un « État de gouvernement » défini essentiellement par la masse, « la masse de la population », « *et cet État de gouvernement, qui porte essentiellement sur la population et qui se réfère à et utilise l'instrumentation du savoir économique, correspondrait à une société contrôlée par les dispositifs de sécurité. […]. La pastorale, la nouvelle technique diplomatico-militaire et, enfin, la police,* […ont] *été les trois grands points d'appui à partir desquels a pu se produire ce phénomène fondamental dans l'histoire de l'Occident, qui a été la gouvernementalisation de l'État* », induisant « l'art de gouverner »[2645].

Le biopouvoir a donc la vocation principale de gouverner les individus dans leurs particularités mais aussi en tant que figures d'une population, cet ensemble vivant possédant ses propres caractéristiques biologiques et qui est susceptible d'être gouverné, discipliné, régulé et modelé. Selon le Professeur, l'apparition de la gestion biopolitique des populations a permis le développement de la rationalité libérale et de l'infiltration du libéralisme dans l'ensemble des technologies de pouvoir à la disposition de l'État « moderne ». C'est la problématique de la gouvernementalité et de ses procédures qui marque donc l'entrée de la question de l'État dans le champ d'analyse des micro-pouvoirs, analyse qui, loin d'être « limitée à un domaine précis qui serait défini par un secteur de l'échelle », révèle « un point de vue, une méthode de déchiffrement valable pour l'échelle toute entière, quelle qu'en soit la grandeur »[2646]. Par ailleurs, la gestion des « processus bio-sociologiques des masses humaines », à la différence des disciplines mises en œuvre dans le cadre d'institutions limitées, implique précisément l'appareil d'État, dans la mesure où c'est au niveau de celui-ci que se trouvent les « organes complexes de coordination et de centralisation » nécessaires à cette gestion, caractérisant le fait que la biopolitique n'est autre qu'une « bio-régulation par l'État »[2647].
Cette nouvelle forme d'État, « réalité composite », n'est rien d'autre finalement que « l'effet mobile d'un régime de gouvernementalités multiples »[2648]. C'est alors que se met en place cet

[2644] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibidem*, Leçon du 1er février 1978 - p. 111-113.
[2645] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibidem*, Leçon du 1er février 1978 - p. 113.
[2646] M. FOUCAULT, *Naissance de la biopolitique*, *op. cit.*, Leçon du 7 mars 1979 - p. 192 où le Professeur précise que « *Autrement dit, l'analyse des micro-pouvoirs, ce n'est pas une question d'échelle, ce n'est pas une question de secteur, c'est une question de point de vue* ». Plus particulièrement, explique-t-il, « *[…] cette grille de la gouvernementalité, on peut bien supposer qu'elle est valable lorsqu'il s'agit d'analyser la manière dont on conduit la conduite des fous, des malades, des délinquants, des enfants ; […] cette grille de la gouvernementalité peut valoir, également, lorsqu'il s'agit d'aborder les phénomènes d'une toute autre échelle, comme par exemple une politique économique, comme la gestion de tout un corps social, etc.* »
[2647] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 223.
[2648] M. FOUCAULT, *Naissance de la biopolitique*, *Id.*, Leçon du 31 janvier 1979 - p. 79.

art de gouverner selon la raison d'État, caractérisé par deux ensembles technologiques : le système diplomatico-militaire ordonné au maintien de l'équilibre européen et la police, au sens classique de « l'ensemble des moyens nécessaires pour faire croître, de l'intérieur, les forces de l'État »[2649]. Par conséquent, le lieu d'émergence de la population, objet central de ce nouvel État, peut être mieux situé en ce sens qu'il est « en dérivation par rapport à la technologie de « police » et en corrélation avec la naissance de la réflexion économique »[2650] ; d'où l'apparition du libéralisme comme forme de rationalité propre aux dispositifs de régulation biopolitique. En effet, au principe de limitation externe de la raison d'État, que constituait le droit, s'est substitué, au XVIII[e] Siècle, un principe de limitation interne, sous la forme de l'économie, ce « grand déplacement de la véridiction juridique à la véridiction épistémique »[2651] indique Foucault.

L'économie politique, précisément, qui porte en elle l'exigence d'une autolimitation de la raison gouvernementale, fondée sur la connaissance du cours naturel des choses, marque ainsi l'irruption d'une nouvelle rationalité dans l'art de gouverner, celle de gouverner moins, par souci d'efficacité maximum, en fonction de la « naturalité »[2652] des phénomènes auxquels on a affaire. C'est donc cette gouvernementalité, liée dans son effort d'autolimitation permanente à la question de la vérité, que Foucault nomme « le libéralisme », le libéralisme constituant alors la condition d'intelligibilité de la biopolitique[2653]. Selon l'auteur, « *avec l'émergence de l'économie politique, avec l'introduction du principe limitatif dans la pratique gouvernementale elle-même, une substitution importante s'opère, ou plutôt un doublage, puisque les sujets de droit sur lesquels s'exerce la souveraineté politique apparaissent eux-mêmes comme une population qu'un gouvernement doit gérer. […]. Mais qui ne voit pas que c'est là une part seulement de quelque chose de bien plus large, et qui est cette nouvelle raison gouvernementale ? Étudier le libéralisme comme cadre général de la biopolitique* »[2654].

[2649] M. FOUCAULT, *Sécurité, Territoire, Population*, *Id.*, Résumé du Cours - p. 373-376.
[2650] M. FOUCAULT, *Sécurité, Territoire, Population*, *Ibid.*, Leçon du 5 avril 1978 - p. 359-362.
[2651] M. FOUCAULT, *Naissance de la biopolitique*, *Id.*, Leçon du 10 janvier 1979 - p. 20-21.
[2652] M. FOUCAULT, *Naissance de la biopolitique*, *Id.*, Leçon du 10 janvier 1979 - p. 24 ; à ce titre l'auteur fait une remarque : « *cette raison libérale s'établit comme autolimitation du gouvernement à partir d'une « naturalité » des objets et pratiques propres à ce gouvernement. Cette naturalité, quelle est-elle ? celle des richesses ? oui, mais simplement en tant que moyens de paiement se multipliant ou se raréfiant, stagnant ou circulant. Mais plutôt les biens en tant qu'ils sont produits, qu'ils sont utiles et utilisés, en tant qu'ils sont échangés entre partenaires économiques. C'est aussi celle des individus. Non pas cependant en tant que sujets obéissants ou indociles, mais en tant qu'ils sont eux-mêmes liés à cette naturalité économique, que leur nombre, leur longévité, leur santé, leur manière de se comporter se trouvent dans des rapports complexes et enchevêtrés avec ces processus économiques.* »
[2653] M. FOUCAULT, *Naissance de la biopolitique*, *Id.*, Leçon du 10 janvier 1979 - p. 17-19.
[2654] M. FOUCAULT, *Naissance de la biopolitique*, *Ibid.*, Leçon du 10 janvier 1979 - p. 24.

En effet, Foucault indique que pour comprendre la biopolitique, il faut nécessairement comprendre le régime général de la raison gouvernementale, « ce régime général que l'on peut appeler la question de vérité, premièrement de la vérité économique à l'intérieur de la raison gouvernementale », ce régime qui est le « libéralisme », « *[…] ce nouveau type de rationalité dans l'art de gouverner, ce nouveau type de calcul qui consiste à dire et à faire dire au gouvernement : à tout cela, j'accepte, je veux, je projette, je calcule qu'il ne faut pas toucher* », et qui s'oppose à la raison d'État, ou plutôt la « modifie fondamentalement sans en remettre en question les fondements », et qui permet de saisir ce qu'est la biopolitique telle qu'appliquée par les États modernes[2655]. Ce libéralisme qui caractérise, selon l'auteur, « *[…] le nouvel art de gouverner formé au XVIII^e^ siècle,* [et qui] *implique en son cœur un rapport de production/destruction avec la liberté. Il faut d'une main produire la liberté, mais ce geste même implique que, de l'autre, on établisse des limitations, des contrôles, des coercitions, des obligations appuyées sur des menaces, etc.* »[2656].

Le libéralisme doit, selon l'auteur, être entendu « dans un sens très large », non pas comme « une théorie », ni comme « une idéologie », encore moins comme « une manière pour la « société » de se « représenter … » », mais comme « une pratique, c'est-à-dire comme une « manière de faire » orientée vers des objectifs et se régulant par une réflexion continue », et doit donc être envisagé « comme principe et méthode de rationalisation de l'exercice du gouvernement – rationalisation qui obéit, et c'est là sa spécificité, à la règle interne de l'économie maximale »[2657]. Dans la conception de Foucault, le mot de libéralisme se justifie alors « *par le rôle que joue la liberté dans l'art libéral de gouverner : liberté garantie, sans doute, mais également produite par ce dernier, qui a besoin, pour atteindre ses fins, de la susciter, de l'entretenir et de l'encadrer en permanence. Le libéralisme, ainsi, peut se définir comme le calcul du risque – le libre jeu des intérêts individuels – compatible avec l'intérêt de*

[2655] M. FOUCAULT, *Naissance de la biopolitique*, *Ibid.*, Leçon du 10 janvier 1979 - p. 23-24 où l'auteur fait une remarque importante : « *cette autolimitation de la raison gouvernementale, caractéristique du libéralisme, se trouve dans un rapport étrange au régime de la raison d'État. Celle-ci ouvre à la pratique gouvernementale un domaine d'intervention indéfinie, mais d'autre part elle se donne, par le principe d'une balance concurrentielle entre États, des objectifs internationaux limités. L'autolimitation de la pratique gouvernementale par la raison libérale s'est accompagnée de l'éclatement des objectifs internationaux et de l'apparition d'objectifs illimités avec l'impérialisme. La raison d'État avait été corrélative de la disparition du principe impérial, au profit de l'équilibre concurrentiel entre États. La raison libérale est corrélative de l'activation du principe impérial, non sous la forme de l'Empire, mais sous la forme de l'impérialisme, et ceci en liaison avec le principe de la libre concurrence entre les individus et les entreprises. Chiasme entre objectifs limités et objectifs illimités quant au domaine de l'intervention intérieure et au champ de l'action internationale* ».

[2656] M. FOUCAULT, *Naissance de la biopolitique*, *Ibid.*, Leçon du 10 janvier 1979 - p. 65.

[2657] M. FOUCAULT, *Naissance de la biopolitique*, *Ibid.*, Leçon du 10 janvier 1979 - p. 24 et, Résumé du Cours, p. 323.

chacun et de tous », de sorte que finalement les individus, et la population en général, participent à la formation de la rationalité biopolitique[2658].

C'est ce qui implique, par ailleurs, l'établissement de multiples mécanismes de sécurité, le libéralisme s'engageant « dans un mécanisme où il aura à chaque instant à arbitrer la liberté et la sécurité des individus autour de cette notion de danger »[2659]. Ainsi, selon le Professeur, « *liberté et sécurité : ce sont les procédures de contrôle et les formes d'intervention étatique requises par cette double exigence qui constituent le paradoxe du libéralisme et sont à l'origine des « crises de gouvernementalité »[2660] qu'il a connues depuis deux siècles* »[2661] et qu'il continue toujours, semble-t-il, de connaître. Cette gouvernementalité, cette « *manière dont on conduit la conduite des hommes* »[2662], permet ainsi de maîtriser l'existence des individus par le biais du modèle médical, notamment de la « médecine sociale », en prévenant systématiquement les risques et menaces qui pèsent sur eux, mais aussi de gérer les comportements en vue de créer les conditions d'une coexistence pacifique et productive des individus, représentant une force de travail et une ressource économique nécessaires au fonctionnement efficace du marché, ce « nouveau lieu de véridiction »[2663].

La biopolitique repose donc, dans la conception foucaldienne, sur plusieurs principes : d'une part, le pouvoir est une tactique, une stratégie entendue comme la somme d'une multitude de « micro-pouvoirs », donc comme un agencement complexe de pratiques et de techniques pour la plupart issues de la guerre, de la sécurité-sûreté et de la santé, de discours historico-politiques traduisant les « discours de la vérité », de lutte des races, ce « racisme d'État » répondant à l'hybridation du pouvoir souverain et du biopouvoir, de faire vivre et laisser mourir, de savoirs, représentant en soi un dispositif, un agencement d'énoncés diffusés et de diverses institutions

---

[2658] M. FOUCAULT, *Naissance de la biopolitique*, *Ibidem*, Situation du Cours, p. 335.

[2659] M. FOUCAULT, *Naissance de la biopolitique*, *Ibidem*, Leçon du 24 janvier 1979 - p. 67, l'auteur précise ainsi « *Au fond, si d'un côté, le libéralisme c'est un art de gouverner qui manipule fondamentalement les intérêts, il ne peut pas – et c'est là le revers de la médaille –, il ne peut pas manipuler les intérêts sans être en même temps gestionnaire des dangers et des mécanismes de sécurité/liberté, du jeu sécurité/liberté qui doit assurer que les individus ou la collectivité seront le moins possible exposés aux dangers.* »

[2660] M. FOUCAULT, *Naissance de la biopolitique*, *Ibidem*, Leçon du 24 janvier 1979 - p. 69-70, où l'auteur précise : « *Troisième conséquence (la seconde étant la conjonction entre les disciplines et le libéralisme), c'est l'apparition aussi, dans ce nouvel art de gouverner, de mécanismes qui ont pour fonction de produire, d'insuffler, de majorer des libertés, d'introduire un peu plus de liberté par un peu plus de contrôle et d'intervention. […]. On ne garantit les libertés démocratiques dans ce cas-là que par un interventionnisme économique qui est dénoncé comme étant une menace pour les libertés. De sorte qu'on arrive, […], à cette idée que cet art libéral de gouverner, finalement, introduit de lui-même ou est victime de l'intérieur de ce qu'on pourrait appeler des crises de gouvernementalités. Ce dont des crises qui peuvent être dues à l'augmentation, par exemple, du coût économique de l'exercice des libertés. […]. Problème donc, crise, si vous voulez, ou conscience de crise à partir de la définition du coût économique de l'exercice des libertés.* »

[2661] M. FOUCAULT, *Naissance de la biopolitique*, *Ibidem*, Situation du Cours, p. 335.

[2662] M. FOUCAULT, *Naissance de la biopolitique*, *Ibidem*, Leçon du 7 mars 1979 - p. 192.

[2663] M. FOUCAULT, *Naissance de la biopolitique*, *Ibidem*, Leçon du 17 janvier 1979 - p. 34-37.

coordonnées et centralisées ; d'autre part, les individus réunis sous une même autorité sont formés en « population » à gouverner, et non plus en peuple de sujets à soumettre ; enfin, la raison d'État nouvellement mise en œuvre, caractérisant les intérêts biopolitiques de l'État et de la population, détermine l'orientation des politiques opérée par le biopouvoir. Ce dernier représente, *in fine*, un mode de gouvernement qui prône le contrôle de tous les versants de la vie des personnes, étant donné que leur gestion est devenue un enjeu politique pour la survie de la population et la gestion de sa productivité.

Ce biopouvoir qui repose sur deux stratégies principales, le pouvoir disciplinaire, « qui s'applique singulièrement aux corps par les techniques de la surveillance, les sanctions normalisatrices, l'organisation panoptique des institutions privées », et le pouvoir régulateur ou la bio-régulation, « qui s'applique globalement à la population, à la vie et aux vivants »[2664], donc deux aspects du contrôle social, coexistent et correspondent à une prise en compte généralisée et systématique des risques et leur prévention. Les contrôles par précaution et par prévention, caractéristiques de la biopolitique, apparaissent de manière évidente dans les politiques et les sociétés modernes, comme il a pu être observé dans le cadre des développements de cette étude, notamment *via* la gestion actuelle par les États des risques associés à la mondialisation et à la globalisation, ainsi que par la gestion actuelle de la société et ses individus. Comme l'a si bien souligné le Professeur, suivant le modèle pastoral, le biopouvoir finalement gère la population comme un « troupeau », en portant une attention particulière à chaque brebis, tout en veillant à la sécurité et au bien-être de l'ensemble du « troupeau »[2665].

L'exercice de la souveraineté sous sa forme moderne, la biopolitique, semble bien être à l'origine d'une surveillance et d'un contrôle accru des individus, de leurs comportements, de leurs habitudes et de leurs déplacements, afin d'assurer le « bien-être » de la population, sa sécurité et sa sûreté. Plus encore, les individus extérieurs à la population, en particulier, les étrangers, sont aussi étroitement surveillés grâce aux dispositifs et techniques de pouvoir mis en place, et sont traités de manière différentielle, voir discriminante et raciste, en fonction des risques qu'ils représentent, notamment eu égard au fait que cette domination politique innovante que constitue le biopouvoir est caractérisée par une dialectique inclusion-exclusion et par la mise en place du « racisme d'État »[2666].

[2664] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Situation du Cours - p. 247.
[2665] M. FOUCAULT, *Sécurité, Territoire, Population*, *Id.*, Leçon du 8 février 1978 - p. 128-134.
[2666] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 227-234 où l'auteur explique que, grosso modo, le racisme « *assure la fonction de mort dans l'économie du biopouvoir, selon le principe que la mort des autres, c'est le renforcement biologique de soi-même en tant que l'on est membre d'une race ou*

Cette nouvelle gestion biopolitique de la vie engendre une certaine radicalisation des rationalités développées par les États, d'autant que la rationalité biopolitique a été celle qui a facilité le triomphe du capitalisme dans la mesure où elle permettait un encadrement strict des individus, une gestion efficace des modalités de leur travail, et une maximisation de leur force de travail. La mise en place de dispositifs de surveillance et de contrôle, désormais omniprésents et omniscients, ainsi que la normalisation de la vie conduisent à une interrogation sceptique sur la place de la liberté dans ces nouvelles formes de sociétés. La gouvernementalité biopolitique, qui repose sur des régimes d'énoncés et de visibilité du pouvoir[2667], donc sur les ordres de discours et le développement des machines, la visibilité étant inséparable des machines, dont l'exemple le plus abouti est celui de la machine panoptique, n'est dès lors pas transcendante ou atemporelle. Cette gouvernementalité s'adapte plutôt aux conditions présentes et, dans une logique préventive, tente d'anticiper et d'appréhender les besoins ou les problèmes futurs, et la détermination des énonçables et des visibles propres à une époque permet de façonner les comportements et les mentalités ainsi que la norme intégrée par la société[2668].

Le biopouvoir ne se résume pas, en conséquence, à la loi, celle-ci n'étant que l'un des éléments facilitant la gestion, la redistribution des rapports de forces sociaux pour les pacifier, mais comprend également la stratégie de pouvoir s'appuyant sur un « ordre du discours », qu'il contribue à façonner et qui « met en œuvre des mécanismes d'organisation du réel à travers la production de savoirs, de stratégies, et de pratiques »[2669]. Dans cette perspective, il y aurait alors un complexe pouvoir-savoir[2670] permettant au pouvoir de modeler la vérité en fonction d'une rationalité biopolitique et d'exercer, ainsi, une influence sur les représentations communes : « *le dispositif biopolitique semble agir comme une technique d'autocontrôle, une sorte de rapport entre pouvoir et savoir qui pousse jusqu'au bout l'adéquation totale* »[2671].

Et comme l'a souligné Agamben, « *tout dispositif implique un processus de subjectivation sans lequel le dispositif ne saurait fonctionner comme dispositif de gouvernement, mais se réduit à*

---

d'une population, en tant que l'on est élément dans une pluralité unitaire et vivante », et prend l'exemple du nazisme : « *Pas d'État plus disciplinaire, bien sûr que le régime nazi ; pas d'État, non plus, où les régulations biologiques soient reprises en compte d'une manière plus serrée et plus insistante.* »

[2667] O. RAZAC, *Avec Foucault après Foucault : Disséquer la société de contrôle*, Paris, Ed. Harmattan, 2008, p. 23, où l'auteur précise que les régimes d'énoncés et de visibilité du biopouvoir sont intrinsèquement liés : « *les visibilités n'apparaissent que formalisées par des discours et les énoncés ne s'actualisent que remplis par des objets* ».

[2668] G. DELEUZE, *Foucault*, Paris, Les Éditions de Minuit, Coll. Critique, 1986, p. 56.

[2669] J. REVEL, *Le vocabulaire de Foucault, Id.,* p. 36.

[2670] G. DELEUZE, *Foucault, Id.,* p. 81.

[2671] T. VILLANI, « Michel Foucault et le territoire : gouvernement et biopolitique », *In* T. PAQUOT et C. YOUNÈS (dir.), *Le territoire des philosophes. Lieu et espace de la pensée au XX*ème *siècle*, Paris, Ed. La découverte, Coll. Recherches, 2009, p. 175.

un pur exercice de violence »[2672]. En effet, sans une intériorisation par les individus des normes que ces dispositifs matérialisent, ceux-ci n'auront pas « le moindre fondement dans l'être » et se résument à un exercice de violence pure[2673]. C'est pourquoi, précise l'auteur, « les dispositifs doivent toujours impliquer un processus de subjectivation »[2674], et donc d'intériorisation, processus aboutissant à la production de « sujets » dociles et d'une « population » régulée et modulée. Or, souligne Agamben, la « *phase extrême du développement du capitalisme dans laquelle nous vivons* [… constitue] *une gigantesque accumulation et prolifération de dispositifs* »[2675], qui implique une multitude croissante de processus de subjectivation et où « *il semble qu'aujourd'hui il n'y ait plus un seul instant de vie des individus qui ne soit modelé, contaminé, ou contrôlé par un dispositif* »[2676]. L'auteur va même plus loin en affirmant que la prolifération de ces technologies et dispositifs est à l'origine d'un processus inverse de désubjectivation et de crises identitaires : « *les sociétés contemporaines se présentent ainsi comme des corps inertes, traversés par de gigantesques processus de désubjectivation auxquels ne répond aucune subjectivation réelle. De là, l'éclipse de la politique qui supposait des sujets et des identités réels et le triomphe de l'économie, c'est-à-dire d'une pure activité de gouvernement qui ne poursuit rien d'autre que sa propre reproduction* »[2677].

La mobilisation des concepts foucaldiens et des théories d'Agamben, relatifs aux dispositifs et à l'instauration d'un état d'exception permanent, ainsi qu'à la coexistence du pouvoir souverain et de la biopolitique permettent, en outre, de souligner la radicalisation de l'exercice des techniques de pouvoir, la subjectivation et l'asservissement des individus et de leurs identités, mais aussi les dérives sécuritaires possibles d'un pouvoir se revendiquant pourtant libéral, et qui, à l'aube du XXI^{e} Siècle, se manifestent simultanément et de façon évidente, tendant alors à un renouveau de la biopolitique, du biopouvoir et de la gouvernementalité, lesquels se présentent, à l'époque de la révolution numérique, d'une façon innovante tout en préservant leurs conditions et mécanismes classiques. En effet, la biopolitique comporte intrinsèquement une possible dérive sécuritaire étant donné que santé et sécurité y sont profondément liées, et que « *la survie n'est pas un désir mais une passion à laquelle personne ne peut résister, surtout pas les « citoyens sanitaires » de la biopolitique* »[2678].

[2672] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, op. cit.,* p. 41-42 ; et, *Cf.* p. 371 et s.
[2673] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Id.,* p. 26-27.
[2674] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Id.,* p. 27.
[2675] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Ibid.,* p. 34.
[2676] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Ibid.,* p. 33-34.
[2677] G. AGAMBEN, *Qu'est-ce qu'un dispositif ?, Ibidem,* p. 46.
[2678] O. RAZAC, « Il faut lutter contre les morts prématurées », *In* A. KIÉFER et D. RISSE (dir.), *La biopolitique outre-Atlantique après Foucault*, Paris, Ed. Harmattan, Colloque de 2012 (Série Esthétiques, Culture et politique), p. 137.

Dans ce contexte, se manifeste alors le volet sécuritaire de la biopolitique, la « biosécurité » qui correspond à « *l'ensemble des dispositifs et des rationalités publiques mis en place pour répondre à de nouvelles menaces venues d'agents biologiques, institutionnels ou non, qui ont pris une place croissante dans les rationalités publiques depuis le 11 septembre 2001* »[2679]. Ainsi, le biopouvoir évolue vers la gouvernementalité fondée sur la peur, l'angoisse et l'incertitude, légitimant la mise en place des dispositifs et mécanismes de sécurité : « *l'effet de la biopolitique dans le domaine de la sécurité est qu'au motif de protéger la vie, les dispositifs publics ne cessent de la multiplier en y introduisant de nouvelles inquiétudes* »[2680].
En outre, les progrès scientifiques en matière de connaissances sur le vivant et le corps de l'homme, facilités par le développement des nouvelles technologies, mais aussi les nouvelles plateformes et les nouveaux outils traitant de la santé offrent des possibilités accrues de contrôle des individus, de leur corps et de leur identité. Les biotechnologies, en particulier, résultant d'une combinaison entre les connaissances en biologie et le développement de technologies, permettent de maîtriser des facteurs qui, jusqu'à présent, étaient impossibles à influencer. De plus, les avancées en matière de recherche génétique, l'accumulation massive de données génétiques et biométriques, peuvent entraîner l'adoption d'une nouvelle approche de la reproduction de l'homme-espèce. *In fine*, ces biotechnologies, constituant « *une forme de biopolitique dans la mesure où elles conduisent à relier tous les phénomènes sociaux à la possibilité d'intervention dans le code génétique* »[2681], ouvrent la voie à une nouvelle économie du vivant et à un « capital humain »[2682] qui abondent en dérives possibles tant les biotechnologies offrent un potentiel de contrôle infini.
Comme le note Foucault, « *cet excès du biopouvoir apparaît lorsque la possibilité est techniquement et politiquement donnée à l'homme, non seulement d'aménager la vie, mais de faire proliférer la vie, de fabriquer du vivant, de fabriquer du monstre, de fabriquer – à la limite- des virus incontrôlables et universellement destructeurs* »[2683].

[2679] F. KECK, « Les usages du biopolitique », *op. cit.*, p. 309.
[2680] F. KECK, « Les usages du biopolitique », *Id.*, p. 309, et l'auteur poursuit avec une citation : « *« Enquêter sur le bioterrorisme et la biosécurité comme sites de problématisation, c'est poser des questions comme : quelle sorte d'"incertitude" ou de "perte de la familiarité" a été introduite par la menace de bioterrorisme, et dans quels domaines ? Quelles formes de compréhension, d'action et de vie en commun sont détruites ? Quelles formes d'analyse politique, de réflexion morale et de pratiques techno-scientifiques sont mobilisées par les acteurs dans la modélisation et la mise en opération de quelque chose comme la biosécurité ? » (Collier, Lakoff & Rabinow 2004, p. 3).* »
[2681] F. KECK, « Les usages du biopolitique », *Ibid.*, p. 307.
[2682] M. FOUCAULT, *Naissance de la biopolitique, Id.,* Situation du Cours - p. 335.
[2683] M. FOUCAULT, *Il faut défendre la société*, *Id.*, Cours du 17 mars 1976 - p. 226.

§2. Vers l'émergence progressive d'un humain réductible ?

Question essentielle sur laquelle il convient de s'arrêter, l'émergence progressive de l'humain réductible comporte deux interrogations d'importances égales et fondamentales, à savoir l'homme devient-il une machine à calculer et à fabriquer ? (A), et alors, qu'en est-il de la « sérendipité » et de l' « irréductible humain » ? (B).

A. L'humain, une machine à calculer et à fabriquer ?

L'impressionnante baisse des coûts des puces RFID ou encore des frais de stockage, entre autres, a favorisé le développement exponentiel des objets connectés donnant lieu à l'Internet des objets et aux objets intelligents ; outils se multipliant récemment de manière régulière et continuelle, touchant divers aspects de la vie quotidienne des individus comme la voiture, la télévision, les villes (*smart-cities*), les maisons et bureaux (équipés d'objets intelligents), les montres (intelligentes), par exemple. De nombreux outils, dispositifs et services technologiques se développent à une vitesse croissante, poussée parfois à l'extrême, tous porteurs de différentes atteintes à la vie privée et à l'autonomie et la liberté des personnes dans la construction de leur soi, de leur identité ; alors même que leur mise en œuvre est justifiée par des soucis relatifs à l'autonomie individuelle, le confort et le bien-être des individus, la suppression des contraintes quotidiennes et routinières, l'ouverture du marché et la forte demande, la compétition et la concurrence, ou encore la liberté de la recherche. Il suffit, pour s'en convaincre, de citer « la position européenne sur les nanotechnologies », indique Delmas-Marty, « *la Commission européenne évoquant d'emblée la compétitivité et comparant les niveaux et les rythmes des investissements. En revanche, l'hypothèse d'un moratoire est repoussée comme « dangereusement contre-productive ». Quant à la question d'éthique, la Communication de 2004 l'aborde seulement à travers l'autonomie de l'individu et la liberté de la recherche ; tandis que la consultation sur le plan 2010-2015 évoque vaguement des recherches à engager sur « les aspects éthiques, légaux et sociaux des nanotechnologies* »[2684].

Cette communication, et les textes et orientations mises en place par la suite, notamment l'orientation de la toute dernière politique de sécurité et de défense précitée[2685], érige en place centrale l'augmentation des budgets et des investissements récoltés pour la Recherche et le Développement en matière informatique et scientifique. L'ancien Commissaire à la recherche de la Commission européenne annonçait, en préface de la Communication en faveur des

[2684] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, op. cit.,* p. 81-82.
[2685] *Cf.* p. 498 et s.

nanotechnologies, que « *l'Europe a investi très tôt dans les nanosciences et les nanotechnologies et a créé une solide base de connaissances. Néanmoins, le domaine est toujours à son début et davantage de connaissances fondamentales doivent être acquises. L'Europe devrait renforcer son excellence scientifique et la compétition entre ses équipes de recherche. À tous les niveaux, les dépenses en R&D devraient être augmentées de manière à compenser les importants investissements réalisés par nos principaux concurrents. Ce qui exige des efforts tant de la part du public que du secteur privé* »[2686].

En France, un « programme multidisciplinaire « Nanosciences et Nanotechnologies » » a été amorcé prévoyant « *un investissement de 210 millions d'euros sur la période 2005-2007, autour de quatre thématiques prioritaires : nano-objets, nano-composants, nanobiosciences et nanomatériaux* »[2687]. De plus, l'effort public français en matière de R&D, même s'il est difficile à cerner avec exactitude, s'avère être également en croissance continue, et, en ce qui concerne le financement public de la recherche en nanotechnologies, celui-ci augmente de « *l'ordre de plus de 10 % par an.* [Ainsi] *de 2001 à 2005, plus de 1 milliard d'euros ont été consacrés à la R&D publique dans les secteurs des nanomatériaux, de la nanoélectronique, de l'électronique moléculaire et des nanotechnologies. Pour l'année 2007, l'effort public est de l'ordre de 280 millions d'euros. Un quart du budget est abondé par le ministère en charge de la recherche, un quart par le CEA*[2688] *et un tiers par le CNRS. Les 20 % restants relèvent principalement du Ministère de l'Économie, de l'industrie et de l'emploi, et à moins de 5 % de l'INSERM et*

[2686] Communication de la Commission, « Vers une stratégie européenne en faveur des nanotechnologies », Office des publications officielles des Communautés européennes, 2004, p. 1 ; Disponible en ligne : https://ec.europa.eu/research/industrial_technologies/pdf/policy/nano_com_fr_new.pdf

[2687] Avis du Conseil Économique et Social, « Les nanotechnologies », présenté par M. A. Obadia rapporteur, au nom de la section des activités productives, de la recherche et de la technologie, Avis N° 21, La documentation française, juin 2008, p. 17 ; Disponible en ligne : https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000408.pdf

[2688] CEA, « Le CEA, acteur clef de la recherche technologique », Présentation générale publiée le 4 mai 2021 : « *Acteur majeur de la recherche, du développement et de l'innovation, le CEA intervient dans quatre domaines : la défense et la sécurité, les énergies bas carbone (nucléaire et renouvelables), la recherche technologique pour l'industrie et la recherche fondamentale (sciences de la matière et sciences de la vie). S'appuyant sur une capacité d'expertise reconnue, le CEA participe à la mise en place de projets de collaboration avec de nombreux partenaires académiques et industriels.* » : https://www.cea.fr/Pages/le-cea/acteur-clef-de-la-recherche-technologique.aspx#/scene_lmj_1/

d'OSEO-Anvar[2689] »[2690]. Quant à la dernière orientation française en matière de défense et de sécurité, elle avance, suivant les mêmes logiques, que « *dans un contexte d'incertitude sur l'environnement stratégique et d'évolution permanente de la menace, le maintien de l'ambition de couvrir tous les domaines industriels et techniques devient plus prégnant et requiert l'augmentation du niveau des ressources budgétaires dédiées à la S&T (science, recherche, technologie et innovation)* », et que cet effort financier « *rendra également possible une démarche exploratoire accrue dans les domaines technologiques porteurs de ruptures et issus du domaine civil (intelligence artificielle, robotique et autonomie décisionnelle, mise en réseau des systèmes, nouveaux matériaux, biotechnologies...)* »[2691].

En fonction de l'utilisation des objets connectés et intelligents, de nombreuses données, pour la plupart des données « sensibles », sont créées, transmises et diffusées. De multiples outils permettant, en outre, la traçabilité des activités au quotidien sont de nos jours utilisés couramment, générant également de nombreuses données personnelles à caractère parfois sensible, révélatrices des habitudes, préférences et comportements de leurs utilisateurs, des données pouvant être, de surcroît, facilement désanonymisées, comme il a pu être observé à travers cette étude. Ces différents objets produisant lesdites données intimes et personnelles peuvent non seulement servir au profilage, à la création de dossiers détaillés uniformes, au ciblage des individus, mais peuvent également être détournées à des fins d'espionnage industriel et commercial, eu égard à la forte motivation et à la demande de la société ainsi qu'aux soucis de compétition et de concurrence accompagnant tout développement dans le marché. Les analyses génétiques, ou les analyses d'ADN et de tissus humains seraient-elles alors le tout dernier secteur marchand compétitif comparable, suivant la logique économique,

---

[2689] Rapport d'information n° 220 (2006-2007), au nom de la commission des Finances, du contrôle budgétaire et des comptes économiques de la Nation sur l'enquête de la Cour des comptes relative au fonctionnement de l'Agence nationale de valorisation de la recherche (ANVAR) et à sa transformation en OSEO-ANVAR, par M. Maurice BLIN, déposé au Sénat le 7 février 2007, Annexe Communication de la Cour des comptes à la commission des finances du Sénat sur l'agence nationale de valorisation de la recherche (ANVAR) et sa transformation en OSEO-ANVAR (p. 55), p. 7, §3 Statut et mission de la société anonyme OSEO ANVAR : « *La réforme de l'ANVAR faite en 2005 traduit la volonté des pouvoirs publics de permettre aux PME de trouver, au sein d'une même entité juridique et financière, une gamme de produits et prestations qui leur est dédiée. OSEO ANVAR est régie par les textes de 2005 précités et les dispositions générales applicables aux sociétés anonymes. Ses parts sont détenues à 100 % par un nouvel établissement public industriel et commercial de l'État, OSEO, qui a OSEO BDPME comme autre filiale principale.*
L'article 7 de l'ordonnance n° 2005-722 du 29 juin 2005 fixe comme suit les missions d'OSEO ANVAR : « promouvoir et de soutenir le développement industriel et la croissance par l'innovation, notamment technologique, ainsi que contribuer au transfert de technologies. [OSEO ANVAR] peut se livrer à toutes activités de service, de conseil, de financement ou de mobilisation de ressources complémentaires, et d'expertise, aux échelons local, national, communautaire et international, de nature à soutenir la croissance des entreprises innovantes. » » ; Disponible en ligne : https://www.senat.fr/rap/r06-220/r06-2209.html ; https://www.senat.fr/rap/r06-220/r06-2201.pdf

[2690] Avis du Conseil Économique et Social, « Les nanotechnologies », *Id.*, p. 17.

[2691] Revue Stratégique de défense et de sécurité nationale 2017, *loc. cit*., p. 70, points 231-232.

à celui qui s'était mis en place lors des percées en matière d'analyses statistiques des concepteurs des scores et cotations des organismes financiers ? À ce titre, la CNIL annonce que *« le domaine des données génétiques va aussi constituer un « champ de bataille » considérable (médecine prédictive, assurances, traitement automatisé de l'ADN...) auquel les acteurs de la régulation et les citoyens ne sont pas du tout préparés* »[2692].

De façon générale, il est frappant de constater la rapidité avec laquelle les sciences cognitives, et les nanosciences et neurosciences se sont insinuées dans la société et le quotidien des individus : il est fréquemment question de neuro-marketing, neuro-psychanalyse, neuro-justice, neurotechnologie, nanotechnologie, nanomonde, nanotubes, nanomètres, nanomatériaux, nano-émulsions, nano-pigments, biotechnologie, ou encore bionique. Le tout manifesté, souvent, « *dans un contexte idéologique de réductionnisme biologique des comportements et de défiance vis-à-vis de tout ce qui passe par la conscience humaine* »[2693], la « conscience » étant un « mot qui fait cruellement défaut dans le débat actuel » entourant, notamment, les biotechnologies et les nano et neuro technologies ; or, « rappelons-nous », note Delmas-Marty, que « *lors des travaux sur l'article 1 de la DUDH, les rédacteurs avaient ajouté à la « raison » le mot « conscience » […]* »[2694]. C'est à travers l'ensemble de ces développements et avancées technologiques et scientifiques qu'il est, par exemple, aisé et facile d'explorer et d'analyser les actions et activités de la vie quotidienne des personnes, leurs habitudes, passions, préférences, achats, fréquentations et groupes sociaux, préférences ou habitudes de navigation, dans le but de mieux les comprendre, de mieux les appréhender, de mieux prédire leurs besoins et leurs décisions d'achats et de mieux les profiler et les cibler, de façon encore plus personnalisée, singulière et individualisante ; l'ensemble assidûment orienté vers la demande et la logique du marché.

Les nanotechnologies semblent correspondre à un terme collectif englobant différentes branches des nanosciences et des nanotechnologies qui, à la fois, constituent des nouvelles approches en matière de recherche et développement « *visant à maîtriser la structure fondamentale et le comportement de la matière au niveau des atomes et des molécules* »[2695]. Les nanotechnologies renvoient, dans ce cadre, « *aux activités scientifiques et technologiques menées à l'échelle atomique et moléculaire, ainsi qu'aux principes scientifiques et aux*

[2692] CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », 2012, p. 28-29 : https://www.cnil.fr/sites/default/files/typo/document/CNIL-CAHIERS_IPn1.pdf

[2693] CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », *Id.*, p. 29.

[2694] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 91.

[2695] Communication de la Commission, « Vers une stratégie européenne en faveur des nanotechnologies », *Id.*, p. 3 ; et, Avis du Conseil Économique et Social, « Les nanotechnologies », *Id.*, p. 10-11 (Définition assez similaire).

propriétés nouvelles qui peuvent être appréhendés et maîtrisés au travers de ces activités » ; ces propriétés pouvant être observées et exploitées pour mettre au point des dispositifs et des matériaux dotés de « *fonctions et de performances nouvelles* »[2696]. Ainsi, souligne la Communication de la commission, « *les applications des nanotechnologies font actuellement leur apparition et auront demain des incidences dans la vie de chacun* »[2697] ; et le Conseil économique et social indique à cet égard : « *technologies transversales, irriguant de multiples secteurs d'activités, révélant et libérant des capacités que la matière ne dévoile pas à un niveau supérieur d'agrégation, les nanotechnologies recèlent un potentiel de développement économique et de création d'emplois incontournable pour le devenir de notre pays et celui de l'humanité toute entière. Elles ouvrent sur un monde où les frontières traditionnelles entre la physique, la chimie, la biologie et l'ingénierie s'estompent voire disparaissent, où l'inerte et le vivant se rejoignent […]* »[2698].

En ce qui concerne les neurotechnologies, elles désignent un ensemble d'outils techniques et informatiques permettant de mesurer et d'analyser les signaux chimiques et électriques émis par le système nerveux, que ce soit le cerveau ou les nerfs dans les membres. Elles sont employées afin de déterminer les propriétés de l'activité nerveuse, comprendre le fonctionnement du cerveau, diagnostiquer des affections et émotions ou contrôler des appareils externes, tels que neuroprothèses ou les interfaces cerveau-machine par exemple, dans le but, notamment, d'améliorer les facultés cérébrales et le bien-être des individus. Ces neurotechnologies sont, plus précisément, définies comme « *the assembly of methods and instruments that enable a direct connection of technical components with the nervous system. These technical components are electrodes, computers, or intelligent prostheses. They are meant to either record signals from the brain and "translate" them into technical control commands, or to manipulate brain activity by applying electrical or optical stimuli* »[2699].

Quant aux biotechnologies, elles se réfèrent à « *un ensemble de technologies apparentées ayant des applications dans un grand nombre de secteurs économiques – agriculture, sylviculture, aquaculture, extraction minière, raffinage du pétrole, remise en état de l'environnement, santé humaine et animale, transformation des aliments, chimie, systèmes de sécurité – et dans de*

[2696] Communication de la Commission, « Vers une stratégie européenne en faveur des nanotechnologies », *Ibid.*, p. 4.
[2697] Communication de la Commission, « Vers une stratégie européenne en faveur des nanotechnologies », *Ibidem*, p. 3.
[2698] Avis du Conseil Économique et Social, « Les nanotechnologies », *Id.*, p. 7.
[2699] O. MÜLLER et S. ROTTER, "Neurotechnology: Current Developments and Ethical Issues", Frontiers in systems Neuroscience, Vol. 11 n° 93, publié le 13 décembre 2017 : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5733340/

nombreux procédés industriels », ouvrant la voie à une multitude d'applications diverses et présentant des impacts économiques, environnementaux et sociaux non négligeables[2700]. Cette définition est, selon l'OCDE, délibérément large incluant plusieurs domaines de la biotechnologie moderne mais aussi beaucoup d'activités classiques, et ce en raison des nombreux développements que ce secteur, et celui de la collecte des données, peut subir[2701]. À ce titre, elle propose, pour des raisons statistiques, une définition unitaire, tout en précisant qu'elle n'est aucunement exhaustive et qu'elle demeure à titre indicatif, qui est la suivante : « *L'application de la science et de la technologie à des organismes vivants, de même qu'à ses composantes, produits et modélisations, pour modifier des matériaux vivants ou non-vivants aux fins de la production de connaissances, de biens et de services* »[2702].

L'OCDE fournit à cet égard une liste de « techniques de biotechnologie » destinée à être employée comme un guide d'interprétation de la définition unitaire, mais qui est elle aussi « indicative et non exhaustive » en raison des nombreuses avancées potentielles dans ce domaine et celui du recueil et du traitement des données, liste dans laquelle sont énumérés les « ADN/ARN : génomique, pharmacogénomique, sondes géniques, génie génétique, détermination de séquences/synthèse/amplification de l'ADN/ARN, profil de l'expression génique et utilisation de la technologie antisense », les « protéines et autres molécules : détermination de séquences/synthèse/ingénierie des protéines et peptides (y compris les hormones à grosse molécule) ; amélioration des méthodes d'administration des médicaments à grosse molécule ; protéomique, isolation et purification des protéines, signalisation, identification des récepteurs cellulaires », la « culture et ingénierie des cellules et des tissus : culture de cellules/tissus, génie tissulaire (y compris les structures d'échafaudage tissulaires et le génie biomédical), fusion cellulaire, vaccins/stimulants immunitaires, manipulation embryonnaire », les « vecteurs de gènes et d'ARN : thérapie génique, vecteurs viraux », la « bioinformatique : construction de bases de données sur les génomes, les séquences de protéines ; modélisation de procédés biologiques complexes, y compris les systèmes biologiques », ou encore la « nanobiotechnologie : applique les outils et procédés de

[2700] OCDE, « Statistiques des biotechnologies : Méthodologie », Direction de la science, de la technologie et de l'innovation, 2005-2006, p. 1 : http://www.oecd.org/fr/science/tech-emergentes/40222697.pdf
[2701] OCDE, « Définition statistique de la biotechnologie », Direction de la science, de la technologie et de l'innovation, Les technologies émergentes, mise à jour en 2005 : http://www.oecd.org/fr/sti/tech-emergentes/definitionstatistiquedelabiotechnologiemiseajouren2005.htm
[2702] OCDE, « Définition statistique de la biotechnologie », *Id.*

nano/microfabrication afin de construire des dispositifs permettant d'étudier les biosystèmes, et des applications dédiées aux diagnostics, à l'administration des médicaments, etc. »[2703].

Comme il a pu être observé dans cette recherche, non seulement de plus en plus de données personnelles sont récoltées par les objets employant des techniques nanotechnologiques, neurotechnologiques ou biotechnologiques, mais de plus en plus de données pouvant être qualifiées de « sensibles », au sens du RGPD, le sont également, y compris les données biométriques, génétiques ou celles relatives à la santé ; l'ensemble étant porteur d'informations extrêmement révélatrices sur la constitution physique, biologique, psychique et mentale des individus concernés, renforçant son individualisation et sa singularisation. Précisément, les outils du *quantified self* et les objets connectés intelligents[2704], utilisés régulièrement pour améliorer sa santé ou ses performances physiques par exemple, fournissent une quantité astronomique de données permettant, désormais, d'analyser le corps humain et sa constitution biologique unique, y compris ses comportements et habitudes en matière de santé, afin de contribuer au bien-être de la personne, et ont la possibilité de contribuer éventuellement à son amélioration voire à sa fabrication. Pourtant, plusieurs témoignages ont récemment révélé que les montres intelligentes, notamment les *FitBit*[2705], destinées à aider les personnes physiques dans l'amélioration de leur santé et leurs activités et performances physiques, créaient du stress, des allergies ou des réactions corporelles nocives et exerçaient beaucoup de pression sur les personnes les utilisant, quitte à affecter leur santé mentale, psychique et physique[2706].

[2703] OCDE, « Définition statistique de la biotechnologie », *Id.* ; et OECD, « Biotechnology Statistics », rédigé par B. van Beuzekom et A. Arundel, 2006, p. 7 : http://www.oecd.org/science/inno/36760212.pdf

[2704] *Cf.* p. 156, 408 et 430.

[2705] *Cf.* p. 411-412 et 443.

[2706] Par ex.: S. POPE, "Why a Fitbit Harms More Than Helps Your Healt", The healthy home economist, du 29 mai 2019: "*In March 2014, the Consumer Product Safety Commission officially recalled the Fitbit Force due to injuries to an estimated 9,900 people. These customers suffered from skin irritations such as blisters, rashes, and peeling skin after the continual wearing of the Fitbit Force for a period of time. Fitbit stated that after consulting with medical professionals, the general assessment is that the skin problems were likely allergic reactions to nickel, an alloy in the stainless steel or adhesives used to assemble the Fitbit Force*.": https://www.thehealthyhomeeconomist.com/fitbit-health-concerns/ ; I. JOVIN, "Some Fitbit users are reporting "shocking" side-effects", Gadgets & Wearables, du 23 mai 2018: "*[…] a number of users in America say that instead of promoting good health, the device on their wrist is causing them pain. Some have posted their complaints on the company's community forums. Do a search and you'll find a number of threads flagging up the issue*.": https://gadgetsandwearables.com/2018/05/23/fitbit-shock/ ; K. JOHNSON, "Dangerous Side Effects Reported From Popular Fitness Trackers", New York CBS local news, du 21 mai 2018: "*There's a new warning for anyone who wears a fitness tracker after some dangerous side effects have been reported. Instead of promoting good health, some have led to a fitness fail.*": https://newyork.cbslocal.com/2018/05/21/fitbit-fitness-fail/ ; R. VITT, « Témoignage : un mois avec une montre connectée c'est effrayant », Phonandroid, du 26 octobre 2015: « *[…] cette montre connectée m'a donné cette sensation que je ne contrôlais plus la situation. Et plutôt que d'être un outil pratique, il est devenu envahissant. Je n'avais plus le contrôle sur la technologie, c'est elle qui prenait le contrôle sur moi. J'agissais selon les informations qu'elle me fournissait. Elle ne me servait*

Déjà, en 2012, Google, avec toutes les données qu'il détient, celles auxquelles il a accès ou qu'il se procure aisément, un des développeurs initiaux de voitures autonomes et de lunettes à réalité augmentée, a, de plus, créé un « cerveau informatique », un réseau neuronal de machines « intelligentes » capables d'apprendre seules, constitué de 16 000 processeurs et connecté à internet où « il étanche sa soif de connaissances à partir d'images extraites de dix millions de vidéos YouTube »[2707]. Par ailleurs, la même année, R. Kurzweil, inventeur de plusieurs technologies, telles que les technologies d'analyses automatiques de caractères ou de la voix, « futurologue » célébré pour ses idées transhumanistes, notamment aux États-Unis, et rédacteur de nombreux ouvrages relatifs à l'allongement de la vie et du futur de l'intelligence artificielle, des nanotechnologies, de la robotique et des biotechnologies[2708], a rejoint Google en tant que « director of engineering » avec une mission définie : « *faire avancer la capacité de Google à comprendre le langage naturel et les mécanismes du cerveau, de l'apprentissage. Ray Kurzweil rejoint Google parce qu'il s'agit de l'une des organisations les mieux dotées dans le monde pour atteindre ses objectifs en termes de « machine learning » et d'intelligence artificielle* »[2709]. En outre, grâce aux idées de ce futurologue et, notamment, à sa vision sur la « Singularité », une « Université de la Singularité » a été fondée par différentes entités, les contributeurs principaux étant Google et la NASA, qui correspond à une entreprise privée californienne représentant à la fois une institution académique privée, un *think-tank* et un centre d'incubation des entreprises, grandement promue depuis 2009 par Google et la NASA et prévoyant depuis 2015 d'ouvrir des antennes en France[2710]. Elle se présente comme « *preparing Global Leaders and*

---

plus à être plus productif, elle polluait littéralement mon espace. Elle altérait ma concentration. » : https://www.phonandroid.com/temoignage-mois-avec-montre-connectee-effrayant.html

[2707] P. FONTAINE, « Google crée un cerveau informatique capable de reconnaître un chat », 01net.com, du 26/06/2012 : https://www.01net.com/actualites/google-cree-un-cerveau-informatique-capable-de-reconnaitre-un-chat-569065.html, et CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », *Id.*, p. 29.

[2708] Les plus célèbres étant : R. KURZWEIL, *The Age of Spiritual Machines : When Computers Exceed Human Intelligence*, Ed. Penguin Books, 2000; R. KURZWEIL, *The Singularity Is Near: When Humans Transcend Biology*, Ed. Penguin Books, 2006; R. KURZWEIL, *How to Create a Mind: The Secret of Human Thought Revealed*, Ed. Penguin Books, 2013.

[2709] CNIL – Cahier IP Innovation & Prospective N° 02, « Le corps, Nouvel objet connecté », 2014, p. 39 ; Disponible en ligne : https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf ; également annoncé par l'équipe de Google Brain, Google AI, « Healthcare and biosciences » : https://ai.google/healthcare/ ; https://guce.techcrunch.com/copyConsent?sessionId=3_cc-session_d876be65-e903-44d1-9f6f-6c1e3e0852e8&lang=en-US ; et, Kurzweil Network | accelerating intelligence, « Ray Kurzweil biography » : https://www.kurzweilai.net/ray-kurzweil-biography ; http://www.kurzweiltech.com/aboutray.html

[2710] C. ENJALBERT, « L'Université de la Singularité arrive en France », Philosophie magazine, du 28/07/2015 : « *L'Université de la Singularité, fondée aux États-Unis et prônant l'étude des technologies émergentes afin d'améliorer le futur de l'humanité, prévoit d'établir une antenne parisienne d'ici la fin de l'année 2015.* » : https://www.philomag.com/lactu/breves/luniversite-de-la-singularite-arrive-en-france-11947 ; B. Le CORRE, « Bientôt à Paris, une très singulière « université » », Nouvel Obs, du 8 juillet 2015 : « *[…] on comprend le message : l'université de la Singularité a vocation à former des individus singulièrement intelligents*. » : https://www.nouvelobs.com/rue89/rue89-nos-vies-connectees/20150708.RUE9807/bientot-a-paris-une-tres-

Organizations for the Future : Explore the opportunities and implications of exponential technologies and connect to a global ecosystem that is shaping the future and solving the world's most urgent problems » ; la formation de cette "université" visant ainsi à « *equip you with the mindset, tools, and resources to successfully navigate your transformational journey to the future. We are powered by our world class faculty, trailblazing practitioners, and global network of alumni, partners, and impact startups* »[2711].

La "Singularité", notion popularisée par Kurzweil qui prévoit qu'elle prendra corps avant la moitié du XXI[e] Siècle, désigne « le moment où l'augmentation exponentielle de la puissance de calcul des ordinateurs fera émerger une intelligence supérieure à l'intelligence humaine », c'est donc un seuil au-delà duquel « l'intelligence artificielle aura surpassé l'intelligence humaine »[2712]. Il semble bien que le développement et la convergence des biotechnologies, des sciences cognitives, des nanotechnologies et de l'intelligence artificielle annoncent la transformation radicale de l'humanité et l'avènement de l'homme-machine fabriqué. En effet, tout permet de penser, indique le Professeur Gil, que, bientôt, « *il sera possible de décrypter les processus mentaux mais aussi d'agir sur les mécanismes cérébraux qui sous-tendent les intentions, les émotions, les actions, les décisions humaines. Des attributs spécifiquement humains seront ainsi menacés par des groupes de pression, des pirates informatiques voire des gouvernements : il s'agit notamment du respect de la vie privée et de l'agentivité qui est la capacité des êtres humains à décider de leurs propres actes et non d'être agis par des manipulations faites à leur insu dans leur chair en altérant l'entité esprit-cerveau qui les constitue* »[2713].

Par ailleurs, un auteur souligne que « *les nanotechnologies suscitent une sorte de fascination parce que "l'on met de l'intelligence dans des objets". En fait, on confond intelligence et interaction. Les nanotechnologies risquent d'être à l'origine d'une perte d'autonomie de*

---

singuliere-universite.html ; G. LEDIT, « La Singularity University débarque à Bordeaux : « On est là pour animer une communauté locale » », Usbek & Rica du 02/09/2017 : « *« La Singularity University arrive à Bordeaux » : quand on s'intéresse à l'actualité de la Silicon Valley, voilà le genre d'information - repérée par La Tribune Bordeaux - qui intrigue. On se demande quel rapport peut bien exister entre la Singularity University, cette université/think-tank fondée par le plus emblématique des transhumanistes, Ray Kurzweil, et la préfecture de la Gironde.* » : https://usbeketrica.com/article/la-singularity-university-debarque-a-bordeaux-on-est-la-pour-animer-une-communaute-locale ; et Paris Singularity : http://paris-singularity.fr

[2711] Singularity University : https://su.org

[2712] CNIL – Cahier IP Innovation & Prospective N° 02, « Le corps, Nouvel objet connecté », *Id.*, p. 39.

[2713] R. GIL, « Neurotechnologies : Prendre conscience de leurs dangers éthiques », Espace éthique Poitou-Charentes, janvier 2018, p. 1, où l'auteur précise que « *Le concept d'agentivité désigne, selon le psychologue américain Albert Bandura, la capacité des individus à être des agents actifs de leur propre vie, c'est-à-dire à exercer un contrôle et une régulation de leurs actes.* » (note de bas de page n° 5) : https://www.espace-ethique-poitoucharentes.org/obj/original_140334-cor-neurotechnologies-prendre-conscience-de-leurs-dangers-ethiques.pdf

l'individu sur son environnement. L'exemple du GPS est révélateur : la vision anthropomorphique de l'ordinateur conduit à dire que celui-ci est plus fort que le cerveau humain »[2714]. C'est également ce que suggère Cardon qui indique que « *lorsqu'on questionne des individus lambda sur leur vision de la biométrie, on les interroge plus, finalement, sur leur fascination pour les films de science-fiction que sur leur quotidien et leur vécu... De même, le fait qu'avec la biométrie — comme d'ailleurs aussi avec le « sans contact » — l'impression de « donner » de la donnée soit amoindrie compte tenu des possibilités de capture automatique, ne facilite sans doute pas l'appréhension par le grand public de ces techniques* », de sorte que la biométrie, comme les nanotechnologies, est davantage « subie » par les personnes et « pourra d'ailleurs de plus en plus se faire à leur insu »[2715].

Mais les idéologies transhumanistes et posthumanistes militant pour l'amélioration de la vie humaine grâce à ces nouvelles technologies voient les choses différemment, quoiqu'avec autant de fascination. Précisément, pour ces personnes et celles adeptes de l'université de la singularité, appelées les « bio-progressistes », « la vie s'apparente à une « nano-machine particulièrement sophistiquée », mais aussi largement manipulable », instiguant certaines d'entre elles à tenter d'ores et déjà de « modéliser l'intelligence de l'être humain, son autonomie, sa mémoire, le désir, la douleur, la souffrance, le rêve ou la conscience », l'ensemble de ces travaux visant à faire disparaître, à terme, « toute opposition entre le naturel et l'artificiel, le vivant et le non-vivant, le conscient et son contraire » ; le tout prônant, en outre, l'amélioration de l'individu, de son bien-être, de sa concentration, de ses capacités intellectuelles ou physiques, de son intelligence, de la condition humaine, ou encore l'abolition de la vieillesse, de la souffrance, de la maladie, voire de la mort[2716]. Or, précise Delmas-Marty, « *cet hymne au progrès technologique ne précise cependant pas sur quels critères, quantitatifs ou qualitatifs, sont définis les objectifs de l'humanité. En revanche, on voit déjà comment le cyberespace et les technologies du virtuel, par leurs effets de « dématérialisation » et de « décorporation », favorisent une « désaffectation pour l'humanité qu'il faut prendre au sérieux »* »[2717].

Néanmoins, le processus de développement et d'innovation des techniques et pratiques permettant de « fabriquer » un être humain, milité par les idéologues du trans et post-humanisme, semble être déjà lancé avec l'assistance médicale à la procréation, la sélection

[2714] CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », citation de Dominique Wolton, *Id.*, p. 28.
[2715] CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », *Id.*, p. 25.
[2716] CNIL – Cahier IP Innovation & Prospective N° 02, « Le corps, Nouvel objet connecté », *Id.*, p. 39.
[2717] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 90.

d'embryons, ou encore les technologies visant l'amélioration de l'homme, dites de « *human enhancement* », « l'homme augmenté ou amélioré », largement facilité aujourd'hui par toutes les données personnelles, y compris génétiques ou biométriques, collectées et exploitées en masse. Déjà, à l'heure actuelle, il existe au moins sept façons différentes de fabriquer un enfant, « insémination artificielle intraconjugale, fécondation *in vitro* intraconjugale, insémination artificielle avec donneur (dons d'ovules, de sperme ou d'embryon), injection intra-ovocytaires de spermatozoïdes (*in vitro*) »[2718], amorçant dès lors la banalisation de la « fabrique de l'être humain » et celle du « bricolage du vivant », comme le montre, entre autres, le succès de « La paillasse », « laboratoire communautaire pour les biotechnologies citoyennes » en région parisienne, ayant le soutien de la mairie de Paris[2719]. Par ailleurs, depuis 2002 aux États-Unis, un large programme de recherche, doté de plusieurs milliards de dollars en termes d'investissement, a été consacré à l'approfondissement de « la convergence entre quatre voies technologiques, pour permettre à l'homme de faire mieux que la nature : les biotechnologies et la biologie, notamment génétique, les nanotechnologies, les technologies de l'information et les sciences cognitives » ; convergence appelée depuis la « révolution NBIC »[2720].

De nombreuses technologies sont désormais développées, notamment par des entreprises privées, destinées à être portées, insérées et intégrées au corps humain, comme les interfaces cerveau-machine, « Brain Computer Interfaces (BCIs) », visant à relier les commandes des pensées des individus aux dispositifs du monde, les « Brain-responsive computing systems », systèmes brevetés aspirant à améliorer la productivité et la production des travailleurs, par exemple en utilisant les signaux EEG (électroencéphalogramme) pour déterminer l'état mental de l'utilisateur et adapter l'expérience informatique, ou encore les « "Mindful" wearables » conçus pour améliorer non seulement la santé physique, mais aussi le bien-être mental[2721]. En outre, les techniques de sélection d'embryons, « *un mot qui évoque le fantôme de l'eugénisme* », peuvent dorénavant être négatives, dépistage anténatal et avortement, ou positives, choix d'embryon à implanter ou d'ovocyte à féconder, risquant de conduire à « *un « eugénisme*

[2718] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 85 ; et M. DELMAS-MARTY*, Les forces imaginantes du droit (IV) – Vers une communauté de valeurs ?*, Ed. du Seuil, Coll. La couleur des idées, 2011, p. 227-228.

[2719] CNIL – Cahier IP Innovation & Prospective N° 02, « Le corps, Nouvel objet connecté », *Id.*, p. 40.

[2720] CNIL – Cahier IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », *Id.*, p. 29, et, CNIL – Cahier IP Innovation & Prospective N° 02, « Le corps, Nouvel objet connecté », *Id.*, p. 40.

[2721] Pour plus d'informations : A. FERNANDEZ, "10 Neurotechnologies About to Transform Brain Health and Brain Enhancement", SharpBrains, publié le 10 novembre 2015 : https://sharpbrains.com/blog/2015/11/10/10-neurotechnologies-about-to-transform-brain-enhancement-and-brain-health/; Research Briefs, "21 Neurotech Startups to Watch: Brain-Machine Interfaces, Implantables, and Neuroprosthetics", CBInsights, du 28 janvier 2019 : https://www.cbinsights.com/research/neurotech-startups-to-watch/

libéral » qui laisse aux préférences individuelles des acteurs du marché le choix des finalités qui président aux interventions destinées à modifier les caractéristiques génétiques »[2722].

Il semble de plus en plus urgent et nécessaire d'appliquer les priorités éthiques retenues par le Professeur Gil et de les respecter au regard des nombreuses avancées technologiques en la matière et des nouvelles technologies continuellement créées. Précisément, celui-ci rappelle la nécessité de respecter « la vie privée et le consentement » des individus, prône la garantie du respect de « l'agentivité et de l'identité », ce qui équivaut, précise-t-il, « à l'interdiction de toute manipulation volontaire susceptible d'induire chez l'être humain des pensées, des actions, des émotions qui lui seraient imposées ; il s'agit au fond d'une autonomie revisitée par les progrès technoscientifiques devant être garantie par des traités internationaux », suggère de définir des « limites à fixer à tout ce qui vise à dépasser les capacités humaines » tout en interrogeant les frontières entre « l'humain, le surhumain, le transhumain », et appelle à une prise de conscience « du risque d'exclusion de certains groupes sociaux non pris en compte au stade d'élaboration des algorithmes, négligés ou marginaux »[2723].

Quant à J.-M. Besnier, il déplore le fait que ne soit engagée pour ces questions aucune réflexion existentialiste sur la nature de l'humanité et affirme, en ce sens, que « *ce que veut le transhumanisme, ce n'est pas parfaire l'humanité, mais nous arracher à l'humanité. Faire de nous des êtres qui ne naîtront plus mais qui seront fabriqués, lisser la vie psychique, ne plus vieillir grâce au téléchargement de la conscience, éradiquer la souffrance et donc le plaisir. Le désir même, alors que c'est le moteur de l'humanité... Arrêtons de dire que c'est au service de l'humanité, alors que ce n'est que pour la détruire* »[2724].

Plus encore, selon la Professeure Delmas-Marty, « *conçues pour libérer le corps humain des contraintes biologiques et renforcer l'autonomie de l'être humain en exaltant la liberté individuelle et en améliorant les capacités et la créativité de chacun, elles risquent d'avoir pour effet la marchandisation du corps, qui rapproche la personne de la chose, et le formatage de*

[2722] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 87-88, où l'auteure indique que « *Certes, la loi française de 1994 semble poser un interdit absolu en faisant de l'eugénisme, positif ou négatif, un « crime contre l'espèce humaine », mais elle limite l'incrimination aux « pratiques organisant la sélection », ce qui exclut les pratiques individuelles, légitimées par l'autonomie de chaque individu ou couple. Or le futur marché de la génomique personnelle risque à son tour de brouiller les frontières entre interventions thérapeutiques et interventions à des fins d' « amélioration », rendant plus vraisemblable l'hypothèse, évoquée par Habermas, d'un nouvel eugénisme qui ne viendrait pas de la sélection mais des pratiques permettant de perfectionner l'humain par divers artifices*. »

[2723] R. GIL, « Neurotechnologies : Prendre conscience de leurs dangers éthiques », *Id.,* p. 2.

[2724] CNIL – Cahier IP Innovation & Prospective N° 02, « Le corps, Nouvel objet connecté », *Id.*, p. 41.

la personne, qui tend à diluer l'individu dans l'espèce »[2725], tendance d'ailleurs de la biopolitique susvisée[2726].

B. Qu'en est-il de la *sérendipité* et de l'*irréductible humain* ?

Au regard des développements entrepris jusqu'à présent, il y a lieu de soulever quelques interrogations qui paraissent fondamentales et essentielles pour la « survie » de l'homme, de son identité et ses multiples facettes dynamiques et mouvantes, de sa qualité et sa nature humaine, de ses traits caractéristiques et, en particulier, de son caractère « irréductible » et imprévisible ; *in fine*, pour la survie de « l'être humain ».

En effet, avec les avancées et les développements technologiques et scientifiques, notamment des technologies de l'information et de la communication et de leurs utilisations, qu'en est-il du caractère complexe et polymorphe de l'identité, composée de nombreuses facettes et d'une multitude d'attributs irréductibles et en interaction continue avec son environnement ? Cette identité humaine qui ne semble pouvoir être définie que de manière apophatique, à partir de ce qu'elle n'est pas, à l'image de la définition de la nature humaine ou de ce qui fait que l'humain est humain, un être qui ne peut être déterminé qu'à partir de ce qui est inhumain et qui est le fruit d'un processus constant d'interaction, d'appartenance, de représentation, d'évaluation de soi et d'autoréflexion, est-elle destinée à disparaître, à prendre une autre forme et une autre nature, celle alliant l'humain à l'inhumain, le vivant au non-vivant ?

Précisément, il semblerait qu'à travers son interaction avec le cyberespace, le monde des machines et du numérique, l'identité, caractéristique d'une « singularité quelconque » irréductible, tend à être réduite, unifiée et modélisée en une identité qui soit identifiable, authentifiable, individualisante, personnalisable, incapable d'auto-construction, d'auto-détermination ou d'autoréflexion indépendante et non influencée, non biaisée. En effet, l'identité numérique, ce « networked self »[2727], qui finalement ne représente qu'une transposition, une extension de l'identité perçue, conçue et vécue dans le monde du web, traduite dans un langage informatique, langage composé de données, de signaux et de bits, interagit et affecte l'identité vécue et ressentie physiquement, mais aussi le rôle choisi consciemment ou inconsciemment par l'individu ; les deux étant finalement interchangeables et inséparables. Ces influences et interactions s'opèrent par le biais des nouvelles technologies et du réseau d'internet proposant d'accorder plus d'autonomie et de liberté alors même qu'ils

[2725] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 83.
[2726] *Cf.* p. 602.
[2727] J. E. COHEN, *Configuring the Networked Self, op. cit.*

semblent s'être accaparés de cette identité et de cette nature humaine sous l'impulsion de la connaissance, du savoir ou encore de la préservation de la sécurité et de la sûreté des personnes. Aspirant à plus de liberté, à plus de communication et de connectivité, à plus d'autonomie dans son quotidien, l'homme finalement développe une relation intime avec les technologies répondant à ses aspirations, de sorte qu'il en devient dépendant pendant qu'elles deviennent plus autonomes et indépendantes. Ces outils et objets technologiques, étant en relation et en interaction continue avec le Soi, le fascinant et lui accordant un semblant de liberté non exploitée auparavant, modifient indubitablement la manière dont ce Soi, cette identité, se réfléchit et se construit : « *Computers, like dreams and beasts, are objects against which we can measure ourselves ; they have an evocative quality in that "interacting with them provokes reflection on the nature of the self"* »[2728].

En outre, comme le suggère Turkle, ces objets évocateurs avec lesquels l'individu établit une relation intime et dépendante sont « *notable for their concreteness, intimacy, fluidity of roles, emotional force, libidinal charge, uncanniness, and irreducibility to familiar schisms such as natural/artificial and human/inhuman* »[2729]. Ces objets et outils évocateurs et parlants, devenant toujours plus autonomes et prenant une place importante dans la vie des humains, sont en eux-mêmes irréductibles aux schismes familiers à l'homme, ceux distinguant le naturel de l'artificiel, l'humain de l'inhumain, et semblent à travers leurs usages et exploitations tendre à la réductibilité de l'humain et de son identité. Mais alors, qu'en est-il de « l'irréductible humain » au sens que lui accorde la Professeure Delmas-Marty ? La notion d'irréductible se réfère, au sens strict, à ce « qu'on ne peut réduire, qu'on ne peut ramener, assimiler l'une à l'autre ou les unes aux autres, qu'on ne peut assimiler à quoi que ce soit d'autre, qui a sa nature propre, spécifique, foncièrement originale »[2730] ; or, l'homme, l'être humain, du XXI^{e} Siècle paraît être désormais réduit dans une perspective commune répondant à la « norme », à ses besoins, à ses peurs et à ses angoisses, rendant l'individu et la société ainsi que l'environnement juridique, dans son acception large, centrés sur la prévisibilité, la précaution, la sécurité et la sûreté, ne laissant plus de place au hasard, à l'imprévisibilité ou à la « sérendipité ».

Le droit censé organiser et gérer la société, ses institutions et administrations, ne définit ni l'identité ni l'humain, mais définit à l'inverse ce qui peut être incriminé en matière d'atteinte à l'identité des personnes ou à l'humanité et son environnement, « *comme si le droit hésitait à*

[2728] S. TURKLE "Computational technologies and images of self", *In* Social Research, *Technology and the rest of culture*, Vol. 64, N° 3, 1997, (p. 1093-1111), p. 1093.
[2729] G. HARMAN "Zeroing in on evocative objects", *In* Human Studies, Vol. 31, N° 4, 2008 (p. 443-457), p. 455.
[2730] CNRTL, « Irréductible » : https://www.cnrtl.fr/lexicographie/irréductible

dire cet irréductible humain qui ne se confond ni avec la vie, ni avec la liberté »[2731]. Mais le droit, à la suite du choc vécu par les guerres et les actes inhumains et les « violences déshumanisantes » qui les accompagnent, s'est empressé d'interdire l'inhumain, « *interdire aux États de déroger aux droits de l'homme dits indérogeables et interdire aux hommes de transgresser les valeurs qui sous-tendent la nouvelle catégorie des crimes dits imprescriptibles. Indérogeable et imprescriptible : deux adjectifs qui expriment le caractère intangible de l' « irréductible » humain* »[2732].

Le droit, principalement le droit pénal, dresse une liste de ce qui constituent les « actes ou traitements inhumains » et les crimes contre « l'humanité », fournissant ainsi une énumération de ce qui est interdit afin de protéger l'humain, cet être « irréductible », sans pour autant consacrer le droit de l'humain ou de la nature humaine qui se caractérise par son irréductibilité et imprévisibilité. Précisément, l'humain est irréductible notamment « à toute définition juridique ou philosophique et même à toute dénomination » : « *Hannah Arendt disait que « l'impossibilité de durcir en mots l'essence vivante de la personne » est telle que, dans tout le domaine des affaires humaines, « elle exclut en principe que nous puissions jamais traiter ces affaires comme nous manions les choses dont la nature est à notre disposition car nous savons les nommer »* »[2733]. À ce titre, Delmas-Marty souligne que « *si la nature de l'homme n'est pas « à notre disposition », la multiplication et la globalisation des formes de déshumanisation appellent néanmoins à définir cet inhumain qui donnerait tout son sens à l'objectif de résistance. Et l'on découvre à présent que la nature non humaine n'est pas non plus à notre disposition et qu'il faut transformer notre relation de domination en relation d'interdépendance pour responsabiliser l'humain* »[2734].

Or, comme il a pu être observé, l'homme est aujourd'hui non seulement réduit à ses besoins dans la vie quotidienne mais il semble également réduit à ses peurs, ses incertitudes et angoisses face à un monde qui se présente comme étant toujours plus dangereux et menaçant, tel que continuellement évoqué par les discours politiques et les médias. Avec la mondialisation et la globalisation, la communauté humaine mondiale dans son ensemble paraît être affectée par ces problèmes de « terrorisme » et de « risque et danger » générant un sentiment de peur constant, et, indique Delmas-Marty, c'est particulièrement cette propagation de la peur qui « *aurait ainsi*

[2731] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », RSC, 1994, p. 477.
[2732] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, op. cit.,* p. 126.
[2733] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », *Id.*, p. 477.
[2734] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 126.

facilité la transposition du principe de précaution des risques naturels ou technologiques à la criminalité, réelle ou potentielle, au point de justifier presque sans protestation du public, l'autonomisation de la dangerosité, le scandale des sites noirs et de la torture, ou cette redoutable transposition du concept de traçabilité »[2735].

Une des priorités des États actuels est principalement orientée vers la sécurité et la défense de leur population, tentant, à ce titre, d'observer les comportements et les attitudes et d'analyser toujours plus les informations récoltées afin de pouvoir prévenir et anticiper toute atteinte à cette sécurité et déterminer les risques, les menaces, les individus dangereux ou les ennemis, globaux ou nationaux, pouvant atteindre la société civile et affectant cette quête de la sécurité et de la sûreté totale. Des faits divers sont donc employés pour justifier les orientations politiques du moment qui s'imposent aux citoyens avec la « force de l'évidence », et qui affectent indéniablement les individus composant la société, alors même que ces faits divers, ces risques et menaces avérés ou supposés, permettent « toute sorte de manipulations » et ne sont « rien d'autre qu'une diversion »[2736]. Dès lors, il semblerait que *« la diversion, et la confusion, ainsi créées […], conduisent tout droit à l'illusion qu'il existe un moyen d'abolir le hasard et de prévenir les menaces : exclure toute personne identifiée comme dangereuse. Diversion, confusion et illusion s'unissent alors pour démontrer que la sécurité est un droit qui doit l'emporter sur les libertés et finalement justifier le recours à la force* »[2737].

Mais ce recours à la force couplé à cette identification des individus qualifiés de « dangereux », de menaçants pour la sécurité des citoyens, n'est-il pas en soi un retour à l'inhumain, à la tentation de réduire l'homme à ce qui est perçu de lui plutôt qu'à ce qu'il a fait ? Les réponses apportées par le corpus juridique voulant, pour des raisons de nécessité et d'utilité, éradiquer les menaces et les interdits fournit alors des critères permettant de caractériser l'humain tel que conçu par le droit : « sa singularité, liée au processus culturel de l'humanisation, et son égale appartenance à la communauté humaine, liée au processus biologique de l'hominisation »[2738]. Les principes de nécessité et d'utilité semblent bien représenter des expressions essentielles dans le monde numérique du XXI^{e} Siècle et diriger les orientations poursuivies, et ce, que ce soit du côté des gouvernements et de la loi, ou du côté des entreprises et du marché, traduisant une sorte de retour à l' « homo faber ». En effet, comme a pu le souligner Arendt, « *[…] English*

[2735] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *loc. cit.,* p. 107.
[2736] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *Id.,* p. 107.
[2737] M. DELMAS-MARTY, « Comment sortir de l'impasse ? », *Ibid.,* p. 108, où la Professeure indique à cet égard : « *Quelle meilleure définition de l'impasse que le célèbre texte de Pascal « ne pouvant fortifier la justice, on a justifié la force, afin que la justice et la force fussent ensemble, et que la paix fût, qui est le souverain bien »* ? ».
[2738] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 129.

philosophy from the seventeenth century onward and French philosophy in the eighteenth century adopted the principle of utility as the key which would open all doors to the explanation of human motivation and behavior. Generally speaking, the oldest conviction of homo faber – that "man is the measure of all things" – advanced to the rank of a universally accepted commonplace »[2739], alors même que "man", l'homme dans son humanité et sa nature humaine, peine à être défini ou déterminé.

Le droit et les politiques publiques déterminées, « conçus comme un système de normes » visant à réguler les comportements individuels ou institutionnels et à les rendre conformes aux objectifs et orientations fixés, deviennent, au fil du temps, de plus en plus complexes (dans leur compréhension) et semblent bien mettre de côté cette indétermination dans la définition de l'humain ou de son identité, mais aussi cet aspect imprévisible de l'homme, une des caractéristiques essentielles de l'espèce humaine pouvant induire et provoquer les idées, la créativité, l'adaptabilité, la complexité (dans ses rôles et ses représentations) ou encore l'innovation, si chère à la société numérique. Pourtant, selon Danièle Bourcier, appréhender le droit d'une autre manière, moyennant d'autres théories, systèmes et principes, comme par exemple les systèmes complexes, permet de « visualiser les lieux souvent inattendus de cette complexité » et « force à renouveler certains aspects de la théorie du droit »[2740]. Précisément, indique Bourcier, « *les travaux actuels sur la sérendipité et les effets inattendus des interactions et décisions humaines viennent apporter un éclairage nouveau sur les limites des études d'impacts et de l'évaluation des lois. En traitant le droit comme un éco-système, on ne pense plus l'écart entre la complexité du droit et la complexité du réel comme irréductible, mais on enrichit notre vision du monde en introduisant l'émergence, l'auto-organisation et de la dynamique des phénomènes qu'on observe* »[2741].

Or, compte tenu des pratiques actuelles, il semblerait que la loi et la science visent plutôt à réduire la complexité de l'humain en l'observant dans sa singularité et dans sa collectivité, son

---

[2739] H. ARENDT, *The human condition*, *op. cit.*, p. 306.

[2740] D. BOURCIER, « Régulation juridique, complexité et sérendipité », *In* D. Bourcier, R. Boulet & P. Mazzega (éd.), *Politiques publiques – Systèmes complexes*, *op. cit.*, p. 34-44, et l'auteure souligne ainsi que : « *Dans les disciplines du discours, la complexité d'un message a longtemps désigné un échec de la communication. En droit, la complexité des règles a été qualifiée d'atteinte au principe de la « sécurité juridique » et de nombreux instruments juridiques comme la codification (qui crée une autre complexité) sont mis en place pour y remédier. En effet, comment accepter que les dispositions de la loi soient rédigées de telle façon qu'elles empêchent un citoyen d'en imaginer les conséquences et les acteurs politiques d'en prévoir les impacts ? Le thème de la complexité est donc devenu un sujet transdisciplinaire – certains disent un nouveau paradigme – qui se situe, suivant les disciplines concernées, au carrefour de plusieurs dilemmes pratiques : peut-on la prévoir, l'éviter ? En tentant de l'éviter, c'est-à-dire en simplifiant un phénomène, ne provoque-t-on pas d'autres effets inattendus dans une autre échelle de temps ?* » (p. 34).

[2741] D. BOURCIER, « Régulation juridique, complexité et sérendipité », *Id.,* p. 45.

environnement ambiant et quotidien, tout en gagnant elles-mêmes en complexité et en irréductibilité en vue d'assurer son bien-être. Ces pratiques et techniques révèlent ainsi la soif du savoir qui habite la minorité contrôlant la majorité au titre de la sécurité et de la liberté. Dès lors, afin d'assurer la protection de la société contre les risques, les menaces et les individus dangereux, les gouvernements visent à récolter toujours plus de données et d'informations afin de maîtriser le pouvoir du savoir, celui de pouvoir prédire, prévenir et anticiper les atteintes à sa population. De même, afin d'assurer une bonne gestion de l'entreprise et de ses produits ainsi qu'un rendement efficace et capitalisant, les entreprises récoltent également des données et informations sur les consommateurs pour pouvoir prédire et anticiper leurs besoins et leurs tendances et habitudes marchandes. Cette récolte massive et continue d'informations se justifient, dans leurs discours et visions, par les impératifs du développement de la connaissance et du savoir principalement, évoquant ainsi, d'une part, le principe de « *scientia potestas est* », « *knowledge is power* », « savoir, c'est pouvoir », et, d'autre part, la réduction de l'homme à un objet de « science », capable d'être contrôlé, transformé, modélisé, marchandé, voire fabriqué.

Il semblerait que, de nos jours, ce principe est en quelque sorte muté, sous l'influence de l'ère numérique, pour devenir "pouvoir est le savoir", ou plutôt "le savoir, c'est le pouvoir" mais un pouvoir unidirectionnel. En effet, à l'heure actuelle, la majorité des populations fournit continuellement et quotidiennement une quantité exponentielle d'informations les concernant ou concernant leur environnement, renforçant *ipso facto* le pouvoir du savoir et de la connaissance de la minorité élitiste composée principalement de l'État-entreprise, des entreprises et des scientifiques ; renforcement encore plus facilité par l'alliance sensationnelle observée entre gouvernement et marché[2742]. Mais ce pouvoir du savoir ne semble pas être employé pour le bien-être de l'humain, alors qu'il prétend l'être, mais plutôt pour gouverner, réguler et gérer le bien-être de la personne physique, l'homme-espèce, tel qu'il est déterminé et dicté par les besoins gouvernementaux, médicaux ou entrepreneuriaux du moment : « *s'il existe déjà une communauté mondiale, c'est sans doute celle du (ou des) savoir(s), donc des experts, et cette communauté rend possible le rapprochement entre savoir et pouvoir que je propose d'appeler « expertise mondiale de la gouvernance »* »[2743]. Il est donc légitime de s'interroger sur les nouvelles orientations des politiques de défense et de sécurité, celles du marché et des

[2742] *Cf.* p. 355.
[2743] M. DELMAS-MARTY, *Les forces imaginantes du droit (III) : La refondation des pouvoirs*, Ed. du Seuil, Coll. La couleur des idées, 2007, p. 204.

entreprises, ainsi que celles de la santé ou de l'hygiène publique, mais aussi sur l'ensemble des normes, pratiques et techniques mises en œuvre caractérisant, semble-t-il, « *des méthodes qui permettent le contrôle minutieux des opérations du corps, qui assurent l'assujettissement constant de ses forces et leur imposent un rapport de docilité-utilité* »[2744].

Or, ce dressage des corps et des comportements, contribuant à la production de l'individualité, cette singularité déterminée et attestée, s'effectue et se renforce par le biais d'un accroissement, voire d'une intensification, de la relation de pouvoir par une relation de savoir créant ainsi une réalité qui est « *produite en permanence, autour, à la surface, à l'intérieur du corps par le fonctionnement d'un pouvoir qui s'exerce […] sur ceux qu'on surveille, qu'on dresse et corrige* »[2745]. Cette réalité, indique Foucault, représente l'espace « *où s'articulent les effets d'un certain type de pouvoir et la référence d'un savoir, l'engrenage par lequel les relations de pouvoir donnent lieu à un savoir possible, et le savoir reconduit et renforce les effets de pouvoir. Sur cette réalité-référence, on a bâti des concepts divers et on a découpé des domaines d'analyses : psyché, subjectivité, personnalité, conscience etc. ; sur elle on a édifié des techniques et des discours scientifiques ; à partir d'elle, on a fait valoir les revendications morales de l'humanisme. Mais il ne faut pas s'y tromper […]* »[2746].

Dans ce contexte, tout semble alors faire régner « l'universalité du normatif », et l'homme ne semble être autre que cette individualité, et l'identité l'élément permettant d'asseoir cette individualisation renforçant l'objectivation de l'individu, devenu objet de la science, ainsi que la « nouvelle économie du pouvoir » et la « formation du savoir » : « *[...] si les* [sciences] *ont pu se former et produire dans l'épistémê tous les effets de bouleversement qu'on connaît, c'est qu'elles ont été portées par une modalité spécifique et nouvelle de pouvoir : une certaine politique du corps, une certaine manière de rendre docile et utile l'accumulation des hommes. Celle-ci exigeait l'implication de relations définies de savoir dans les rapports de pouvoir ; elle appelait une technique pour entrecroiser l'assujettissement et l'objectivation ; elle comportait des procédures nouvelles d'individualisation. [...]. L'homme connaissable (âme, individualité,*

[2744] M. FOUCAULT, *Surveiller et punir*, *op. cit.,* p. 161, où l'auteur souligne ainsi que « *dans toute société, le corps est pris à l'intérieur des pouvoirs très serrés qui lui imposent des contraintes, des interdits ou des obligations. Plusieurs choses cependant sont nouvelles dans ces techniques. L'échelle, d'abord, du contrôle : il ne s'agit pas de traiter le corps, par masse, en gros, comme s'il était une unité indissociable, mais de le travailler dans le détail ; d'exercer sur lui une coercition ténue, d'assurer des prises au niveau même de la mécanique – mouvements, gestes, attitudes, rapidité : pouvoir infinitésimale sur le corps actif. L'objet, ensuite, du contrôle : non pas ou non plus les éléments signifiants de la conduite ou le langage du corps, mais l'économie, l'efficacité des mouvements, leur organisation interne ; […]. La modalité enfin : elle implique une coercition ininterrompue, constante, qui veille sur les processus de l'activité plutôt que sur son résultat et elle s'exerce selon une codification qui quadrille au plus près le temps, l'espace, les mouvements […]. »*

[2745] M. FOUCAULT, *Surveiller et punir*, *Id.,* p. 38.

[2746] M. FOUCAULT, *Surveiller et punir*, *Ibid.,* p. 38.

conscience, conduite, peu importe ici) est l'effet-objet de cet investissement analytique, de cette domination-observation »[2747]. Cette domination-observation qui englobe désormais les corps physiques, les corps sociaux et l'ensemble des acteurs sociaux individualisés, caractérisée par le biopouvoir renouvelé susmentionné[2748], semble bien se concrétiser à travers les nouveaux développements technologiques et scientifiques tendant à la docilité-utilité et à améliorer le corps humain, voire à le fabriquer.

En aspirant à renforcer la santé et l'hygiène publique, et à améliorer ou perfectionner le corps humain, l'espèce humaine semble devenir une espèce comme les autres, que la « communauté des experts » modifie et fabrique comme elle modifie et fabrique des espèces animales ou végétales. Mais alors qu'en est-il de la dignité humaine, ce principe qui paraît aujourd'hui dépassé et être à la fois trop étroit et trop imprécis pour conceptualiser le « crime contre l'humanité » ou le « crime contre l'espèce humaine », dernière création du droit qui le distingue du crime contre l'humanité ; d'autant que cette notion de dignité, souligne Delmas-Marty, a « *parfois servi d'argument en faveur de pratiques, comme la censure d'ouvrages ou, plus gravement encore, les politiques d'eugénisme mises en place au début du siècle, non seulement en Allemagne, mais aussi en Europe et aux États-Unis. Précisément, ces politiques préconisaient la « libération », le plus souvent en forme de « suppression », d'un certain nombre d'êtres humains, dans le but de préserver... la dignité humaine. Comme l'écrit Charles Richet en 1913 : « C'est une barbarie que de forcer à vivre un sourd-muet, un idiot ou un rachitique... il y a de la mauvaise matière vivante qui n'est digne d'aucun respect ni d'aucune compassion. Les supprimer résolument serait leur rendre service car ils ne pourront jamais que traîner une misérable existence* » »[2749].

Dès lors, pour redonner à la dignité « sa pleine signification de valeur essentielle à l'homme et à la communauté humaine », son analyse théorique et juridique doit être affinée et renouvelée notamment au regard des dernières avancées technologiques et biotechnologiques qui, certes, « ne mettent pas en cause la vie humaine mais tendent, par exemple, au maintien en vie à des fins d'expérimentation sans but thérapeutique, au développement de l'ingénierie génétique, à l'utilisation d'embryons ou fœtus humains à des fins thérapeutiques, scientifiques, industrielles ou commerciales, à la reproduction asexuée par clonage, à la fabrication de chimères, au croisement homme-machine » ; autant de traitements qui « pourraient modifier l'évolution

[2747] M. FOUCAULT, *Surveiller et punir*, *Ibidem,* p. 356-357.
[2748] *Cf.* p. 602.
[2749] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », *Id.*, p. 479.

biologique, autant de risques de « déshominisation », pourrait-on dire »[2750]. Pourtant, comme l'a si bien relevé Foucault, « *l'homme-machine [...] est à la fois une réduction matérialiste de l'âme et une théorie générale de dressage, au centre desquelles règne la notion de « docilité » qui joint au corps analysable le corps manipulable. Est docile un corps qui peut être soumis, qui peut être utilisé, qui peut être transformé et perfectionné* »[2751].

Il semble ainsi que la question du crime par fabrication de vie doit être posée et analysée, celle-ci commençant à faire son apparition dans les législations et est, en France, rattachée à la protection de l'espèce humaine au titre des « infractions en matière d'éthique biomédicale »[2752]. Or, comme le souligne Delmas-Marty, « *s'il est étonnant d'isoler ainsi l'éthique biomédicale, il est encore plus surprenant de séparer le crime contre l'espèce humaine (eugénisme et clonage) du crime contre l'humanité, et donc de séparer l'évolution biologique (homonisation) et l'évolution culturelle (humanisation) pourtant étroitement associées à l'émergence de l'humanité* »[2753] ; faisant également écho à la surprenante tendance, accentuée dernièrement avec les avancées technologiques, de séparer l'humain de ses différents attributs et facettes identitaires qui, pourtant caractérisent son humanité, ce qui fait qu'il est l'individu qu'il est, avec tous ses rôles et ses représentations et sa singularité quelconque. Face au développement des biotechnologies, des nanotechnologies et des neurotechechnologies, parallèlement à la montée en puissance de ceux qui se proclament « bio-progressistes », il faudrait plutôt, « *tout au contraire, renforcer le lien entre les deux processus d'évolution, biologique (l'hominisation marquée par le souci de survie de l'espèce) et culturelle (l'humanisation et le respect de la dignité humaine)* »[2754].

Tout semble donc tendre au renouveau de l' « homo faber » mais, souligne Arendt, c'est une tendance touchant l'intégralité des développements modernes marqués par l'attitude de l'homme maître de la technique, qui applique son intelligence à la « fabrication » : *« indeed, among the outstanding characteristics of the modern age from its beginning to our own time we find the typical attitudes of the homo faber : his instrumentalization of the world, his confidence in tools and in the productivity of the maker of artificial objects; his trust in the all-comprehensive range of the means-end category, his conviction that every issue can be solved*

[2750] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », *Ibid.*, p. 479, et M. DELMAS-MARTY*, Les forces imaginantes du droit (IV) – Vers une communauté de valeurs ?*, *op. cit.*, p. 97.

[2751] M. FOUCAULT, *Surveiller et punir*, *Id.,* p. 160.

[2752] Code pénal, Chap. I[er] : Des infractions en matière d'éthique biomédicale (Art. 511-1 à 511-28).

[2753] M. DELMAS-MARTY, *Résister, responsabiliser, anticiper, Id.,* p. 130.

[2754] M. DELMAS-MARTY*, Les forces imaginantes du droit (IV) – Vers une communauté de valeurs ?*, *Id.*, p. 97.

and every human motivation reduced to the principal of utility; his sovereignty, which regards everything given as material and thinks of the whole of nature as of "an immense fabric from which we can cut out whatever we want to resew it however we like"; his equation of intelligence with ingenuity, that is his contempt for all thought which cannot be considered to be "the first step… for the fabrication of artificial objects, particularly of tools to make tools, and to vary their fabrication indefinitely"; finally, his matter-of-course identification of fabrication with action »[2755].

Ces divers et nombreux exemples révèlent dès lors l'urgence qu'il y a à mieux cerner et à mieux préserver l'irréductible humain, sa singularité quelconque tout comme son appartenance à l'humanité, et à se détacher de l'impulsion et des aspirations réductibles visant simplement à protéger et à préserver la vie humaine ou la dignité humaine. Finalement, « *si l'on admet la singularité et l'égale appartenance comme composantes de l'humanité comprise comme pluralité d'êtres uniques, cela revient à dire que l'expression de crime contre l'humanité pourrait désigner toute pratique délibérée, politique, juridique, médicale ou scientifique, comportant* ***soit*** *la violation du principe de singularité (exclusion pouvant aller jusqu'à l'extermination de groupes humains réduits à une catégorie raciale, ethnique ou génétique ou, à l'inverse, fabrication d'êtres identiques),* ***soit*** *celle du principe d'égale appartenance à la communauté humaine (pratiques discriminatoires, telles que l'apartheid, création de « sur-hommes » par sélection génétique ou de « sous-hommes » par croisement d'espèces)* »[2756].

Enfin, eu égard à l'ensemble de ces développements laissant peu de place à l'imprévisible ou au hasard, émerge une dernière question fondamentale, qui reste pour le moment sans réponse selon cette thèse, tout autant que les autres questions susvisées : qu'en est-t-il de la sérendipité au sens que lui accorde Danièle Bourcier ? Cette sérendipité qui est « inhérente à la conduite humaine », qui désigne « la capacité de découvrir, d'inventer, de créer ou d'imaginer quelque chose de nouveau sans l'avoir cherché »[2757]. Ce phénomène de sérendipité, qui « intéresse toutes les disciplines scientifiques, y compris le droit et la politique », intégrant le hasard et l'imprévu, dans la mesure où, de façon pragmatique, une « vraie découverte, invention, création, est toujours la combinaison d'un élément étonnant, se manifestant généralement *a*

[2755] H. ARENDT, *The human condition*, *Id.*, p. 305-306.
[2756] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », *Id.*, p. 483.
[2757] P. van ANDEL et D. BOURCIER, *De la sérendipité – Dans la science, la technique, l'art et le droit : Leçons de l'inattendu*, Ed. L'Act Mem, Coll. Libres Sciences, 2009, p. 11.

priori, et d'une vérification pertinente, ayant lieu *a posteriori* »[2758]. En effet, précisent P. van Andel et D. Bourcier, « *la recherche systématique et la sérendipité ne s'excluent pas, au contraire elles se complètent et même se renforcent. Dans la recherche et en général dans l'action, il faut planifier. Mais un plan n'est jamais sacré : des milliers d'événements inattendus ou d'effets non anticipés interviennent dans le cours d'une expérience ou d'un projet [...]* »[2759]. Définie de nombreuses fois et de nombreuses façons dans les dictionnaires anglais, il semblerait que la sérendipité se réfère particulièrement à deux types de caractérisations, l'idée d'une aptitude personnelle et celle d'un phénomène objectif : « *en tant qu'aptitude personnelle, la sérendipité peut être décrite comme une faculté, une capacité, un talent, dont le développement, inégal d'un individu à l'autre, est considéré soit comme une donnée naturelle, soit comme le fruit d'un apprentissage. [...]. En tant que phénomène objectif, elle se présente sous la forme d'un processus cognitif dont les diverses définitions accentuent tel ou tel aspect : observation, interprétation, raisonnement, explication, etc.* »[2760] ; caractéristiques que la « communauté des experts » actuelle tend à réduire à la prévisibilité, la prédictibilité, l'attendu, la certitude, etc.
In fine, comme le soulignent si bien ces auteurs, « *la sérendipité ne commence pas par une savante hypothèse ou avec un plan déterminé. Elle n'est pas non plus due seulement à un accident ou au hasard. Les milliers de grandes ou petites innovations qui ont jalonné l'histoire de l'humanité ont un élément commun : ils n'ont pu se transmettre que parce qu'un observateur, un expérimentateur, un artiste, un chercheur à un certain moment ont su tirer profit de circonstances imprévues* »[2761].

[2758] P. van ANDEL et D. BOURCIER, *De la sérendipité*, *Id.,* p. 12.
[2759] P. van ANDEL et D. BOURCIER, *De la sérendipité, Ibid.,* p. 12.
[2760] P. van ANDEL et D. BOURCIER, *De la sérendipité, Ibid.,* p. 34.
[2761] P. van ANDEL et D. BOURCIER, *De la sérendipité, Ibidem,* p. 11.

Conclusion

« *Si je devais écrire un livre pour communiquer ce que je pense déjà, avant d'avoir commencé à écrire, je n'aurais jamais le courage de l'entreprendre. Je ne l'écris que parce que je ne sais pas encore exactement quoi penser de cette chose que je voudrais tant penser. [...] Je suis un expérimentateur en ce sens que j'écris pour me changer moi-même et ne plus penser la même chose qu'auparavant* »[2762].

L'identité, « en tant que production sociale et cognitive, vise la relation qui s'établit entre l'individu et son environnement »[2763], une relation qui a subi différentes influences aussi diverses que variées et qui se construit, au XXI^e^ Siècle, dans un environnement imprégné de nouvelles technologies de l'information et de la communication et de l'évolution d'internet et du cyberespace, comme il a pu être observé dans cette recherche, ayant suscité l'émergence de l'identité numérique.

Le XXI^e^ Siècle voit donc l'époque de l'aboutissement de la conception de l'identité à la suite des nombreuses influences conceptuelles occasionnées, au fil du temps, par les courants et mondes sociologiques, philosophiques et juridiques notamment, révélant son caractère transversal et dynamique ainsi que ses facettes indéfinies. En outre, cette époque montre également la valorisation de l'identité en raison de l'influence interactive provoquée par les outils et dispositifs technologiques, valorisation qui se décompose principalement en deux éléments majeurs : la production des masses de données et la parole qui leurs est accordée soulignant en parallèle, l'importance désormais rattachée à l'économie des données. L'identité numérique s'est alors manifestée comme une réalité sociale, et avec l'entrée en vigueur du RGPD et de la loi informatique et libertés modifiée, en particulier, elle consacre simultanément une réalité légale non négligeable. Précisément, cette réalité induit de nouveaux droits numériques et un régime de protection harmonisé, caractérisant l'influence cadre portée par la réglementation européenne en la matière, ainsi qu'une nouvelle dynamique internationale et un régime de protection transfrontalier dénotant l'influence souveraine opérée par la révolution numérique et le nouveau corpus juridique mis en œuvre ; l'ensemble de ces réalités concrétisant l'existence sociale et légale de l'identité numérique.

Comme il a pu être observé dans cette première partie, le respect de la vie privée en ligne et hors ligne s'exprime dans une perspective dynamique, évolutive, en mutation continue,

[2762] M. FOUCAULT, *Dits et écrits*, t. II (1976-1988), Ed. Gallimard, Coll. Quarto, 2001, p. 860.
[2763] M. ZAVALLONI et C. LOUIS-GUÉRIN, *Identité sociale et Conscience, op. cit.,* p. 8-10 ; M. ZAVALLONI, *Égo-écologie et Identité*, *op. cit.* ; et *Cf.* p. 42 et 52.

comprenant, mais sans en être dépendant, la protection des données personnelles, de la vie privée, de la liberté d'expression en ligne, de l'intimité et de la dignité de la personne à travers ces activités numériques ; ces concepts caractérisant, *a fortiori*, celui de l'identité, dans sa dimension numérique ou physique. Il serait dès lors fallacieux de les circonscrire, les délimiter, les réduire à une définition unique, unifiée et/ou arrêtée, voire à une seule conceptualisation théorique.

Étudier la réalité de l'existence sociojuridique de l'identité numérique a, dès lors, préparé et stimulé l'analyse, *in concreto*, de la réalité des enjeux affectant l'identité numérique, soulignant ainsi l'influence pragmatique et équivoque entraînée par la révolution numérique et informatique ainsi que les innombrables types d'opérations de traitement entreprises. *Primo*, cette deuxième partie a révélé l'importance rattachée aux traitements de données personnelles caractérisant, d'un côté, la combinaison d'influences observée entre les secteurs publics et privés confondus, qui mettent, à la fois, en œuvre des structures, modèles et logiciels insouciants et générateurs de tensions et de confusions, techniques comme juridiques, particulièrement entre les notions de liberté et de sécurité, tout en dénotant de l'autre, la lutte d'influences qui en découle en vue d'une gouvernance des identités numériques et des activités et opérations informatiques, mais aussi afin de tirer toujours plus de valeur et d'avantage des capacités et des applications du Big data *via* l'évolution et la portée de l'économie des données et celles des sciences de l'homme et de l'automaticité ; l'ensemble explicitant la réalité économico-sécuritaire des enjeux de l'identité numérique. *Secundo*, cette partie a, par la suite, montré l'importance rattachée aux traitements, plus large, des identités numériques, provoquant conséquemment des changements sociaux, politiques, juridiques et culturels, et asseyant la réalité sociojuridique des enjeux touchant l'identité en question.

En effet, cette analyse a permis de montrer que ce sont les personnes derrières les données qui font l'objet de traitements et subissent subtilement les changements de politique criminelle et de paradigmes socioculturels manifestés, induisant la société de l'information et de contrôle telle qu'elle se présente à l'heure actuelle. Celle-ci s'apparente, de nos jours, à une société de régulation, de prévision, d'anticipation, d'asservissement, de connectivité, de surveillance, de conditionnement, de gestion, d'exception, de communications et résultats instantanés, de réseaux, d'applications, de plateformes et de services en ligne ; société dans laquelle « *Web services are impossible without identity* »[2764], et où l'art de communiquer instantanément et

[2764] L. LESSIG, *Code 2.0*, *op. cit*., p. 52 ; *Cf.* p. 438.

assidûment domine désormais toutes les sphères, qu'elles soient personnelle, professionnelle, médicale, sociale, légale ou administrative. Dans cette perspective, « *l'acte de communiquer ne se traduit pas par le transfert d'information depuis l'expéditeur vers le destinataire, mais plutôt par le modelage mutuel d'un monde commun au moyen d'une action conjuguée : c'est notre réalisation sociale, par l'acte de langage, qui prête vie à notre monde. Il y a des actions linguistiques que nous effectuons constamment : des affirmations, des promesses, des requêtes, et des déclarations. En fait, un tel réseau continu de gestes conversationnels, comportant leurs conditions de satisfaction, constitue non pas un outil de communication, mais la véritable trame dans laquelle se dessine notre identité* »[2765], y compris celle numérique.

L'objectif de cette deuxième partie était donc de souligner face aux développements théorico-juridiques de la première partie, de manière scientifique, juridique, analytique et pragmatique, la réalité de l'identité numérique, l'identité « prise électroniquement » représentant le prolongement de soi dans l'environnement numérique[2766], notamment, les anomalies et les paradoxes qui découlent des traitements dont elle fait l'objet, de leurs finalités et de leurs impacts sur l'environnement juridique dans sa globalité, et sur l'environnement humain et l'identité dans sa singularité.

L'humain, son corps, ses données et sa vie privée semblent donc devenir l'objet et le produit ultime en matière de nouvelles technologies et d'opérations de traitement de données, faisant, *inter alia*, l'objet de négociation, de surveillance, de gestion, de prédiction, de prévision, de computation, de convention et de marchandisation ; pourtant, « *la vie privée n'est pas un produit négociable* »[2767], tout comme le corps humain ne peut être négociable ou en libre disposition moyennant une valeur patrimoniale ou marchande. Ce corps humain « *porte notre personne, sa chair, nous donne un visage, nous identifie : nous sommes un homme, une femme, petit, grand, laid, beau, gros ou maigre. C'est aussi ce corps qui nous expose socialement, nous fait passer de l'identification à l'identité, individuelle certes, mais aussi collective* »[2768]. Le corps physique est donc composé de chair et d'os, celui social de représentations, perceptions

[2765] F. J. VARELA, *Invitation aux sciences cognitives*, *op. cit.*, p. 215.
[2766] *Cf.* p. 592 ; et, Z. BAUMAN, *Le coût humain de la mondialisation*, *op. cit.*, p. 80.
[2767] Communication de la Commission, Échange et protection de données à caractère personnel à l'ère de la mondialisation, *op. cit.,* p. 6.
[2768] S. ETOA, « Corps humain et liberté », *In* Cahiers de la Recherche sur les Droits Fondamentaux, *Le corps humain saisi par le droit : entre liberté et propriété*, N° 15 (p. 19-26), 2017, p. 19-20, point 6, et l'auteur affirme plus loin qu' « *Axée traditionnellement sur la protection du domicile et des correspondances, la notion de vie privée tend toutefois à dépasser ce domaine pour aborder les rivages de l'identité et de l'intimité. Le domaine de la sexualité en est l'exemple paradigmatique.* » (point 10) ; Disponible en ligne : https://journals.openedition.org/crdf/543

et identifications, et, celui virtuel de données, traces, signaux et bits ; l'ensemble interagit et nous expose socialement, et consacre notre faisceau d'identités multiforme et complexe caractérisant notre identité corporelle, civile, sociale, numérique, professionnelle ou personnelle.

Traditionnellement, le corps humain est « *présenté comme un aspect de la personne juridique, et le principe de dignité comme le mécanisme permettant à la fois de protéger l'intégrité physique de la personne et de limiter les droits de cette dernière sur son propre corps* »[2769]. Le droit français proclame le principe de non-patrimonialité du corps humain et la gratuité des actes[2770], signifiant que le corps, ses produits ou éléments ne peuvent faire l'objet d'un échange ou d'une valorisation pécuniaire ou marchande, dénotant ainsi la primauté de la logique personnaliste en Europe face à celle patrimoniale. Cette étude a montré que le droit à la protection des données relève des droits de la personnalité et non du droit de propriété, étayant alors la logique personnaliste dominante en matière de personne physique, de protection de l'humain, de son intégrité et de sa dignité. De ce fait, et suivant la même logique, pourquoi accepter le postulat selon lequel un droit de propriété peut être envisagé sur les données à caractère personnel, une « patrimonialisation ou patrimonialité des données personnelles »[2771], composante de la personne numérique ?

Rattacher une valeur patrimoniale ou une valorisation marchande aux données à caractère personnel apporterai plutôt, au sens de cette étude, une réponse chimérique et génératrice d'ambiguïtés supplémentaires, légales comme sociales, à la lourde problématique du recueil et du traitement indifférencié et continu des données « générées » par les individus-internautes utilisateurs-consommateurs. C'est d'ailleurs déplacer le paradigme vers une admission de mise en valeur et en propriété, de valorisation, de marchandisation et de patrimonialisation, de différentes facettes identitaires au quotidien, d'autant que cela confirme et consolide, en particulier, le nouveau marché numérique et l'économie des données, la cybersurveillance généralisée et ubiquitaire, les nouvelles politiques de sécurité et de défense ainsi que la revivification et l'applicabilité de la cybernétique, du panoptique (Panopticon) et de la

---

[2769] S. ETOA, « Corps humain et liberté », *Id.*, p. 19, point 1.

[2770] Code civil, Art. 16-5 « *Les conventions ayant pour effet de conférer une valeur patrimoniale au corps humain, à ses éléments ou à ses produits sont nulles* », et Art. 16-6 « *Aucune rémunération ne peut être allouée à celui qui se prête à une expérimentation sur sa personne, au prélèvement d'éléments de son corps ou à la collecte de produits de celui-ci* ».

[2771] Par ex. : les travaux du Think Tank "Génération libre" qui milite pour une patrimonialité des données personnelles : Rapport « Aux data, citoyens ! pour une patrimonialité des données personnelles », septembre 2019 : https://www.generationlibre.eu/wp-content/uploads/2019/09/Rapport-Data-II-_-GL_Web.pdf ; Rapport « Mes data sont à moi. Pour une patrimonialité des données personnelles », janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf

biopolitique ; pratiques et stratégies déjà entreprises par les géants du web et/ou les gouvernements et qui doivent fondamentalement constituer l'objet d'une remise en question, notamment scientifique et juridique, à l'aune des nouvelles règlementations, politiques, jurisprudences, cultures et paradigmes en œuvre en la matière.

Quand s'arrête la surveillance à des fins commerciales et commence la surveillance à des fins sécuritaires ? Les frontières sont aussi floues et inexistantes que celles du cyberespace, concrétisant l'assise de l'État-marché et celle du développement audacieux de l'économie des données et de l'économie des sciences de l'homme, et ce sans compter la dynamique et la stratégie des portes tournantes, les « revolving-doors »[2772], susmentionnée ; l'ensemble impactant les libertés individuelles[2773].

En définitive, tous les secteurs confondus se retrouvent aujourd'hui dans le business de l'information et l'économie des données, deux systèmes majeurs pouvant être contrôlés et gérés par les stratégies et les pratiques de la cybersurveillance, la cybernétique, la cybersécurité, la cyberdéfense ou encore de la biopolitique ou du Cryptopticon, chacun en fonction de ses intentions et finalités du moment manifestées[2774] : « *What is money (and all its derivative forms) other than information about how much of our collective goods and services its owner can demand? And what are reputation and search firms establishing other than new currencies for allocating opportunity and attention? All these firms try to process information to score quick gains. But we should never lose sight of the fact that the numbers on their computer terminals have real effects, deciding who gets funded and found, and who is left discredited or obscure* »[2775].

[2772] *Cf.* p. 355 et s. ; et, F. PASQUALE, *The Black Box Society*, *Id.,* p. 216, où l'auteur précise à cet égard que : « *Twenty-first-century revolving-door dynamics present a constant temptation for public servants to "cash out" for private-sector pay-days, leaving them loath to do anything that might disrupt either their own main chance or similar opportunities for their peers and protégés* ».

[2773] Ainsi, « *the stakes are too high for us to ignore this new reality: that politicians and bureaucrats will contravene only so far the interests of a business community they aspire to join or serve. […]. Furthermore, the state's immense powers of compulsion and enforcement can now be enlisted in support of the black box technologies of the search, reputation, and finance sectors. Pundits overlook real dangers to indulge a puerile fixation on the obsolete polarity between "state" and "market" solutions. This is a recipe for paralysis and worse; it is a guarantee that we will never achieve the societal ideals of security, fairness, and dignity that most of us desire, if not always in identical detail. It is time to take a fresh look at where we want to go from here, and at what gets in our way* » : F. PASQUALE, *The Black Box Society*, *Ibid.,* p. 207.

[2774] *Cf.* p. 128 et s., 135 et s., 149 et s., 380 et s., 422 et s., 438 et s., 525 et s., 575 et s., 584 et s., 602 et s.

[2775] F. PASQUALE, *The Black Box Society*, *Ibid.,* p. 215.

Au regard de l'analyse effectuée, il s'est avéré que les nouvelles lois européennes et françaises mises en place sont dépassées et devancées par la nouvelle gestion imposée par le code et l'architecture du cyberespace[2776], et ce au détriment de la liberté, objet philosophique, et des libertés, objets juridiques. En effet, il existe une nette différence en droit entre la liberté, d'une part, et la libre disposition, de l'autre, ramenant la liberté à une faculté d'agir ou de ne pas agir, donc à un pouvoir d'autodétermination : « *la problématique se déplace d'autant puisqu'il n'est plus question de se demander si l'homme est libre dans l'absolu, mais dans quelle mesure les normes juridiques offrent à l'individu la possibilité de se déterminer, autrement dit dans quelle mesure le droit permet à ses sujets d'opérer leurs propres choix* »[2777]. C'est bien cette dernière question qui a été un des fils conducteurs de cette étude en vue d'examiner si le nouveau corpus juridique mis en place permet, de façon concrète et efficace, aux individus d'opérer leurs propres choix, de se déterminer et se développer de manière libre, éclairée et autonome, que ce soit dans l'espace numérique et/ou physique.

Ce point mérite d'être soulevé et débattu scientifiquement, de manière interdisciplinaire et comparée, afin de déterminer si la réglementation prévue en matière de protection des données personnelles accorde, réellement et concrètement, le droit à ses sujets d'opérer leurs propres choix et décisions, et de construire leurs propres pensées et représentations librement. D'autant que, « *[...] l'histoire de la pensée humaine montre que la science, et donc également la science du droit, se libère toujours de l'état de dépendance dans lequel la politique tente continuellement de la maintenir. [...] Dans la lutte incessante du pouvoir contre la pensée, [...], la victoire du pouvoir contre la pensée n'est jamais définitive. Celle-ci organise une résistance d'autant plus forte qu'elle est fréquemment violée et ce, jusqu'à atteindre à nouveau ce qui seul correspond à sa nature propre, à savoir la liberté* »[2778].

Néanmoins, et compte tenu de l'étude entreprise, cela ne semble pas être le cas, la ou les libertés passant au dernier plan face aux différents objectifs, intérêts et finalités manifestés ou poursuivis. Elles font ainsi souvent l'objet d'une mise en balance ou d'une conciliation, voire d'une violation, face à d'autres droits et intérêts conformément au contrôle de proportionnalité entre autres, et ce, sans compter que la pensée est, de manière subtile, consensuelle et participative, influencée et conduite par l'architecture et les réseaux numériques induisant des modes, tendances, cultures, réflexions et comportements du moment, ramenant ainsi le rôle ou

[2776] *Cf.* p. 104 et s., 232 et s., 271 et s., 363 et s., 390 et s., 402 et s., 430 et s., 438 et s.
[2777] S. ETOA, « Corps humain et liberté », *loc. cit.*, p. 19, point 4.
[2778] H. KELSEN, « Qu'est-ce que la théorie pure du droit ? » (1953), *In* Droit et société n° 22, *Transformations de l'État et changements juridiques : l'exemple de l'Amérique Latine*, LGDJ, 1992 (p. 551-568), p. 568 ; Disponible en ligne : https://www.persee.fr/doc/dreso_0769-3362_1992_num_22_1_1187

le choix du rôle à jouer par la personne[2779] à un rôle et des perceptions libres illusoirement ; l'ensemble annihilant, *de facto*, toute tentative d'organisation de résistance avant même son balbutiement dans la pensée humaine.

La liberté exige, pour être réelle et effective, le respect de la vie privée, de l'intimité de la personne, de son intégrité et de sa dignité humaine, « un homme n'étant plus vraiment libre si son for intérieur devient une sorte de forum public ouvert à toutes les curiosités »[2780] ; une réalité pourtant avenue et avérée avec l'émergence du cyberespace et de la révolution numérique et des tentatives d'appropriation, de centralisation, d'uniformisation et de gestion des identités numériques émergentes.

Dans l'empire des données que représente le monde actuel, il serait, au sens de cette étude, plus juste et utile de prôner le droit à une identité numérique libre, multiforme, décentralisée, hétérogène, éparpillée, décomposée en autant de facettes identitaires porteuses d'évolutions et de changements en fonction des différentes perspectives, perceptions et représentations choisies de façon libre et autonome. Or, l'espace de sécurité, entendu largement, qui se développe en parallèle du cyberespace et de l'architecture numérique semble plutôt imposer une norme, une politique, une culture, une doctrine, à suivre ; se conformer aux règles de cet espace assure la protection, la sûreté et la liberté, mais, à l'inverse, l'imprévisibilité, les comportements hors du commun, cachés ou à risque peuvent être stigmatisés et pointés du doigt, voire à terme exclus[2781]. Pourtant, tout le monde a quelque chose à cacher, ne serait-ce que pour ce qui est de l'intimité : il suffit de penser au moment où l'on rentre chez soi, gardons-nous la porte ouverte ? Si nous la fermons, est-ce uniquement en raison du fait que nous avons quelque chose de grave à cacher ou que nous adoptons un comportement à risque ? D'autant que dire que nous n'avons rien à cacher, c'est comme dire que nous n'avons rien à dire, affectant la liberté d'expression.

Similairement, donnons-nous dans la vie physique à n'importe quelle personne ou entité un libre accès à nos comptes, mails, documents administratifs ou juridiques, pensées, décisions ou encore nos réflexions et actions intimes ? Nous choisissons avec qui les partager et comment, pourquoi alors n'aurons-nous pas les mêmes choix et les mêmes libertés dans le monde numérique que dans le monde physique ? Sans compter que les applications informatiques et

---

[2779] *Cf.* p. 52 ; et, E. GOFFMAN, *La mise en scène de la vie quotidienne, 1. La présentation de soi*, *op. cit.,* p. 27.

[2780] Débats parlementaires – Compte-rendu intégral, Séance du 4 octobre 1977, *op. cit.,* p. 5787.

[2781] *Cf.* Transition, p. 309, et notamment que « *[…] you don't have to worry if you have nothing to hide. But if your political activities or interests deviate even slightly out of the mainstream, you do* » : F. PASQUALE, The Black Box Society, *Id.*, p. 42.

numériques ainsi que les innombrables bases de données engendrent autant d'impacts et d'effets concrets et réels sans véritablement faire l'objet d'une remise en question ou d'un débat. Quelle est donc la valeur à long terme du progrès technologique imbibant les sociétés modernes ? Pourquoi ne parle-t-on pas plus ouvertement et librement des mauvais aspects du recours massif et indifférencié au numérique ?

Plus encore, pourquoi ne pas tenter de créer un système remplaçant les recommandations personnalisées à finalité économique et marchande par des recommandations personnalisées à finalité de partage du savoir dans un but de partage, d'accès et d'approfondissement du savoir et de la connaissance, contribuant ainsi à la construction d'un Soi libre et conscient, et d'une société réellement libre et démocratique.

À l'heure actuelle, n'importe quel commentaire, opinion, avis, tweet, like, click ou autre, manifesté a la possibilité de provoquer des effets et/ou dégâts inimaginables par le passé, créant en conséquence des anomalies et des paradoxes, de nature technique, légale ou sociale, que cette étude a tenté de soulever. Chaque individu vit dans sa bulle personnalisée dans laquelle il reste confiné et prévisible, réduit à un certain nombre de gestes, d'habitudes, de modèles et de discours, permettant de prédire ses pensées, comportements, actions, contributions et achats futurs. *In fine*, un traitement des sociétés en masse, à l'image du traitement de leurs données personnelles, paraît ainsi se manifester et se cristalliser.

Ce qui est paradoxal et antinomique en ce sens que le développement et/ou le fonctionnement des technologies et des nouveaux outils et dispositifs numériques deviennent imprévisibles, obscurs, opaques, caractérisant la théorie de la « boîte noire » susmentionnée, tandis que l'homme, l'être humain, initialement imprévisible, indéterminé, irréductible, devient prévisible, réductible et aisément modelable et gérable. En outre, cela révèle un autre paradoxe découlant, en particulier, de l'influence numérique sur l'environnement juridique qui repose sur le fait que, au nom de la sécurité, nous assistons graduellement à un effondrement des libertés fondamentales[2782]. Au fil de l'histoire de l'humanité, plusieurs auteurs ont tenté de prévenir des abus et des effets pouvant découler des applications récurrentes et massives des technologies et

[2782] En effet, « *[…], the sweeping techniques of post-9/11 surveillance and data gathering are of a scale appropriate to wholesale calamities like terror attacks and natural disasters, not to ordinary crime or protest. Thousands of people are being caught in data-driven dragnets for being activists, or just belonging to a suspect "identity" group. Careful protection of the boundary between crime and dissent is not a high priority of the intelligence apparatus. One state official commented, "You can make an easy kind of a link that, if you have a protest group protesting a war where the cause that's being fought against is international terrorism, you might have terrorism at that protest. You can almost argue that a* ***protest*** *against [the war] is a* ***terrorist*** *act." It would be nice to be able to dismiss this statement as an outlier, but FBI director Robert Mueller legitimized it all the way back in 2002, warning that "there is a continuum between those who would express dissent and those who would do a terrorist act." That is a frightening expansion of the "threat matrix."* » : F. PASQUALE, *The Black Box Society*, *Id.,* p. 47.

outils numériques. En ce sens, « *Huxley presents a narrative about a society controlled not by a despotic coercive government like Big Brother, but by manipulation and consumption, where people participate in their own enslavement* »[2783], évoquant dans ce contexte les nouvelles cultures de contrôle, d'asservissement et de conditionnement sociales mises en œuvre par le biais des nouvelles technologies et leurs utilisations récurrentes, tel qu'il a pu être observé dans cette analyse, alors même que « la sauvegarde de la dignité de la personne humaine contre toute forme d'asservissement et de dégradation est un principe à valeur constitutionnelle »[2784] : ainsi, « *the government achieves obedience through social conditioning, propaganda, and other forms of indoctrination. It does not use the crude coercive techniques of violence and force, but instead employs a more subtle scientific method of control—through genetic engineering, psychology, and drugs. Power works internally—the government actively molds the private life of its citizens, transforming it into a world of vapid pleasure, mindlessness, and numbness* »[2785], un monde véhiculé et entretenu par les géants du web et les nouveaux modèles économiques émergents[2786].

Dans cette perspective, de nombreuses questions fondamentales résultent, méritant de profondes réflexions et études, que ce soit à une échelle collective ou individuelle, notamment celle de savoir quelle identité nous souhaitons. Quel environnement voulons-nous envisager pour la liberté et l'autonomie dans la construction de notre Soi, de notre identité, que ce soit dans une dimension physique ou numérique ? Quelles structure et architecture de société choisissons-nous, plus particulièrement, à l'époque de la révolution numérique, que reste-t-il de la société démocratique, de l'État de droit, de l'autonomie individuelle et de l'autodétermination en droit, de l'égale souveraineté entre États, de la séparation et de l'équilibre des pouvoirs, du respect des frontières et des libertés fondamentales et individuelles ?

Depuis un moment déjà, les pratiques et techniques numériques ainsi que les technologies et objets connectés et intelligents sont présentés comme le rempart des sociétés modernes, la solution parfaite à tous les problèmes du quotidien et de la vie humaine, solution vivement prônée par le secteur public et le secteur privé qui garantissent que les technologies vont résoudre des problèmes aussi divers que variés, allant des embouteillages aux conditions

[2783] D. SOLOVE, *The Digital Person*, *op. cit.*, p. 39.
[2784] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », *loc. cit.*, p. 479 ; *Cf.* p. 168 et s., 415 et s., 630 et s.
[2785] D. SOLOVE, *The Digital Person*, *Id.*, p. 39.
[2786] *Cf.* p. 135 et s., 142 et s., 422 et s.

météorologiques anormales et aux infections ; et ce, en toute subtilité et opacité, au détriment des droits et libertés au savoir, à la connaissance, à l'autodétermination, à l'autonomie de choix, de perception, de représentation ou de construction. Or, compte tenu de tout ce qui a été analysé, la complaisance ou l'inertie est désormais injustifiée[2787] : « *today these rights to privacy, knowledge, and application have been usurped by a bold market venture powered by unilateral claims to others' experience and the knowledge that flows from it. What does this sea change mean for us, for our children, for our democracies, and for the very possibility of a human future in a digital world?* »[2788].

La question semble donc fondamentalement toucher la nature et les comportements humains, *a fortiori*, l'identité humaine – dans son autonomie, dans sa dignité, dans sa singularité, dans son humanité ; l'irréductible humain qu'on essaie *via* la révolution numérique de réduire à un produit, une série de données, un profil, un être prédictible, prévisible, calculable, modelable, contrôlable et réductible, voire à un homme-machine à améliorer ou à fabriquer - cela semble être le prix du développement et des innovations technologiques, l'intention ultime avancée étant le bien-être de l'humanité et l'amélioration de la vie humaine et de l'être humain par le numérique.

Cela dit, c'est, au sens de cette étude en particulier, négliger, d'une part, que « le chemin de l'enfer est pavée de bonnes intentions »[2789] et, d'autre part, « *que ces pratiques passent ou non par la destruction physique d'êtres humains, elles portent en commun, plus grave encore, une « destruction métaphysique », […] « et cette destruction est inacceptable car elle signifie la destruction de l'ordre humain tout entier, la négation de l'effort même par lequel il y a l'humanité de l'homme »* »[2790], engendrant conséquemment la question du crime contre l'espèce humaine ainsi que celle du crime par fabrication de vie.

[2787] F. PASQUALE, *The Black Box Society*, *Id.,* p. 16 où l'auteur precise que « *The corporate strategists and governmental authorities of the future will deploy their massive resources to keep their one-way mirrors in place; the advantages conferred upon them by Big Data technologies are too great to give up without a fight. But black boxes are a signal that information imbalances have gone too far. We have come to rely on the titans of reputation, search, and finance to help us make sense of the world* ».

[2788] S. ZUBOFF, *The Age of Surveillance Capitalism*, *op. cit.,* p. 8.

[2789] Proverbe ou idiome célèbre « The road to hell is paved with good intentions » : M. BROWN, *Wit and Humor of Well-known Quotations*, Small, Maynard & Company, 1905, p. 121: "*Hell is paved with good intentions*"; C. AMER, *The American Heritage Dictionary of Idioms*, Houghton Mifflin, 1997, p. 542: "*Hell is full of good wishes and desires*"; W. PETERSON, *Against the Stream: Reflections of an unconventional demographer*, Transaction Publishers, 2004, p. 3 ; et, F. A. HAYEK, *The road to Serfdom*, University of Chicago Press, Coll. Phoenix Books, 1944, p. 24: "*What has always made the state a hell on earth has been precisely that man has tried to make it his heaven*".

[2790] M. DELMAS-MARTY, « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », *Ibid.*, p. 479.

Il paraît dès lors que, comme signifié dans cette étude, seule la réelle et vraie poursuite de l'adage « *scienca potestas est* », « le savoir c'est le pouvoir », puisse contrebalancer et rétablir un équilibre dans l'ordre humain et le droit au savoir et à la connaissance libre, et sauvegarder, voire enrichir, *in concreto* et *in jure*, l'espèce humaine, son autonomie et sa liberté de pensée et d'être, sa singularité quelconque, son hominisation et son humanisation, son irréductible identité, physique ou numérique.

Lexique

Application Programming Interface **(API) – interface de programmation applicative ou interface de programme d'application :**

Solution informatique qui permet à des applications de communiquer entre elles et d'échanger mutuellement des services ou des données ; un ensemble de fonctions, méthodes et procédures permettant de créer des applications qui accèdent aux données et aux caractéristiques d'autres applications, services ou systèmes d'exploitation.

Arithmétique politique :

Désigne des opérations ayant pour but des recherches utiles à l'art de gouverner la société, en appréhendant trois variables : les nombres, le réel et la subjectivité (le moi) ; art de raisonner, par des chiffres et du calcul, sur des objets qui tiennent à l'administration publique.

Big data **:**

Traduit en mégadonnée ou données massives, se réfère à des ensembles de données extrêmement volumineux pouvant être analysés de façon computationnelle et analytique pour révéler des modèles, des tendances et des associations, en particulier en ce qui concerne les interactions et les comportements humains.

Biopolitique et biopouvoir :

Conception foucaldienne pour caractériser le passage de la politique à la biopolitique, une forme de pouvoir sur la vie, une technologie de pouvoir fonctionnant aux côtés de la technique et du pouvoir disciplinaires, marquant le passage du droit de « faire mourir ou laisser vivre » au droit de « faire vivre et laisser mourir », à savoir le passage d'un gouvernement dédié à la préservation de son intégrité, de sa société et de la continuité du fonctionnement politique, à un gouvernement dédié à assurer la sécurité et la protection de la société civile et ses conditions de survie, y compris biologiques et/ou environnementales.

Bytes ou bits :

Unité de stockage d'un ordinateur, quantifie la capacité de mémoire de l'ensemble des puces de l'ordinateur ; aujourd'hui, selon l'AFNOR, le Byte est défini comme l'unité d'information correspondant à un octet, soit 8 bits.

Capitalisme de surveillance :

Conception de Zuboff, nouvel ordre économique qui revendique l'expérience humaine comme matière première libre pour des pratiques commerciales opaques d'extraction, de prédiction et de vente ; une logique économique parasitaire dans laquelle la production de biens et de services est subordonnée à une nouvelle architecture globale de modification comportementale ; une mutation rebelle du capitalisme marquée par des concentrations de richesse, de savoir et de pouvoir sans précédent dans l'histoire de l'humanité ; le cadre fondateur d'une économie de surveillance.

Capteurs ou sondes-capteurs :

Dispositif (installé dans les objets connectés et intelligents, les villes intelligentes, etc.) qui sert à observer, récolter, traiter et transmettre les données de l'environnement physique.

***Cloud computing* – informatique en nuage :**

Mode de traitement des données, dont l'exploitation s'effectue par internet, sous la forme de prestations de services à distance.

Code :

Dans le cyberespace, le code, une composante de l'architecture du web et du fonctionnement du réseau, régule également le fonctionnement, le développement et le contrôle du web et des réseaux. Selon Lessig, il est le « *salient regulator* – régulateur saillant » de la nouvelle architecture régulant le cyberespace tout en le composant.

Computation :

Action, manière de calculer, de calcul, d'évaluation.

Computationnel :

En informatique, se réfère au traitement logico-algébrique et analytique d'un système ou terminal.

Cookie et cookie tiers :

Un cookie ou témoin de connections (RGPD Cons. 30) correspond à un petit fichier stocké par un serveur dans le terminal (ordinateur, tablette, téléphone, etc.) d'un utilisateur, associé à un domaine web et des pages d'un site web, qui est automatiquement renvoyé lors de contacts ultérieurs de la part de l'utilisateur avec le même nom de domaine. Et le cookie tiers est un cookie venant d'une tierce partie, placé par le serveur d'un domaine autre que celui du site visité par l'utilisateur qui sert, de manière générale, à suivre les activités de l'utilisateur à des fins analytiques ou de ciblage comportemental.

Corrélation :

Rapport de dépendance ou lien de causalité entre deux notions, faits, objets, données, dont l'un implique l'autre et *vice versa*.

***Cryptopticon* :**

Un écosystème opaque d'informations de surveillance massive des entreprises et des États, qui fonctionne de pair, et de manière dépendante, avec le Big data.

***Datafication* :**

Néologisme qui désigne la mise en données du monde et/ou la mise en corrélations des comportements en ligne, une méthode inédite employée de manière récurrente.

***Data aggregation* – agrégation des données :**

Un type de processus d'extraction de données et d'informations où les données sont recherchées, recueillies et présentées sous forme de rapport, synthétisé ou résumé pour atteindre des objectifs ou des processus opérationnels précis et/ou effectuer une analyse humaine.

***Data brokers* – courtiers en données :**

Prestataires qui recueillent, achètent, regroupent et revendent des données ou des ensembles de données aux différents acteurs souhaitant les acquérir en fonction de leurs objectifs et finalités du moment.

***Data centers* – centres de données :**

Lieux, infrastructures regroupant des équipements ou des installations informatiques (serveurs, routeurs, etc.) pour stocker, distribuer, traiter et analyser de grandes quantités et volumes de données à travers un réseau interne ou *via* le web (par ex. les centres de fusion – *fusion centers*).

***Data exhaust* :**

Traces, empreintes numériques, traces électroniques ; analyse de la piste des données.

***Data points* – points de données :**

Une unité d'informations distincte, une chaîne d'informations unique transmise par les dispositifs ou objets connectés (compteur, capteur, objet intelligent, etc.) ; dans un contexte statistique ou analytique, un point de données est habituellement dérivé d'une mesure ou d'une recherche et peut être représenté numériquement et/ou graphiquement.

Hypertexte :

Technique ou fonction qui permet d'établir des liens directs entre divers éléments (image, texte, son, etc.) de documents différents, liée au protocole de transfert hypertexte (Http), le protocole de communication entre un internaute et un serveur sur le web ; un lien hypertexte (hyperlien), un des éléments de base du langage informatique, permet de rajouter au contenu d'une page web des liens internes ou externes à un autre lien ou document (par ex. référencement d'un site web).

Intrant et extrant – *input-output :*

Appelée aussi analyse entrées-sorties, désigne en informatique, l'entrée des données en vue d'un traitement et la sortie des données après traitement, l'action d'extraire des données, et se réfère à la communication entre un terminal, un dispositif technologique ou un système de traitement d'informations et l'environnement physique.

Métadonnée – *metadata :*

Une donnée sur une donnée, caractérisant une autre donnée ; indique une donnée qui sert à définir ou à décrire une autre donnée, quelle que soit sa nature ou son support.

Objets connectés ou Internet des objets – *Internet of things* :

Nommés également objets intelligents, des objets qui sont connectés à internet, dotés de moyens de communications (avec ou sans fil) et qui ont la capacité de capter, d'enregistrer, de stocker, de traiter et de transmettre des données.

***Open data* :**

Données dont l'accès et l'usage sont libres ; mouvement d'ouverture et de mise à disposition des données publiques.

I. Ouvrages

* Ouvrages spéciaux

ABELSON Hal, LEDEEN Ken et LEWIS Harry R., *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion,* Ed. Addison-Wesley, 2008, 366 p.

AGAMBEN Giorgio, *État d'exception – Homo Sacer II, 1*, Ed. Seuil, Coll. L'Ordre Philosophique, t. 1, 2003, 160 p.

AGAMBEN Giorgio, *La communauté qui vient : Théorie de la singularité quelconque*, Ed. Seuil, Coll. La librairie du XXIe siècle, 1990, 128 p.

AGAMBEN Giorgio, *Qu'est-ce qu'un dispositif ?,* Paris, Ed. Payot & Rivages, Coll. Rivages Poche Petite bibliothèque n°569, 2014, 80 p.

AMMER Christine, *The American Heritage Dictionary of Idioms*, Ed. Houghton Mifflin, 1997, 729 p.

ANDEL Pek van et BOURCIER Danièle, *De la sérendipité – Dans la science, la technique, l'art et le droit : Leçons de l'inattendu*, Ed. L'Act Mem, Coll. Libres Sciences, 2009, 298 p.

ANCEL Marc, *La défense sociale nouvelle*, Paris, Ed. Cujas, 2ème éd., 1966, 391 p.

ANDERS Günther, *Nous, fils d'Eichmann*, Ed. Rivages Poche, Coll. Petites Bibliothèques rivages, 2003, 176 p.

ARENDT Hannah, *The human condition*, The University of Chicago Press, 2ème Ed., 1998, 349 p.

ATLAN Henri, *Les étincelles du hasard, t. 2. Athéisme de l'écriture*, Ed. Seuil, Coll. La librairie du XXIe Siècle, 2003, 448 p.

BACHAUMONT Louis Petit de*, Mémoires secrets pour servir à l'histoire de la République des Lettres en France*, depuis MDCCLXII jusqu'à nos jours, ou J. 1534, Journal d'un observateur, t. 29, Londres – Chez John Adamson, 1785, 328 p.

BARTH Friedrik, *Ethnic Groups and Boundaries: The Social Organisation of Culture Difference*, Waveland Press, 1998, 153 p.

BASDEVANT Adrien et MIGNARD Jean-Pierre, *L'empire des données – Essai sur la société, les algorithmes et la loi*, Ed. Don Quichotte, 2018, 360 p.

BATTISTINI Yves, *Trois contemporains. Héraclite, Parménide, Empédocle*, Paris, Ed. Gallimard, Coll. Les Essais n° 78, 1955, 208 p. (rééd. revue et augmentée sous le titre *Trois Présocratiques* (1968), Paris, Ed. Gallimard, Coll. Tel n° 136, 1988, 196 p.)

BAUGNET Lucy, *Métamorphoses identitaires*, Bruxelles, P.I.E.- Peter Lang S. A., Éditions scientifiques internationales, 2001, 245 p.

BAUMAN Zygmunt, *La vie liquide*, Ed. Rouergue-Chambon, Coll. Les Incorrects, 2006, 224 p.

BAUMAN Zygmunt, *Le coût humain de la mondialisation*, Librairie Arthème Fayard, Coll. Pluriel, 2011, 208 p.

BAUMAN Zygmunt, *Le présent liquide : Peurs sociales et obsessions sécuritaires*, Ed. Seuil, Coll. Débats, Paris, 2007, 144 p.

BAUMAN Zygmunt, *Vies perdues : La modernité et ses exclus*, Paris, Ed. Payot, Coll. Manuels Payot, 2006, 272 p.

BAYART Jean-François, *L'Illusion identitaire*, Librairie Arthème Fayard, Coll. Pluriel, 2018, 320 p.

BECK Ulrich, *La société du risque : Sur la voie d'une autre modernité*, Paris, Ed. Aubier, Coll. Alto, 2001, 528 p.

BECKER Gary S., *The Economic Approach to Human Behavior*, The University of Chicago Press, Chicago, 1978, 314 p.

BENJAMIN Walter, *Critique de la violence et autres essais*, Ed. Payot & Rivages, Coll. Petite Biblio Payot, Paris, 2018, 160 p.

BENTHAM Jeremy, *The panopticon writings*, Verso Ed., 1995, 158 p.

BERNAYS Edward, *Propaganda*, Introduction by Mark Crispin Miller, Ig Publishing, New York, 2004 (publication paru initialement en 1928), 175 p.

BLACK Edwin, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, Washington DC, Dialog Press, Expanded Ed., 2012, 592 p.

BLAUG Mark, *La Méthodologie Économique*, Ed. Economica, Paris, 2ème Ed. 1994, 285 p.

BOX George E. P. et DRAPER Norman R., *Empirical Model-Building and Response Surfaces*, John Wiley & Sons, New York, 1987, 688 p.

BRAIBANT Guy, *La Charte des droits fondamentaux de l'Union Européenne : témoignages et commentaires,* Paris, Ed. Points, Coll. Points Essais n° 469, 2001, 336 p.

BRASSEUR Christophe, *Enjeux et usages du Big Data : Technologies, méthodes et mises en œuvre*, Paris, Ed. Hermès - Lavoisier, Coll. Management et Informatique, 2013, 214 p.

BROWN Marshall, *Wit and Humor of Well-known Quotations*, Boston, Ed. Small, Maynard & Company, 1905, 376 p.

CARBONNIER Jean, *Droit Civil, Introduction, Les personnes, La famille, l'enfant, le couple, 2 Vol.,* Paris, PUF, Coll. Quadrige, 2004, 2573 p.

CARBONNIER Jean, *Sociologie juridique*, PUF, Coll. « Quadrige », 2ème Ed., Paris, 2004, 415 p.

CARDON Dominique, *À quoi rêvent les algorithmes – Nos vies à l'heure des big data*, Ed. Seuil et La République des Idées, France, octobre 2015, 106 p.

CASILLI Antonio A., *En attendant les robots : Enquête sur le travail du clic*, Ed. Seuil, Coll. La couleur des idées, 2019, 400 p.

CHRISTENSEN Clayton M., *The innovator's dilemma: When new technologies cause great firms to fail*, Harvard Business School Press, Boston, Massachusetts, 1997, 288 p.

CLARK Robert M., *The Technical Collection of Intelligence*, Washington D.C., Ed. CQ Press, 1ère édition, 2010, 344 p.

COHEN Julie E., *Configuring the networked self – Law, Code, and the play of everyday practice*, Yale University Press, 2012, 350 p.

CONFUCIUS, *The Analects*, written in ca 500 B.C., Annping Chin (trad. & eds.), Ed. Penguin Classics, 2014, 468 p.

CONFUCIUS, *The Doctrine of the mean: How to achieve equilibrium*, written ca 500 B.C.E., Ed. CreateSpace Independent Publishing Platform, 2014, 28 p.

COOLEY Charles Horton, *Human Nature and the Social Order,* New York, Charles Scribner's sons, 1902, 412 p.

COOPER Milton William, *Behold a pale horse*, Light Technology Publishing, 1991, 470 p.

COUFFIGNAL Louis, *La cybernétique*, PUF, Coll. Que sais-je ? n° 638, Paris, 1963, 125 p.

COUFFIGNAL Louis, *Les machines à penser*, Les Éditions de Minuit, Coll. Grands documents, 2ème Ed., Paris, 1964, 140 p.

COURMONT Barthélémy et RIBNIKAR Darko, *Les guerres asymétriques : Conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces*, PUF, Coll. Enjeux stratégiques, Paris, 2002, 284 p.

CRÉPON Marc, *La culture de la peur - I. Démocratie, identité, sécurité*, Ed. Galilée, 2008, 136 p.

DE LA HAYE Anne-Marie, *La catégorisation des personnes*, Grenoble, Presses Universitaires de Grenoble, Coll. La Psychologie en plus, 1998, 224 p.

DE FILIPPI Primavera et WRIGHT Aaron, *Blockchain and the Law – The Rule of Code*, Ed. Harvard University Press, 2018, 300 p.

DELMAS-MARTY Mireille, *Aux quatre vents du monde – Petit guide de navigation sur l'océan de la mondialisation*, Ed. Seuil, Coll. Sciences humaines, 2016, 156 p.

DELMAS-MARTY Mireille, *Les forces imaginantes du droit (III) – La refondation des pouvoirs*, Ed. Seuil, Coll. La couleur des idées, 2007, 320 p.

DELMAS-MARTY Mireille*, Les forces imaginantes du droit (IV) – Vers une communauté de valeurs ?*, Ed. Seuil, Coll. La couleur des idées, 2011, 448 p.

DELMAS-MARTY Mireille, *Les grands systèmes de politique criminelle*, PUF, Coll. Thémis, 1992, 448 p.

DELMAS-MARTY Mireille, *Résister, responsabiliser, anticiper*, Ed. Seuil, Coll. Débats, 2013, 208 p.

DELEUZE Gilles, *Foucault*, Paris, Les Éditions de Minuit, Coll. Critique, 1986, 144 p.

DELEUZE Gilles, *Pourparlers (1972-1990)*, Les Éditions de Minuit, 1990, 256 p.

DENNING Peter J. et MARTELL Craig H., *Great Principles of Computing*, Cambridge, MIT press, 2015, 320 p.

DERRIDA Jacques, *Force de loi : le "Fondement mystique de l'autorité",* Ed. Galilée, Coll. La philosophie en effet, Paris, 1994, 160 p.

DESGENS-PASANAU Guillaume, *La protection des données personnelles*, Paris, LexisNexis, 2ème Ed., 2016, 250 p.

DESGENS-PASANAU Guillaume et FREYSSINET Éric, *L'identité à l'ère numérique*, Ed. Dalloz-Sirey, Coll. Présaje, 2009, 170 p.

DESROSIÈRES Alain, *La politique des grands nombres – Histoire de la raison statistique*, Paris, Ed. La Découverte, Coll. Sciences et techniques, 1993, 364 p.

DUBAR Claude, *La Crise des identités. L'interprétation d'une mutation,* Paris, PUF, Coll. Le Lien Social, 3ème éd. corrigée, 2007, 239 p.

DURKHEIM Émile, *Les Règles de la méthode sociologique*, Ed. Flammarion, Coll. Champs, Paris, 1988 [1894], 255 p.

DÜRRENMATT Friedrich, *The Assignment: Or, on the Observing of the Observer of the Observed*, Joel Agee translation, University of Chicago Press, 1988, 152 p.

ERIKSON Erik, *Adolescence et crise. La quête de l'identité*, Paris, Ed. Flammarion, Coll. Champs Essais, 2011, 352 p.

ERIKSON Erik, *Enfance et société*, Ed. Delachaux et Niestlé, 1982, 285 p.

ERTZSCHEID Olivier, *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies*, Marseille, OpenEdition Press, Coll. Encyclopédie numérique 1, 2013, 72 p.

FERRI Enrico, *La sociologie criminelle*, Trad. de l'Italien par Léon Terrien, Ed. Félix Alcan, Paris, 2ème Ed., 1914 (1ère éd. 1893), 640 p.

FOUCAULT Michel, *Du gouvernement des vivants*, Cours au Collège de France 1979-1980, Ed. Gallimard – Seuil, Coll. Hautes études, EHESS, 2012, 400 p.

FOUCAULT Michel, *Dits et Écrits t. I* (1954-1975), Ed. Gallimard, Coll. Quarto, 2001, 1728 p.

FOUCAULT Michel, *Dits et écrits t. II* (1976-1988), Ed. Gallimard, Coll. Quarto, 2001, 1760 p.

FOUCAULT Michel, *Dits et écrits t. III* (1976-1979), Ed. Gallimard, Coll. Bibliothèque des sciences humaines, 1994, 848 p.

FOUCAULT Michel, *Il faut défendre la société*, Cours au collège de France 1975-1976, Ed. Gallimard – Seuil, Coll. Hautes Études, EHESS, 1997, 304 p.

FOUCAULT Michel, *Les mots et les choses : Une archéologie des sciences humaines*, Ed. Gallimard, Coll. Bibliothèque des Sciences Humaines, 1966, 404 p.

FOUCAULT Michel, *Naissance de la biopolitique*, Cours au collège de France 1978-1979, Ed. Gallimard – Seuil, Coll. Hautes Études, EHESS, 2004, 368 p.

FOUCAULT Michel, *Sécurité, Territoire, Population*, Cours au collège de France 1977-1978, Ed. Gallimard – Seuil, Coll. Hautes Études, EHESS, 2004, 448 p.

FOUCAULT Michel, *Surveiller et Punir*, Coll. Tel, Ed. Gallimard, 1975, Impression de 2013, 360 p.

FOURASTIÉ Jean et Jacqueline, *La réalité économique*, Ed. Hachette, Coll. Pluriel, 1986, 456 p.

FREUD Sigmund, *Trois essais sur la théorie sexuelle*, Paris, Ed. Gallimard, Coll. Connaissances de l'inconscient, 1987, 211 p.

GADENNE Emmanuel, *Le guide pratique du Quantified Self. Mieux gérer sa vie, sa santé, sa productivité*, Ed. Fyp, Coll. Entreprendre, 2012, 224 p.

GARLAND David, *The culture of control: Crime and social order in contemporary society*, Oxford University Press, 2001, 308p.

GAROFALO Raffaele, *La criminologie –Étude sur la nature du crime et la théorie de la pénalité*, Ed. Félix Alcan, 2ème éd. entièrement refondue, 1890, 452 p.

GOFFMAN Erving, *La mise en scène de la vie quotidienne, 1. La présentation de soi*, Les Editions de Minuit, Coll. Le sens commun, 1973, 256 p.

GOFFMAN Erving, *Stigmate. Les usages sociaux des handicaps*, Les Éditions de Minuit, Coll. Le sens commun, 1975, 176 p.

GOODFELLOW Ian, BENGIO Yoshua et COURVILLE Aaron, *Deep learning*, MIT Press, 2016, 800 p.

GREENWALD Glenn, *No place to hide: Edward Snowden, The NSA & The U.S. Surveillance State*, Ed. Penguin Books, Penguin Random House UK, 2014, 272 p.

GRIBAUDI Maurizio, *Itinéraires ouvriers. Espaces et groupes sociaux à Turin au début du XXe siècle*, Paris, Éd. de l'EHESS, Coll. Recherches d'histoire et de sciences sociales, 1987, 264 p.

GUINCHARD Serge et DEBARD Thierry (dir.), *Lexique des Termes Juridiques*, Paris, Dalloz, 19ème Ed., 2012, 918 p.

HAYEK Friedrich A., *The road to Serfdom*, University of Chicago Press, Coll. Phoenix Books, 1944, 2007, 304 p.

HEINICH Nathalie, *Ce que n'est pas l'identité*, Ed. Gallimard, Coll. Le débat, Paris, 2018, 134 p.

HOBBES Thomas, *Léviathan ou Matière, forme et puissance de l'État chrétien et civil,* (1651), éd. et trad. de l'anglais par Gérard Mairet, Ed. Gallimard, Coll. Folio essais n° 375, 2000, 1024 p.

HUGO Victor, *Actes et Paroles II – Pendant l'exil* (1852-1870), Œuvres complètes in-8°, Paris, Ed. J. Hetzel & C^{ie} et A. Quantin, 1883, 584 p.

KANT Emmanuel, *Fondements de la Métaphysique des mœurs*, (1785), Trad. de Victor Delbos, Éd. Hachette Livre BNF, 2013, 167 p.

KHALIL GIBRAN Gebran, *The Prophet*, Vintage Books New-York, reprinted ed., 2015, 112 p.

KILKELLY Ursula, *Le droit au respect de la vie privée et familiale : un guide de mise en œuvre de l'article 8 de la Convention européenne des droits de l'homme*, Ed. Conseil de l'Europe, Précis sur les droits de l'homme n° 1, 2003, 73 p.

KUHN Thomas S., *La Structure des révolutions scientifiques*, Paris, Ed. Flammarion, Coll. Champs, 1999, trad. de la nouvelle éd., *The Structure of Scientific Revolutions*, publiée par The University of Chicago Press (1970), 288 p.

KURZWEIL Ray, *How to Create a Mind: The Secret of Human Thought Revealed*, Ed. Penguin Books, 2013, 352 p.

KURZWEIL Ray, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*, Ed. Penguin Books, 2000, 388 p.

KURZWEIL Ray, *The Singularity Is Near: When Humans Transcend Biology*, Ed. Penguin Books, 2006, 672 p.

LABOUÉRIE Guy Vice-Amiral d'escadre, *Stratégie : Réflexions et Variations*, Ed. ADDIM, Coll. Esprit de défense, 1993, 196 p.

LAGRANGE Hugues, *Demandes de sécurité : France, Europe, États-Unis,* Ed. du Seuil, Coll. La République des Idées, Paris, 2003, 112 p.

LANDES William M. et POSNER Richard A., *The Economic Structure of Intellectual Property Law*, The Belknap Press of Harvard University Press, Cambridge, 2003, 448 p.

LANGBAUM Robert Woodrow, *The Mysteries of Identity. A Theme in Modern Literature*, Oxford University Press, 1977, 383 p.

LAURENT Sébastien, *Politiques de l'ombre - État, renseignement et surveillance en France*, Paris, Ed. Fayard, 2009, 701 p.

LENDREVIE Jacques et LÉVY Julien, *Dictionnaire bilingue Mercator, Tout le marketing à l'ère numérique*, 11ème édition, Dunod, Coll. Livres en or, 2014, 1040 p.

LESCA Humbert, *Veille stratégique : concepts et démarche de mise en place dans l'entreprise,* Guides pour la pratique de l'information scientifique et technique, Ministère de l'Éducation Nationale, de la Recherche et de la Technologie, 1997, 27 p.

LESSIG Lawrence, *Code – Version 2.0*, Ed. Basic Books, New York, 2006, 410 p.

LÉVY Pierre, *Qu'est-ce que le virtuel ?*, Paris, La Découverte, Coll. Poche n° 49, 1998, 160 p.

LIPIANSKY Edmond-Marc, *Identité et Communication : l'expérience groupale*, PUF, Coll. Psychologie sociale, 1992, 262 p.

LOMBROSO Cesare, *L'Anthropologie criminelle et ses récents progrès*, Ed. Félix Alcan, 1890, 180 p.

LOVELUCK Benjamin, *Réseaux, Libertés et Contrôle : Une généalogie politique d'internet*, Ed. Armand Colin, Coll. Le temps des idées, 2015, 368 p.

MAYER-SCHÖNBERGER Viktor et CUKIER Kenneth, *Big Data: A revolution that will transform how we live, work and think*, Great-Britain, John Murray Publishers, 2013, 242 p.

MEAD George H., *L'Esprit, le Soi et la Société*, Paris, PUF, Coll. le Lien Social, 2006, 436 p.

MÉLIN-SOUCRAMANIEN Ferdinand, *Constitution de la République française*, Ed. Dalloz, Coll. Dalloz Gestion Systèmes et stratégies, 2009, 130 p.

MERCURO Nicholas et MEDEMA Steven G., *Economics and the Law: From Posner to post-modernism*, Princeton University Press, 1997, 235 p.

MERLE Roger et VITU André, *Traité de droit criminel : problèmes généraux de la science criminelle, droit pénal général*, t. I, Ed. Cujas, 7ème éd., 1997, 1068 p.

MILLER Arthur R., *The assault on privacy: Computers, Data banks and Dossiers*, Ed. Ann Arbor-The University of Michigan Press, 1971, 384 p.

MORIN Edgar, *La Méthode 1. La Nature de la nature*, Ed. Seuil, Coll. Points Essais, 2014, 416 p.

MORIN Edgar, *Penser l'Europe*, Ed. Gallimard, Coll. Folio actuel n° 20, 1987, revue et complétée en 1990, 288 p.

MUCCHIELLI Alex, *L'Identité*, Paris, PUF, Coll. Que sais-je ?, 2013, 128 p.

MUSSO Pierre, *Le temps de l'État-Entreprise : Berlusconi, Trump, Macron*, Ed. Fayard, Coll. Documents, témoignages, 2019, 352 p.

NEEF Dale, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization and Digitally Driven Innovation*, FT Press Analytics, Ed. Pearson FT Press, 2014, 320 p.

NELSON Theodor Holm, *Literary Machines: The report on, and of, Project Xanadu concerning word processing, electronic publishing, hypertext, thinkertoys, tomorrow's intellectual revolution, and certain other topics including knowledge, education and freedom*, Sausalito, California, Mindful Press, 1981, 286 p.

NISSENBAUM Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, 304 p.

ORTOLAN Jean-Louis-Elzéar, *Éléments de droit pénal : Pénalité – Juridictions – Procédure*, t. I, Librairie de Henri Plon, 3ème éd., 1863, 616 p.

PASQUALE Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, USA, 2015, 320 p.

PENNEL Denis, *Travailler pour soi : Quel avenir pour le travail à l'heure de la révolution individualiste ?*, Ed. du Seuil, Coll. Essais, 2013, 240 p.

PETERSEN William, *Against the Stream: Reflections of an unconventional demographer*, Transaction Publishers, 2004, 154 p.

PETTY William Sir, *Political Arithmetick Or a Discourse Concerning, The Extent and Value of Lands, People, Buildings: Husbandry, Manufacture, Commerce, Fishery, Artizans, Seamen, Soldiers; Publick Revenues, Interest, Taxes, Superlucration, Registries, Banks, Valuation of Men, Increasing of Seamen, of Militia's, Harbours, Situation, Shipping, Power at Sea, etc. as the same relates to every country in general, but more particularly to the territories of His Majesty of Great Britain, and his neighbors of Holland, Zealand, and France*, Printed for Robert Clavel at the Peacock, and Hen. Mortlock at the Phoenix in St. Paul's Church-yard, London, 1690, Cambridge University Press, 1899, 2 Vol., 313 p.

PIAZZA Pierre, *Histoire de la Carte Nationale d'Identité*, Ed. Odile Jacob, Coll. Histoire et Document, 2004, 462 p.

PLATON, *Les Lois – Livres VII à XII*, Ed. Flammarion, Coll. Garnier Flammarion, 2006, 434 p.

PLATON, *Œuvres de Platon*, traduites par Victor Cousin, t. 9ème, Paris, Rey et Gravier libraires, quai des Augustins, n° 45, In-8°, 1833, 395 p. [Contient la traduction de La République, Livre I-V, Notes additionnelles (p. 325-394)].

PORTER Michael E., *Competitive Advantage: creating and sustaining superior performance*, The Free Press, New York, 1985, 557 p.

RAZAC Olivier, *Avec Foucault après Foucault : Disséquer la société de contrôle*, Paris, Ed. L'Harmattan, Coll. Esthétiques - Culture et Politique, 2008, 176 p.

REVEL Judith, *Le vocabulaire de Foucault*, Ed. Ellipses Marketing, Coll. Vocabulaire de…, 2002, 70 p.

REY Olivier, *Quand le monde se fait nombre*, Ed. Stock, Coll. Les essais, 2016, 328 p.

RICHELSON Jeffrey T., *The U.S. Intelligence Community*, Boulder, Co., Ed. Westview Press, 6ème édition, 2011, 624 p.

RICŒUR Paul, *Soi-même comme un autre*, Paris, Éd. Seuil, Coll. L'ordre philosophique,1990, 432 p.

ROUSSEAU Jean-Jacques, *Du Contrat Social ou Principes du Droit Politique*, in-8°, Ed. Marc Michel Rey, Amsterdam, (1762), 1896, Ed. Hachette Livre Bnf de juin 2012, 324 p.

SADIN Éric, *La Vie algorithmique - Critique de la raison numérique,* Paris, Ed. L'Échappée, Coll. Pour en finir avec, 2015, 288 p.

SALAS Denis, *La volonté de punir : Essai sur le populisme pénal*, Ed. Fayard, Coll. Pluriel, 2010, 288 p.

SCHMITT Carl, *La Dictature*, Ed. du Seuil, Coll. L'Ordre Philosophique, Paris, 2000, 336 p.

SCHMITT Carl, *Théologie politique*, Ed. Gallimard, Coll. Bibliothèque des Sciences humaines, 1988, 204 p.

SCHNEIER Bruce, *Click here to kill everybody: Security and survival in a Hyper-connected world*, Ed. W. W. Norton & Company, New-York, 2018, 288 p.

SCHNEIER Bruce, *Data and Goliath – The Hidden battles to collect your data and control your world*, Ed. W.W. Norton & Company Independent Publishers, 2015, 400 p.

SCHNEIER Bruce, *Secrets & Lies: Digital Security in a Networked World – With new information about post 9/11 security*, Wiley Publishing Inc., Paperback Edition, 2004, 414 p.

SCHUMPETER Joseph A., *Capitalism, Socialism and Democracy*, Routledge, London and New York, revised ed., 1994, 460 p.

SEARLE John R., *La construction de la réalité sociale [The Construction of Social Reality],* Trad. de l'anglais par C. Tiercelin, Ed. Gallimard, Coll. Nrf Essais, 1998, 320 p.

SOLOVE Daniel J., *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004, 296 p.

SUPIOT Alain, *La gouvernance par les nombres*, Cours au Collège de France (2012-2014), en partenariat avec l'Institut d'études avancées de Nantes, Ed. Fayard, Coll. Poids et mesures du monde, 2015, 520 p.

TAYLOR Charles, *Hegel et la société moderne*, Québec, Presses de l'Université Laval, Paris, Ed. du Cerf, 1998, 192 p.

TOCQUEVILLE Alexis De, *De la démocratie en Amérique*, t. I, Ed. GF Flammarion, Paris, 1981, 570 p.

TOCQUEVILLE Alexis De, *De la démocratie en Amérique*, t. II, Ed. Hachette Bnf, Coll. Sciences sociales, 1848, 426 p.

TURKLE Sherry, *Life on the Screen: Identity in the Age of the Internet*, New-York, Ed. Simon and Schuster, 1995, 347 p.

VAIDHYANATHAN Siva, *Anti-social media: How Facebook disconnects us and undermines Democracy*, Oxford University Press, New York, 2018, 288 p.

VAILLÉ Eugène, *Le Cabinet Noir*, un vol. in-8°, Paris, PUF, 1950, 412 p.

VARELA Francisco J., *Invitation aux sciences cognitives*, Ed. Seuil, Coll. Points sciences, nouvelle éd., 1996, 123 p.

VERNIER Jean-Pierre, *H.G. Wells et son temps*, Presses Universitaires de Rouen et du Havre, Coll. PU Rouen Hors C, 1971, 557 p.

WALLER Irvin, *Lutter contre la délinquance - Comment le tout répressif tue la Sécurité*, Ed. L'Harmattan, Paris, 2009, 224 p.

WEBER Max, *Économie et société*, t. I, Ed. Librairie Plon, 1971, 650 p.

WEBER Max, *Economy and Society: An outline of interpretive sociology*, Guenther Roth & Claus Wittich (trad. & Eds.), University of California Press, 1978, 1469 p.

WEBER Max, *From Max Weber: Essays in Sociology*, Hans H. Gerth & C. Wright Mills (trad. & Eds.), New York, Oxford University Press, 1946, 490 p.

WELCHMAN Gordon, *The Hut Six story – Breaking the Enigma codes*, Ed. McGraw-Hill, 1982, 326 p.

WHITAKER Reginald, *The end of privacy: how total surveillance is becoming a reality*, The New Press, New York, 1999, 195 p.

WIENER Norbert, *Cybernetics or, Control and Communication in the Animal and the Machine*, Ed. Martino Publishing, (1948-1961 The MIT Press), 2013, 234 p.

WIENER Norbert, *The human use of human beings: Cybernetics and society*, Da Capo Press, (1950-1954 Houghton Mifflin), 1988, 200 p.

ZAVALLONI Marisa, *Égo-écologie et Identité : une approche naturaliste*, PUF, Coll. Psychologie sociale, 2007, 216 p.

ZAVALLONI Marisa et LOUIS-GUÉRIN Christiane, *Identité sociale et Conscience : Introduction à l'égo-écologie*, Montréal, Presses Universitaires de Montréal, 1984, 284 p.

ZUBOFF Shoshana, *The Age Of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, Ed. Public Affairs, Profile Books, 2019, 691 p.

* Ouvrages généraux

AUGOUSTINOS Martha, "Social categorization: Toward theorical Integration", *In* DEAUX Kay et PHILOGÈNE Gina (éds.), *Representations of the social: Bridging theoretical traditions*, Oxford, Blackwell publishing, 2001, p. 201-216.

BELLEY Jean-Guy, « Le rayonnement intellectuel de Jean Carbonnier au Québec : le succès d'estime d'un honnête homme », *In* VERDIER Raymond et TOSELLO-BANCAL Jean-Émile (éds. & dir.), *Jean Carbonnier (1908-2003). Art et Science de la législation*, du 5 et 6 novembre 2008, Palais du Luxembourg, Colloque international organisé par la Bibliothèque Cujas en coopération avec le Sénat et l'Association Française Droit et Cultures, avec le soutien de la Mission de recherche Droit et Justice, Coll. Les colloques du Sénat, 2012, p. 102-112.

BONFANTE Larissa, CHADWICK John, COOK B.F., DAVIES W.V., HEALEY John F., HOOKER J.T. et WALKER C.B.F. (Collectif), *La Naissance des écritures. Du cunéiforme à l'alphabet*, Paris, Ed. Seuil, 1994, 503 p.

BOURCIER Danièle, « Régulation juridique, complexité et sérendipité », *In* BOURCIER Danièle, BOULET Romain et MAZZEGA Pierre (éds.), *Politiques publiques – Systèmes complexes*, Ed. Hermann, 2012, p. 31-48.

BOURCIER Danièle, BOULET Romain et MAZZEGA Pierre, « La gouvernance des systèmes complexes : Réflexions et recherches sur les politiques publiques aujourd'hui », *In* BOURCIER Danièle, BOULET Romain et MAZZEGA Pierre (éds.), *Politiques publiques – Systèmes complexes*, Ed. Hermann, 2012, p. 9-18.

BOUZEGHOUB Mokrane et MOSSERI Rémy (dir.), *Les Big Data à découvert*, Ed. CNRS, Coll. Société, 2017, 368 p.

BREAKWELL Glynis, “Integrating paradigms, methodological implications”, *In* BREAKWELL Glynis M. et CANTER David V. (éds.), *Empirical approaches to social representations*, Oxford University Press, 1993, p. 180-201.

BROUILLET Pascal, « Sécurité intérieure et gestion de la violence », *In* Frédéric DEBOVE et Olivier RENAUDIE (dir.), *Sécurité Intérieure : Les nouveaux défis*, Ed. Magnard-Vuibert, 2013, p. 3-10.

CASILLI Antonio A., « Quatre thèse sur la surveillance numérique de masse et la négociation de la vie privée », *In* Conseil d’État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, La documentation française, Les rapports du Conseil d’État n° 65, juillet 2014, p. 423-434.

CONSEIL D’ÉTAT, *Les conséquences du développement de l’informatique sur les libertés publiques et privées et sur les décisions administratives,* Rapport annuel de 1969-1970, La Documentation française, 1970, 446 p.

CONSEIL D’ÉTAT, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, La documentation française, Les rapports du Conseil d’État n° 65, juillet 2014, 441 p.

CONSEIL D’ÉTAT, *La citoyenneté – Être (un) citoyen aujourd’hui*, Étude annuelle 2018, La documentation française, Les rapports du Conseil d’État n° 69 (ancienne collection Études et Documents du Conseil d’État), septembre 2018, 211 p.

CHAUCHAT Hélène, « Du fondement social de l’identité du sujet », *In* CHAUCHAT Hélène, DURAND-DELVIGNE Annick, *De l’identité du sujet au lien social*, Paris, PUF, Coll. Sociologie d’aujourd’hui, 1999, p. 3-26.

CHAUVIER Stéphane, « La question philosophique de l’identité personnelle », *In* HALPERN Catherine et RUANO-BORBALAN Jean-Claude (dir.), *Identité(s) : L’individu, le groupe, la société*, Ed. Auxerre, Coll. Sciences Humaines, 2004, p. 25-32.

COHEN Julie E., “The surveillance-innovation complex: The irony of the participatory turn”, *In* BARNEY Darin, COLEMAN Gabriella, ROSS Christine, STERNE Jonathan et TEMBECK Tamar (eds. & dir.), *The participatory condition in the digital age*, University of Minnesota Press, 2016, p. 207-226.

DIDEROT Denis, « Arithmétique Politique », article de *Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers, par une société de gens de lettres*, t. I, Mis en ordre & publié par M. DIDEROT, de l’Académie Royale des Sciences & des Belles Lettres de Pruffe ; quant à la Partie Mathématique, par M. D'ALEMBERT, de l'Académie Royale des Sciences de Paris, de celle de Pruffe, et de la Société Royale de Londres, Paris, Chez Briasson, David l’aîné, Le Breton, Durand, 1751, Gallica Bnf, p. 678-680.

DIERS-LAWSON Audra, “Crisis Communication”, *In* Howard Giles et Jake Harwood (Eds), *The Oxford Encyclopedia of Intergroup Communication*, Oxford University Press, 2018, 1464 p.

DOISE William, « L’individualisme comme représentation collective », *In* DESCHAMPS Jean-Claude, MORALES Francisco J., PAEZ Dario et WORCHEL Stephen (éds.), *L’identité sociale, La construction de l’individu dans les relations entre groupes,* Grenoble, Presses Universitaires de Grenoble, 1999, p. 195-212.

DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace », *In* Hérodote N° 152-153, *Cyberespace : Enjeux géopolitiques*, Ed. La Découverte, 1er-2ème trimestre 2014, p. 3-25.

DUVEEN Gerard, “Representations, Identities, Resistance”, *In* DEAUX Kay et PHILOGÈNE Gina (éds.), *Representations of the social: Bridging theoretical traditions*, Oxford, Blackwell publishing, 2001, p. 257-270.

ERNST Wolfgang, “Beyond the rhetoric of panopticism: surveillance as cybernetics” *In* LEVIN Thomas Y., FROHNE Ursula and WEIBEL Peter Weibel (eds.), *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*, ZKM Centre for Art and Media: Karlsruhe, The MIT Press, 2002, 665 p., 460-473.

FRYDMAN Benoît, « Le calcul rationnel des droits sur le marché de la justice : l'école de l'analyse économique du droit », *In* ANDRÉANI Tony et ROSEN Menahem (dir.), *Structure, Système, Champ et Théorie du Sujet*, Ed. L'Harmattan, Coll. Ouverture philosophique, 1997, p. 127-146.

GOLDMAN Berthold, « Frontières du droit et *lex mercatoria* », *In Archives de philosophie du droit*, t. IX - Le droit subjectif en question, Paris, Ed. Sirey, 1964, p. 177-192.

HALPERN Catherine, « Faut-il en finir avec l'identité ? », *In* HALPERN Catherine et RUANO-BORBALAN Jean-Claude (dir.), *Identité(s) : L'individu, le groupe, la société*, Ed. Auxerre, Coll. Sciences Humaines, 2004, p. 11-20.

IOGNA-PRAT Dominique, « Introduction générale : la question de l'individu à l'épreuve du Moyen Âge », *In* BEDOS-REZAK Brigitte-Myriam et IOGNA-PRAT Dominique (dir.), *L'Individu au Moyen Âge, individuation et individualisation avant la modernité*, Paris, 2005, p. 7-29.

JODELET Denis (dir.), *Les représentations sociales*, PUF, Coll. Sociologie d'aujourd'hui, 2003, 452 p.

JODELET Denis, « Représentation sociale : phénomènes, concept et théorie », *In* MOSCOVICI Serge (dir.), *Psychologie sociale,* PUF, Coll. Quadriges, 2003, p. 357-378.

JOVIC Ljiljana, « Représentations (sociales) », *In* FORMARIER Monique et JOVIC Ljiljana (éd.), *Les concepts en sciences infirmières*, 2ème éd., Toulouse, Ed. Association de Recherche en Soins Infirmiers, Coll. « Hors collection », 2012, p. 265-267.

KARDINER Abram, « Identité », *In* BONTE Pierre et IZARD Michel (dir.), *Dictionnaire de l'ethnologie et de l'anthropologie*, Paris 2002, p. 403-404.

KLAPISCH-ZUBER Christiane, « La construction de l'identité sociale. Les magnats dans la Florence du Moyen Âge », *In* LEPETIT Bernard (dir.), *Les formes de l'expérience. Une autre histoire sociale*, Paris, Ed. Albin Michel, 1995*,* p. 151-164.

KORNHAUSER Lewis, "The Economic Analysis of Law", *In* ZALTA Edward N. (ed.), *The Stanford Encyclopedia of Philosophy,* Fall 2017 Edition, Ed. The Metaphysics Research Lab, Center for the study of language and information, Stanford University.

LAURENT Maryline et BOUZEFRANE Samia (dir.), *La gestion des identité numériques*, Ed. iSTE, Coll. Systèmes d'information, web et informatique ubiquitaire, 2015, 284 p.

LEE Min Kyung, KUSBIT Daniel, METSKY Evan et DABBISH Laura, "Working with machines: The impact of algorithmic and data-driven management on human workers", *In* BEGOLE Bo, KIM Jinwoo, INKPEN Kori et WOO Woontack (dir.), *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI 2015, Seoul, Republic of Korea, April 18-23, ACM Digital library, 2015, p. 1603-1612.

LENOIR Éric, « La prévention de la délinquance : un nouvel axe de la sécurité intérieure à la croisée des enjeux de la cohésion sociale », », *In* Frédéric DEBOVE et Olivier RENAUDIE (dir.), *Sécurité Intérieure : Les nouveaux défis*, Ed. Magnard-Vuibert, 2013, p. 11-20.

LEPETIT Bernard, « Histoire des pratiques, pratique de l'histoire », *In* LEPETIT Bernard (dir.), *Les formes de l'expérience. Une autre histoire sociale*, Paris, Ed. Albin Michel, 1995, p. 13 et s.

MAUSS Marcel, « L'âme, le nom et la personne » [1929], *In* MAUSS Marcel et KARADY Viktor (éds.), *Œuvres : Représentations collectives et diversité des civilisations*, t. II, Paris, Les Éditions de Minuit, Coll. Le sens commun, 1968-1969, p. 131-135

MAUSS Marcel, « Une catégorie de l'esprit humain : la notion de personne, celle de "moi" » [1938], *In* MAUSS Marcel, *Sociologie et anthropologie*, PUF, Coll. Bibliothèque de sociologie contemporaine, 1968, p. 331-362.

MEAD Margaret, « Identité », *In* BONTE Pierre et IZARD Michel (dir.), *Dictionnaire de l'ethnologie et de l'anthropologie*, , Paris 2002, p. 458-459.

MESTRE Jacques, PANCRAZI Marie-Ève, GROSSI Isabelle, MERLAND Laure et TAGLIARINO-VIGNAL Nancy, *Droit commercial : Droit interne et aspects de droit international*, Paris, Ed. LGDJ Lextenso, 2012, 29ème édition, 1324 p.

OYSERMAN Daphna et MARKUS Hazel Rose, "Self as social representation", *In* FLICK Uwe S. (éd.), *The Psychology of the Social,* Cambridge, Cambridge University Press, 1998, p. 107-125.

OPPENHEIMER Agnès, « Identité », *In* MIJOLLA Alain De (dir.), *Dictionnaire international de la psychanalyse*, 1, Ed. Calmann-Levy, Coll. Psychologie, Psychanalyse, Pédagogie, 2002, p. 783-784.

PERRIAULT Jacques, « Protection des identités numériques personnelles : des futurs incertains », *In* GALINON-MÉLÉNEC Béatrice et ZLITNI Sami (dir.), *Traces numériques : De la production à l'interprétation,* Paris, CNRS Éditions, OpenEdition books select, 2013, p. 23-34.

PÉTINIAUD Louis, « Cartographie de l'Affaire Snowden », *In* Hérodote N° 152-153, *Cyberespace : Enjeux géopolitiques*, Ed. La Découverte, 1er-2ème trimestre 2014, p. 35-42.

PETTY William Sir, *The Economic Writings of Sir William Petty, together with The Observations upon Bills of Mortality, more probably by Captain John Graunt*, Charles Henry Hull (ed.), Cambridge University Press, 1899, 2 Vol., 411 p. et 412 p.

PETTY William Sir, "The political anatomy or Ireland [1672], London 1691" *In The Economic Writings of Sir William Petty, together with The Observations upon Bills of Mortality, more probably by Captain John Graunt*, Charles Henry Hull (ed.), Cambridge University Press, 1899, Vol. I, p. 201 et s.

POULLET Yves et ROUVROY Antoinette, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », *In* BENYEKHLEF Karim et TRUDEL Pierre (dir.), *État de droit et virtualité*, Montréal, Ed. Thémis, 2009, p. 157-222.

RAZAC Olivier, « Il faut lutter contre les morts prématurées », *In* KIÉFER Audrey et RISSE Danielle (dir.), *La biopolitique outre-Atlantique après Foucault*, Colloque de 2012, Ed. L'Harmattan, Coll. Esthétiques - Culture et politique, 2012, p. 129-139.

RENAUDIE Olivier, « La vidéoprotection mobile à la recherche de son régime juridique », », *In* Frédéric DEBOVE et Olivier RENAUDIE (dir.), *Sécurité Intérieure : Les nouveaux défis*, Ed. Magnard-Vuibert, 2013, p. 251-262.

REY-DEBOVE Josette et REY Alain (dir.), *Le nouveau Petit Robert. Dictionnaire alphabétique et analogique de la langue française*, Paris, 1993, 2467 p.

ROBINET Jean-Baptiste-René, *Dictionnaire universel des sciences morale, économique, politique et diplomatique ; ou Bibliothèques de l'Homme-d'État et du citoyen*, t. 6, Tome premier[-trentième], À Londres, Chez les libraires associés. M.DCC.LXXVII [-M.DCC.LXXXIII], 1777-1778, reproduit par Gallica Bnf, p. 127-170.

ROSTAING Corinne, « Stigmate », *In* PAUGAM Serge (dir.), *Les 100 mots de la sociologie*, PUF, Coll. Que Sais-Je ?, 2010, p. 100-103.

ROUSSEAU Jean-Jacques, « Discours sur l'Économie Politique », Texte publié comme article dans *l'Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers, par une société de gens de lettres*, t. V, Mis en ordre & publié par M. DIDEROT, de l'Académie Royale des Sciences & des Belles Lettres de Pruffe ; quant à la Partie Mathématique, par M. D'ALEMBERT, de l'Académie Royale des Sciences de Paris, de celle de Pruffe, et de la Société Royale de Londres, Paris, Chez Briasson, David l'aîné, Le Breton, Durand, Gallica Bnf, 1755, p. 252 et s.

ROUSSEAU Jean-Jacques, « Huitième lettre écrite de la montagne » (1764), *In Œuvres complètes*, t. III : Du contrat social – Écrits politiques, Ed. Gallimard, Coll. Bibliothèque de la Pléiade n°169, 1964, 2240 p., p. 841 et s.

ROUVROY Antoinette, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des big data », *In* Conseil d'État, *Le numérique et les droits*

fondamentaux, Étude annuelle 2014, La documentation française, Les rapports du Conseil d'État n° 65, juillet 2014*,* p. 407-422.

SHEARING Clifford D. et STENNING Philip C., "From the Panopticon to Disney World: The development of discipline", *In* DOOB Anthony N. et GREENSPAN Edward L. (éds.), *Perspectives in Criminal Law: Essays in Honour of John Ll. J. Edwards,* Toronto, Canada Law Books, 1985, p. 335-349.

STROWEL Alain, « Le « droit à l'oubli » : mal nommé, mal défini, mais bienvenu : À propos de l'arrêt Google de la Cour de justice », (préf.), *In* CASTETS-RENARD Céline (dir.), *Quelle protection des données personnelles en Europe ?*, Bruxelles, Ed. Larcier, 2015, p. 9-15 (Conférence Quelle protection des données personnelles en Europe ? Toulouse, 14/03/2014).

TAJFEL Henri et TURNER John, "An integrative theory of intergroup conflict", *In* AUSTIN William G. et WORCHEL Stephen (éds.), *The social psychology of intergroup relations,* Monterey, CA, Ed. Brooks/Cole, 1979, p. 33-47.

TAJFEL Henri, « La catégorisation sociale », *In* MOSCOVICI Serge (éd.), *Introduction à la psychologie sociale*, t. I, Paris, Librairie Larousse, 1972, p. 272-302.

TOCQUEVILLE Alexis DE, *Considérations sur la Révolution* (1850-1858), I, 5, *In Œuvres*, t. 3, Ed. Gallimard, Coll. Bibliothèques de la Pléiade (n°503), 2004, p. 492 et s.

TURNER John C., "Some currents issues in research on social identity and self categorisation theories" *In* ELLEMERS Naomi, SPEARS Russel, et DOOSJE Bertjan (éds.), *Social Identity: Context, commitment, content*, Oxford, UK, Ed. Blackwell, 1999, p. 6-34.

VILLANI Tiziana, « Michel Foucault et le territoire : gouvernement et biopolitique », *In* PAQUOT Thierry et YOUNÈS Chris (dir.), *Le territoire des philosophes. Lieu et espace de la pensée au XX^{ème} siècle*, Ed. La découverte, Coll. Armillaires, 2009, p. 161-176.

WATIN-AUGOUARD Marc Général d'Armée, « Le *continuum* défense sécurité intérieure », », *In* Frédéric DEBOVE et Olivier RENAUDIE (dir.), *Sécurité Intérieure : Les nouveaux défis*, Ed. Magnard-Vuibert, 2013, p. 303-330.

ZAVALLONI Marisa, “E-motional memory and the identity system: Its interplay with representations of the social world”, *In* DEAUX Kay et PHILOGÈNE Gina (éds.), *Representations of the social: Bridging theoretical traditions*, Oxford, Blackwell publishing, 2001, p. 285-304.

ZAVALLONI Marisa, « L’identité psychosociale, un concept à la recherche d’une science », *In* MOSCOVICI Serge (éd.), *Introduction à la psychologie sociale,* t. II, Paris, Librairie Larousse, 1972, p. 245-265.

II. Articles et contributions

AGAMBEN [G.], « Comment l’obsession sécuritaire fait muter la démocratie », Le monde diplomatique n° 178, janvier 2014, p. 22-23.

AÏT-EL-HADJ [S.], « De la théorie du système technique à la systémique technologique. Une formalisation pertinente pour rendre compte de l'innovation technologique », *In* Innovations, Vol. 46, n° 1, 2015, p. 227-250.

BANAT-BERGER [F.] et HUC [C.], « Section 9 – Métadonnées », *In* PIAF – Portail International archivistique francophone, Version 1, 22 novembre 2011, p. 3-26.

BANISAR [D.], “Big Brother goes High-Tech”, Covert Action Quarterly, N° 56, Spring 1996, p. 6-10.

BEN AMOR [S.] et GRANGET [L.], « L'identité numérique : De la construction au suicide en 52 minutes », *In* Les Cahiers du numérique, *Identité numérique*, n° 2011/1, Vol. 7, Ed. Lavoisier, 2011, p. 103-115.

BENJAMIN [B.], “John Graunt’s “Observations”” (reprint of the 1st edition), *In* Journal of the Institute of Actuaries, Vol. 90, Issue 1, June 1964, p. 1–61.

BERNERS-LEE [T.], HENDLER [J.] et LASSILA [O.], “The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities*”, In Scientific American*, Vol. 284, n° 5, Mai 2001, p. 34-43.

BERTRAND [E.] et DESTAIS [C.], « Le « théorème de Coase », une réflexion sur les fondements microéconomiques de l'intervention publique », *In Reflets et perspectives de la vie économique*, Ed. De Boeck Supérieur, t. XLI, Vol. 2, 2002, p. 111-124.

BONENFANT [M.] et GENVO [S.], « Une approche située et critique du concept de gamification », *In* Revue Sciences du jeu, *Questionner les mises en forme ludiques du web : gamification, ludification et ludicisation*, N° 2, 2014, p. 1-4.

BOX [G. E. P.], "Science and Statistics", *In Journal of the American Statistical Association*, Vol. 71, N° 356, Décembre 1976, p. 791-799.

BRETONNEAU [A.], « Le droit au « déréférencement » : champ territorial », Conclusions sur Conseil d'État, 19 juillet 2017, Google Inc., n° 399922, Lebon (AJDA 2017, p. 1479), RFDA 2017, p. 972.

BRINGS [A.], "Identity Construction Online: An Analysis of Sherry Turkle's Ideas on the Influence of Technology on Identity", Gonzaga University, COML 509, p. 3-17.

BRUNET [E.], « Règlement général sur la protection des données à caractère personnel – genèse de la réforme et présentation globale », Dalloz IP/IT 2016, p. 567.

BUSH [V.], "As we may think", *In* The Atlantic Monthly, Vol. 176, n° 1, July 1945, p. 101-110.

CAPRIOLI [É. A.], MATTATIA [F.] et VULLIET-TAVERNIER [S.], « L'identité numérique », *In* Cahiers de droit de l'entreprise n° 3, entretien 3, LexiNexis, Mai 2011, p. 3.

CATE [F. H.], DEMPSEY [J. X.], RUBINSTEIN [I.], "Systematic government access to private-sector data", *In* International Data Privacy Law, Vol. 2, n° 4, novembre 2012, p. 195–199.

CHARTIER [R.], « Le monde comme représentation », *In* Annales Histoire Sciences sociales, Vol. 44, n°6, novembre- décembre 1989, p. 1505-1520.

CHINOY [S.], « La reconnaissance faciale, impossible d'y échapper », *In* Courrier International n° 1487, *Tous surveillés,* Mai 2019, p. 32-34.

CITRON [D. K.], "Technological Due Process," *In* Washington University Law Review, Vol. 85, Issue 6, 2008, p. 1249-1314.

COASE [R. H.], « The problem of social cost », *In* The journal of Law & Economics, Vol. III, Octobre 1960, p. 1-44.

COHEN [J. E.], "Examined Lives: Informational Privacy and the Subject as Object", *In* Stanford Law Review Vol. 52, Mai 2000, p. 1373-1438.

CONKLIN [J.] et BEGEMAN [M. L.], "gIBIS: a hypertext tool for exploratory policy discussion", *In* CSCW '88 Proceedings of the 1988 ACM conference on Computer-supported cooperative work, Portland, Oregon-USA, September 26 - 28, 1988, p. 140-152.

CULTURES & CONFLITS, « Société de la connaissance, société de l'information, société de contrôle. Entretien avec Armand Mattelart », *In* Cultures & Conflits n°64 – *Identifier et surveiller*, hiver 2006, Vol. 4, p. 167-183.

DANET [J.], « Les politiques sécuritaires à la lumière de la doctrine de la défense sociale nouvelle », RSC 2010, p. 49.

DEFFERRARD [F.], « Chasser l'oubli comme du gibier », Dalloz IP/IT 2017, p. 672.

DELAGE [P.-J.], « La dangerosité comme éclipse de l'imputabilité et de la dignité », RSC 2007, p. 799.

DELAGE [P.-J.], « Vérité et ambiguïté autour de l'imputabilité morale - À propos de Crim. 21 janvier 2009 », RSC 2009, p. 69.

DELMAS-MARTY [M.], « Comment sortir de l'impasse ? », RSC 2010, p. 107

DELMAS-MARTY [M.], « Le crime contre l'humanité, les droits de l'homme, et l'irréductible humain », RSC 1994, p. 477.

DELMAS-MARTY [M.], « Les politiques sécuritaires à la lumière de la doctrine pénale du XIX^e au XXI^e siècle », Introduction, RSC 2010, p. 5.

DENNING [P. J.], COMER [D. E.], GRIES [D.], MULDER [M. C.], TUCKER [A.], TURNER [A. J.] et YOUNG [P. R.], "Computing as a discipline", *In* Communications of the ACM, Vol. 32, n°1, janvier 1989, p. 9-23.

ÉDITORIAL Les Annales, « Histoire et sciences sociales. Un tournant critique ? », *In* Annales ESC- Histoire et Sciences sociales 43ème année, n° 2, mars-avril 1988, p. 291-293.

EMERSON [T. I.], "Nine Justices in Search of a Doctrine", *In* Michigan Law Review, Vol. 64, n° 219, Décembre 1965, p. 219-234.

ENGELBART [D.], « Authorship Provisions in Augment », *In* COMPCON '84 Digest, *Proceedings of the COMPCON Conference*, San Francisco, CA, February 27 – March 1, 1984 (OAD, 2250), 1984, p. 465-472.

ERTZSCHEID [O.], « L'homme, un document comme les autres », *In* Hermès, La Revue 2009/1, n° 53, p. 33-40.

ETOA [S.], « Corps humain et liberté », *In* Cahiers de la Recherche sur les Droits Fondamentaux, *Le corps humain saisi par le droit : entre liberté et propriété*, N° 15, 2017, p. 19-26.

FALQUE-PIERROTIN [I.], « Interview de Madame Isabelle Falque-Pierrotin, Présidente de la CNIL », Dalloz IP/IT 2018, p. 5.

FITZPATRICK [S.], « L'identité de classe dans la société de la NEP », *In* Annales ESC - Histoire et Sciences sociales, n° 2, mars-avril 1989, p. 251-271.

FLICHY [P.], "Connected Individualism between Digital Technology and Society", *In* Réseaux, Vol. n° 124, n° 2, 2004, p. 17-51.

FOREST [D.], « Identité(s) Numérique(s) : Tous authentifiés ? », *In* CNIL – Cahier IP Innovation & Prospective N° 01, *Vie privée à l'horizon 2020*, octobre 2012, p. 38-40.

FOUCAULT [M.], « L'évolution de la notion d'« individu dangereux » dans la psychiatrie légale du XIX^{e} siècle », Communication au symposium de Toronto « Law and Psychiatry », Clarke Institute of Psychiatry, 24-26 octobre 1977, *In* Journal of Law and Psychiatry, Vol. I, 1978, p. 1-18.

FROOMKIN [A. M.], "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases", *In* 15 U. Pittsburgh Journal of Law and Commerce 395, 1996, p. 479-505.

GALTON [F.], "Co-relations and their measurement, chiefly from anthropometric data", *In* Proceedings of the Royal Society, Vol. 45, December 1888, p. 135-145.

GALTON [F.], "Kinship and Correlation", *In* North American Review, Vol. 150, 1890, p. 419-431.

GELABERT [E.], « Le Printemps arabe en perspective », *In* Cahiers de l'action Vol. 39, N° 2, 2013, p. 11-17.

GIL [R.], « Neurotechnologies : Prendre conscience de leurs dangers éthiques », *In* Espace éthique Poitou-Charentes, janvier 2018, p. 1-2.

GINSBERG [J.], MOHEBBI [M. H.], PATEL [R. S.], BRAMMER [L.], SMOLINSKI [M. S.] et BRILLIANT [L.], "Detecting influenza epidemics using search engine query data", *In* Nature Vol. 457, February 2009, p. 1012-1014.

GIUDICELLI-DELAGE [G.], « Droit pénal de la dangerosité - Droit pénal de l'ennemi », RSC 2010, p. 69.

GO [A.], BHAYANI [R.] et HUANG [L.], “Twitter Sentiment Classification using Distant Supervision”, *In* technical report, Stanford University, Processing journal, Vol. 150, 2009, p. 1-6.

GUICHARD [J.], « Se faire soi », *In* OSP, L’Orientation scolaire et professionnelle, Vol. 33, n° 4, Éd. INETOP, 2004, p. 499-533.

HALPERN [S.M.], « Tous fichés, Tous manipulés », *In* Books – L’actualité à la lumière des livres, Hors-série N° 14, *Internet : pièges et maléfices*, Ed. Books, Coll. Books Le Magazine, décembre 2018-Janvier 2019, p. 45-48.

HARCOURT [B.], « Une généalogie de la rationalité actuarielle aux États-Unis aux XIX^{e} et XX^{e} siècles », RSC 2010, p. 31.

HARMAN [G.], “Zeroing in on evocative objects”, *In* Human Studies, Vol. 31, N° 4, 2008, p. 443-457.

HERGERT [M.] et MORRIS [D.], “Accounting Data for Value Chain Analysis”, *In* Strategic Management Journal, Vol. 10, N° 2, Mars - Avril 1989, p. 175-188.

JOURNÈS [C.], « Alternance et continuité en matière de sécurité intérieure », RSC 2013, p. 889.

KAPFERER [J.-N.], « Maîtriser l'image de l'entreprise : le prisme d'identité », *In* Revue Française de Gestion N° 71, novembre-décembre 1988, Lavoisier, 1988, p. 76-83.

KARAS [S.], « Privacy, Identity, Databases », *In* American University Law Review, Vol. 52, Issue 2, 2002, p. 393-445.

KECK [F.], « Les usages du biopolitique », *In* L’Homme n° 187-188, Juillet-Décembre 2008, Miroirs transatlantiques, Ed. EHESS, p. 295-314.

KELSEN [H.], « Qu'est-ce que la théorie pure du droit ? » (1953), *In* Droit et Société n° 22, *Transformations de l'État et changements juridiques : l'exemple de l'Amérique Latine*, LGDJ, 1992, p. 551-568.

KHATCHATOUROV [A.] et CHARDEL [P.-A.], « Fiche 1. La construction de l'identité dans la société contemporaine : enjeux théoriques », *In* Chaire Valeurs et Politiques des Informations Personnelles, *Cahier N°1 Identités numériques*, coordonné par C. Levallois-Barth, Institut Mines-Télécom, mars 2016, p. 11-16.

KROPP [J.] et BRUNEAU [S.] (recension), « Irvin Waller, Lutter contre la délinquance - Comment le tout répressif tue la Sécurité », Notes bibliographiques, RSC 2011, p. 278.

LANERET [N.] et HAMON [S.], « Quel avenir pour les transferts internationaux ? », Dalloz IP/IT 2018, p. 31.

LAUNAY [Amiral J.], « Sécurité et défense », RFDA 2011, p. 1099.

LE BOT [O.], « Le respect de la vie privée comme liberté fondamentale », Note sous CE, ord., 25 oct. 2007, Mme Y, n° 310125, mentionnée aux tables du recueil, RFDA 2008, p. 328.

LE BOT [O.], « Un état d'urgence permanent ? (Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme) », RFDA 2017, p. 1115.

LEVASSEUR [G.], « Confrontation du droit pénal classique et de la défense sociale », Rapport de synthèse - XII^{e} Journées de défense sociale, RSC 1964, p. 721.

LUGMAYR [A.], SUTINEN [E.], SUHONEN [J.], ISLAS SEDANO [C. A.], HLAVACS [H.] et SUERO MONTERO [C.], "Serious storytelling - a first definition and review", *In* Multimedia Tools and Applications Vol. 76, Issue 14, January 2017, Springer Science & Business Media New York, 2016, p. 15707-15733.

MARKUS [H. R.], "Self-schemata and Processing Information about the Self", *In* Journal of Personality and Social Psychology, Vol. 35, N° 2, Février 1977, p. 63-78.

MAZEAUD [V.], « La constitutionnalisation du droit au respect de la vie privée », *In* Les Nouveaux cahiers du Conseil Constitutionnel n° 48, *Dossier : Le Conseil constitutionnel et la vie Privée*, Vol. 48, n° 3, Juin 2015, p. 7 à 20.

MCCORMICK [J.], « Ce que votre voix dit de vous », Extraits de "What AI can tell from listening to you", The Wall street journal, publié le 1er avril 2019, *In* Courrier International n° 1487, *Tous surveillés,* Mai 2019, p. 34-36.

MÜLLER [O.] et ROTTER [S.], "Neurotechnology: Current Developments and Ethical Issues", *In* Frontiers in systems Neuroscience, Vol. 11 n° 93, publié le 13 décembre 2017.

NEISSE [F.] et NOVOSSELOFF [A.], « L'expansion des murs : le reflet d'un monde fragmenté ? » *In* IFRI, Politique étrangère, Vol. Hiver n°4, 2010, p.731-742.

NELSON [T.], "Complex information processing: a file structure for the complex, the changing and the indeterminate", *In* ACM '65 Proceedings of the 1965 20th national conference, Cleveland, Ohio, USA, August 24 - 26, 1965, p. 84-100.

NISSENBAUM [H.], "Privacy as contextual integrity", *In* Washington Law Review, Vol. 79, n° 1, février 2004, p. 119-157.

PARIZOT [R.], « Présomption d'innocence *versus* marqueurs de culpabilité : quel équilibre ? », RSC 2019, p. 127.

PASQUALE [F.], "Reclaiming Egalitarianism in the Political Theory of Campaign Finance Reform," *In* University of Illinois Law Review 45, Vol. 45, N° 2, 2008, p. 599-660.

PATTON [C.], "Electronic Investment Tools Highlight Conference", *In* InfoWorld: the newspaper for the microcomputing community, Vol. 10, n° 32, InfoWorld Media Group Inc., 25 juillet 1988, p. 22-24.

PIAZZA [P.], « Les résistances au Projet INES », *In* Cultures & Conflits n° 64 – *Identifier et surveiller*, hiver 2006, Vol. 4, p. 65-75.

PROZOROVA-THOMAS [V.], « Le classement selon le principe de pertinence comme reflet de la commande d'État : les archives soviétiques », *In* Matériaux pour l'histoire de notre temps, *L'historien face à l'ordre informatique*, Vol. 2, N° 82, La contemporaine, 2006, p. 58-64.

QUÉMÉNER [M.], « Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme », Dalloz IP/IT 2017, p. 657.

QUONIAM [L.] et LUCIEN [A.], « Du web 2.0 à l'intelligence compétitive 2.0 », *In* 7ème colloque du chapitre français de l'ISKO, *Intelligence collective et organisation des connaissances*, Juin 2009, p. 15-24.

RIGAUX [F.], « La liberté de la vie privée », *In* Revue internationale de droit comparé, Vol. 43, N°3, Juillet-septembre 1991, p. 539-563.

RODRIGUES [R.], "The Surveillance Industry in Europe", *In* The IRISS Project, *Surveillance, Fighting Crime and Violence*, IRISS-Increasing Resilience in Surveillance Societies, 17 décembre 2012, p. 71-158.

ROHRBASSER [J.-M.], « John Graunt et les bulletins de Londres : une statistique de la mortalité au XVIIe siècle », *In* Dix-septième siècle, Vol. 243, N° 2, PUF, 2009, p. 345-368.

SAMUEL [A. L.], "Some Studies in Machine Learning Using the Game of Checkers", *In* IBM Journal, Vol. 3, N° 3, July 1959, p. 535-554.

SAURON [J.-L.] et QUÉMÉNER [M.], « Le régime de sanction du RGPD : quand la complétude l'emporte sur la cohérence », Dalloz IP/IT 2018, p. 23.

SCHRAMECK [O.], « Sécurité et liberté », RFDA 2011, p. 1093.

SELIMI [F.], CRISTEA [I. M.], HELLER [E.], CHAIT [B. T.] et HEINTZ [N.], « Comprendre la connectique du cerveau en disséquant chaque type de synapse », "Proteomic Studies of a Single CNS Synapse Type: The parallel Fiber/Purkinje cell synapse", *In* PLoS Biology, Vol. 7, n° 4, 14 avril 2009 (et La recherche en sciences du vivant, Institut des sciences biologiques – CNRS), p. 0949-0957.

SOBEL [R.], “The Degradation of Political Identity under a National Identification System”, *In* Boston University Journal of Science and Technology Law, Vol. 8, Issue 1, Winter 2002, p. 37- 75.

STENGERS [J.], « Vaillé (Eugène). Le Cabinet Noir. », *In* Revue belge de philologie et d'histoire, t. 30, fasc. 1-2, 1952, p. 363-368.

TABET [S.], « Du projet moderne au monde liquide. Entretien avec Zygmunt Bauman », *In* Socio - La nouvelle revue des sciences sociales, *Zygmunt Bauman, critique de la modernité/Entretien*, n° 8, Ed. de la Maison des sciences de l’homme, juin 2017, p. 35-56.

THIETART [R.A.] et VIVAS [R.], “An Empirical Investigation of Success Strategies for Businesses along the Product Life Cycle”, *In* Management Science, Vol. 30, N° 12, Décembre 1984, p. 1405-1423.

TURKLE [S.], “Computational technologies and images of self”, *In* Social Research, *In Technology and the rest of culture*, Vol. 64, N° 3, 1997, p. 1093-1111.

VAIDHYANATHAN [S.], “Remote Control: The rise of electronic cultural policy”, *In* Annals of the American Academy of political and social science Vol. 597, Issue 1, du 1er janvier 2005, p. 122-133.

VULBEAU [A.], « Contrepoint - L’infobésité et les risques de la surinformation », *In* Informations sociales, Vol. 191, N° 5, 2015, p. 35-35.

WEIGEND [T.] et CAPITANT [D.] (comm.), « BVerfG, arrêt du 5 février 2004 Mucke, 2 BvR 2029/01, BVerfGE 109, 133 », RSC 2004, p. 689 (et NJW 2004, p. 911 et s., note J. Kinzig ; KritV 2004, p. 137, note T. Mushoff).

WING [J. M.], “Computational thinking and thinking about computing”, *In* Philosophical Transactions of the Royal Society, Series A - Mathematical, Physical, and Engineering Sciences, n° 366, 2008, p. 3717–3725.

WU [T.], “Network neutrality, Broadband discrimination”, *In* Journal of Telecommunications and High technology Law, Vol. 2, n° 1, 2003, p. 141-179.

ZAFFARONI [E. R.], « Dans un État de droit il n’y a que des délinquants », RSC 2009, p. 43.

ZUBOFF [S.], « Le nouveau visage du capitalisme », Financial Times (extraits), Londres, publié le 25 janvier 2019, *In* Courrier International n° 1487, *Tous surveillés*, mai 2019, p. 36-38.

III. Rapports, avis & débats publics français

* Du parlement et du sénat

Avis n° 110 (2017-2018) présenté au nom de la Commission des affaires étrangères, de la défense et des forces armées sur le projet de loi de finances pour 2018, adopté par l’Assemblée nationale, t. VIII - Défense : Équipement des forces, par M. Cédric PERRIN et Mme. Hélène CONWAY-MOURET, déposé le 23 novembre 2017, Sénat, 135 p.

Débats parlementaires sur la Loi de finances pour 1967, Compte-rendu intégral – 12ème Séance, 1ère Séance du 13 octobre 1966, JO Année 1966-1967 – N° 79 A.N., du 14 octobre 1966, p. 3378-3399.

Débats parlementaires sur le projet de loi Informatique et libertés – Compte-rendu intégral – 2ème Séance, 1ère Séance du 4 octobre 1977, JO Année 1977-1978 – N° 79 A.N., du 5 octobre 1977, p. 5782-5793.

Délégation parlementaire au renseignement, Rapport N° 1012 (Assemblée Nationale) N° 557 (Sénat) (1012/557) relatif à l’activité de la délégation parlementaire au renseignement pour l’année 2012, Par Mme Patricia ADAM, du 30 avril 2013, 21 p.

Délégation parlementaire au renseignement, Rapport N° 4573 (Assemblée Nationale) N° 448 (Sénat) relatif à l’activité de la délégation parlementaire au renseignement pour l’année 2016, Par Mme Patricia ADAM, du 2 mars 2017, 93 p.

Délégation parlementaire au renseignement, Rapport N° 875 (Assemblée Nationale) N° 424 (Sénat) relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017, Par M. Philippe BAS, du 12 avril 2018, 78 p.

Rapport n° 72 fait au nom de la Commission des lois, sur le projet de loi, adopté par l'Assemblée Nationale, relatif à l'Informatique et aux libertés, par M. Jacques THYRAUD, Sénat, Session de 1977-1978, déposé le 10 novembre 1977, 75 p.

Rapport n° 199 fait au nom de la Commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale, sur le projet de loi, adopté avec modifications par l'Assemblée nationale en deuxième lecture, relatif à l'informatique et aux libertés, par M. Jacques THYRAUD, Sénat, Session de 1977-1978, déposé le 19 décembre 1977, 52 p.

Rapport d'information n° 439 (2004-2005) fait au nom de la mission d'information de la Commission des lois sur la nouvelle génération de documents d'identité et la fraude documentaire, par M. Jean-René LECERF, déposé le 29 juin 2005, *Identité intelligente et respect des libertés*, Sénat, Coll. Les Rapports du Sénat, 113 p.

Rapport d'information n° 220 (2006-2007) fait au nom de la Commission des Finances, du contrôle budgétaire et des comptes économiques de la Nation sur l'enquête de la Cour des comptes relative au fonctionnement de l'Agence nationale de valorisation de la recherche (ANVAR) et à sa transformation en OSEO-ANVAR, par M. Maurice BLIN, déposé au Sénat le 7 février 2007, 77 p.

Rapport d'information n° 675 (2010-2011) fait au nom de la Mission commune d'information sur : « Mediator : évaluation et contrôle des médicaments », par Mme. Marie-Thérèse HERMANGE, déposé au Sénat le 28 juin 2011, t. I : Rapport, 271 p.

Rapport d'information n° 559 (2016-2017) fait au nom de la Commission des affaires étrangères, de la défense et des forces armées par le groupe de travail « Les drones dans les forces armées », par MM. Cédric PERRIN, Gilbert ROGER, Jean-Marie BOCKEL et Raymond VALL, *Drones d'observation et drones armés : un enjeu de souveraineté*, déposé au Sénat le 23 mai 2017, 99 p.

Rapport n° 592 (2017-2018) fait au nom de la Commission des Lois Constitutionnelles, de la législation et de l'administration générale de la République sur le Projet de loi relatif à la Protection des données personnelles (n°490), par Mme. Paula FORTEZA, enregistré à la Présidence de l'Assemblée nationale le 25 janvier 2018, 253 p.

Rapport n° 476 (2017-2018) fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, par M. Christian CAMBON, déposé au Sénat le 16 mai 2018, 711 p.

Rapport n° 1302 (2017-2018) fait au nom de la Commission des finances, de l'économie générale et du contrôle budgétaire sur le Projet de loi de finances pour 2019 (n° 1255), par M. Joël GIRAUD, t. I : Exposé général, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2018, 230 p.

Rapport d'information n° 299 (2018-2019) fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, par MM. Olivier CADIC et Rachel MAZUIR, *Cyberattaque contre « ARIANE » : une expérience qui doit nous servir*, déposé au Sénat le 6 février 2019, 55 p.

Rapport n°7 (2019-2020) fait au nom de la Commission d'enquête du Sénat, sur la souveraineté numérique par M. Gérard LONGUET, t. I : Rapport, *Le devoir de souveraineté numérique*, déposé au Sénat le 1er octobre 2019, 207 p.

Rapport d'information n° 3581 (2019-2020) fait par la Commission des affaires étrangères en conclusion des travaux d'une mission d'information constituée le 31 octobre 2018 sur *le contrôle des exportations d'armement*, par M. Jacques MAIRE et Mme Michèle TABAROT, enregistré à la présidence de l'Assemblée Nationale le 18 novembre 2020, 157 p.

Note de synthèse « Projet Identité Nationale Électronique et Sécurisée », par Richard YUNG, sénateur, 2005, 3 p.

Projet de loi pour une République numérique – Étude d'impact, NOR : EINI1524250L/Bleue, 9 décembre 2015, Dossiers législatifs de l'Assemblée Nationale, 148 p.

Texte adopté n° 883 « *Petite loi* », Proposition de loi relative à la protection de l'identité (Texte définitif), du 6 mars 2012, Assemblée nationale, Session ordinaire de 2011-2012, 7 p.

* Des Commissions, conseils et autorités publiques

Autorité de la concurrence, Avis n° 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne, 79 p.

Autorité de la concurrence, Avis n° 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, 125 p.

Autorité de la concurrence, « Droit de la concurrence et données », étude coréalisée avec l'Autorité de concurrence allemande le Bundeskartellamt, du 10 mai 2016, 63 p.

Autorité de la Concurrence, Communiqué de Presse « L'Autorité rend son avis sur la publicité en ligne » : Enquête sectorielle sur la publicité en ligne, publié le 6 mars 2018, 3 p.

Avis du Conseil Économique et Social, « Les nanotechnologies », présenté par M. Alain OBADIA, au nom de la section des activités productives, de la recherche et de la technologie, NOR : CES. X08000121V, JORF du 2 juillet 2008, texte n° 21, La documentation française, juin 2008, 178 p.

CERNA, « La souveraineté à l'ère du numérique : Rester maîtres de nos choix et de nos valeurs », par Jean-Gabriel GANASCIA, Éric GERMAIN et Claude KIRCHNER, CERNA – Allistene, octobre 2018, 36 p.

CESE, Avis du 13 janvier 2015 présenté par M. Eric PERES, au nom de la section de l'éducation, de la culture et de la communication, « Les données numériques : un enjeu d'éducation à la citoyenneté », NOR : CESL1500001X, Les Avis du Conseil économique, social et environnemental, Les Éditions des JO, janvier 2015, 145 p.

CNCDH, Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, JORF n°0126 du 3 juin 2018, Texte n° 63 sur 105.

Commissariat Général à la stratégie et à la prospective, La Note d'analyse N° 08-11/2013, « Analyse des big data : Quels usages, quels défis ? », par MM. Marie-Pierre HAMEL et David MARGUERIT (département Questions sociales), Novembre 2013, 11 p.

Conseil National des politiques de lutte contre la pauvreté et l'exclusion sociale (CNLE), « Contribution au suivi du plan pluriannuel contre la pauvreté et pour l'inclusion sociale », Les Cahiers du CNLE, mars 2017, 155 p.

Commission générale de terminologie et de néologie, Vocabulaire de l'informatique et de l'internet, Avis et Communications, JORF du 6 juin 2010, Texte n° 42 sur 51.

Commission générale de terminologie et de néologie, Vocabulaire de l'informatique et de l'internet (liste de termes, expressions et définitions adoptés), Avis et Communications, JORF n°0001 du 1er janvier 2013, Texte n° 114 sur 120.

Commission générale de terminologie et de néologie, Vocabulaire « tous domaines », Avis et Communications, JORF n°0179 du 5 août 2014 (p. 12995), texte n° 91 sur 99.

Dictionnaire de terminologie archivistique, Direction des archives de France 2002, Mise en forme par les Archives départementales du Nord, du 19 octobre 2007, 36 p.

Direction générale de la concurrence, de la consommation et de la répression des fraudes - DGCCRF, Enquête Communications électroniques : une surveillance attentive du marché, du 10 août 2015, Ministère de l'économie, des finances et de la relance, 2 p.

Institut d'études Opinion et Marketing en France et à l'international, « L'impact de l'e-réputation sur le processus d'achat », Sondage Ifop pour Réputation VIP, décembre 2014, 29 p.

Les Actes de l'ARCEP, « Neutralité de l'internet et des réseaux. Propositions et recommandations », Autorité de régulation des communications électroniques et des postes, septembre 2010, 62 p.

Livre blanc sur la défense et la sécurité nationale, Ed. Odile Jacob/ La Documentation française, Paris, juin 2008, 350 p.

Livre blanc sur la défense et la sécurité nationale, La documentation française, Ministère de la défense, Avril 2013, 159 p.

Note complémentaire destinée à l'Afssaps : benfluorex et décès, CNAMTS-DSES-DEPP (Département des études sur les pathologies et les patients), complète et précise la précédente note intitulée « Benfluorex, valvulopathies cardiaques et décès » demandée par l'Afssaps le 25 août 2010 et transmise à cette dernière le 28 septembre 2010, CNAMTS 2, novembre 2010, 17 p.

Note de recherche n° 52 de l'IRSEM - Institut de recherche stratégique de l'école militaire, « Un espace européen des drones », par Chantal LAVALLÉE et Océane ZUBELDIA, du 7 mars 2018, 9 p.

Projet UTIC - Livrable 1 « Capacités d'interception et surveillance », par Philippe GUILLOT et Daniel VENTRE, Paris 8 – CNRS, Version du 03 avril 2017, 57 p.

Revue Stratégique de défense et de sécurité nationale 2017, DICoD - Bureau des Éditions, Octobre 2017, 109 p.

* De la CNIL

CNIL, Cahiers IP Innovation & Prospective N° 01, « Vie privée à l'horizon 2020 », direction des études, de l'innovation et de la prospective de la CNIL, octobre 2012, 58 p.

CNIL, Cahiers IP Innovation & Prospective N° 02, « Le corps, Nouvel objet connecté – Du Quantified Self à la M-Santé : les nouveaux territoires de la mise en données du monde », direction des études, de l'innovation et de la prospective de la CNIL, mai 2014, 62 p.

CNIL, Cahiers IP Innovation & Prospective N° 06 « La forme des choix : Données personnelles, design et frictions désirables », Linc-CNIL, janvier 2019, 48 p.

CNIL, Communiqué de Presse, « Vidéosurveillance/vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », du 21 juin 2012, 14 p.

CNIL, Décision n° 2015-047 du 21 mai 2015 mettant en demeure la société X (Google Inc.), publiée sur Légifrance le 19 juin 2015.

CNIL, Délibération n° 2005-279 du 22 novembre 2005 portant avis sur le projet de décret instituant le passeport électronique et sur les modifications apportées au traitement DELPHINE permettant l'établissement, la délivrance et la gestion des passeports, NOR : CNIX0508964X, publiée sur Légifrance le 13 novembre 2019.

CNIL, Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X (Google Inc.), publiée sur Légifrance le 26 mars 2016.

CNIL, Délibération de la formation restreinte n° 2016-405 du 15 décembre 2016 prononçant une sanction pécuniaire à l'encontre de la société X, publiée sur Légifrance le 30 décembre 2016.

CNIL, Délibération de la formation restreinte n°2016-406 du 15 décembre 2016 prononçant une sanction pécuniaire à l'encontre de la société X, publiée sur Légifrance le 30 décembre 2016.

CNIL, Délibération n° 2017-165 du 1 juin 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » et « sous-traitant » du groupe BOX. (BCR-040), publiée sur Légifrance le 27 juin 2017.

CNIL, Délibération n° 2017-239 du 7 septembre 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » du groupe UTC (BCR n° 045), NOR : CNIL1726031X, publiée sur Légifrance le 19 septembre 2017.

CNIL, Délibération n° 2017-273 du 12 octobre 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » du groupe Merck & Co (MSD) (BCR n° 046), NOR : CNIL1730041, publiée sur Légifrance le 1 novembre 2017.

CNIL, Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978 (demande d'avis n°17023753), publiée sur Légifrance le 14 décembre 2017, 40 p. ;

CNIL, Délibération n° 2017-306 du 7 décembre 2017 portant autorisation unique de transferts de données à caractère personnel hors Espace économique européen encadrés par les règles internes d'entreprise (BCR) « responsable de traitement » du groupe DANFOSS. (BCR n° 047), NOR : CNIL1736110X, publiée sur Légifrance le 6 mars 2018.

CNIL, Délibération n° 2018-259 du 14 juin 2018 portant avis sur un projet de décret relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire) (demande d'avis n° 18006270), JORF n°0181 du 8 août 2018, texte n° 124 sur 142.

CNIL, Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD), JORF n° 0256 du 6 novembre 2018, texte n° 81 sur 134.

CNIL, Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, JORF n° 0256 du 6 novembre 2018, texte n° 82 sur 134.

CNIL, Rapport de la Commission informatique et libertés remis le 27 juin 1975 (décret n° 74.938 du 8 novembre 1974), par M. Bernard Tricot, La Documentation française (410), Paris, 1975, 106 p.

CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Application aux objets connectés », édition février 2018, 48 p.

CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Étude de cas « CAPTOO » », édition février 2018, 37 p.

CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – La méthode », édition février 2018, 11 p.

CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Les modèles », édition février 2018, 25 p.

CNIL, « Analyse d'impact relative à la protection des données – *Privacy Impact Assessment* (PIA) – Les bases de connaissances », édition février 2018, 106 p.

CNIL, « Le Privacy Shield » - Privacy Shield EU-US, ou Bouclier de protection des données UE-US du 1er août 2016.

CNIL, « Le droit à la portabilité en questions », du 22 mai 2017.

CNIL, « L'accès des autorités publiques aux données chiffrées », du 30 août 2017.

CNIL, « FNAEG : Fichier national des empreintes génétiques », du 15 novembre 2018.

CNIL, « TAJ : Traitement d'Antécédents Judiciaires », du 15 novembre 2018.

CNIL, « La certification et les codes de conduite », 19 décembre 2018.

CNIL, « Approbation des BCR : les différentes étapes ».

CNIL, Définition « Traitement de données personnelles ».

CNIL, Définition « Quantified Self ».

CNIL, « La procédure de sanction ».

CNIL, « Le cadre européen ».

CNIL, « Le Quantified Self, c'est quoi ? ».

CNIL, « Les Guides PIA ».

IV. Rapports, avis & débats publics européens et internationaux

* Du parlement, de la commission et du conseil européens

Amendements du Parlement européen, adoptés le 17 janvier 2018, à la proposition de règlement du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte) (COM(2016)0616 – C8-0393/2016 – 2016/0295(COD)), A8-0390/2017 (Procédure législative ordinaire – refonte).

Commission des Communautés européennes, "Commission Communnication on the protection of Individuals in relation to the processing of personal data in the Community and Information security", COM(90) 314 final - SYN 287 and 288, Bruxelles, 13 Septembre 1990, 133 p.

Commission des Communautés européennes, "Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", COM(92) 422 final - SYN 287, Bruxelles, 15 octobre 1992, 130 p.

Communication de la Commission, « Vers une stratégie européenne en faveur des nanotechnologies », Office des publications officielles des Communautés européennes, COM/2004/0338 final, 12 mai 2004, 24 p.

Communication de la Commission au Parlement Européen et au Conseil, « Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique », COM/2013/0846 final, Bruxelles, 27 novembre 2013, 12 p.

Communication de la Commission au Parlement Européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des

entreprises établies sur son territoire, COM/2013/0847 final, Bruxelles, 27 novembre 2013, 23 p.

Communication de la Commission au parlement européen et au Conseil, « Échange et protection de données à caractère personnel à l'ère de la mondialisation », COM/2017/07 final, Bruxelles, 10 janvier 2017, 18 p.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Artificial Intelligence for Europe", COM/2018/237 final, Bruxelles, 25 avril 2018, 19 p.

Commission européenne - Communiqué de presse, « Concentrations : la Commission inflige des amendes de 110 millions EUR à Facebook pour avoir fourni des renseignements dénaturés concernant l'acquisition de WhatsApp », Bruxelles, le 18 mai 2017.

Commission européenne - Communiqué de presse, « Union de la sécurité : la Commission comble les lacunes en matière d'information afin de mieux protéger les citoyens de l'Union », Strasbourg, le 12 décembre 2017.

Commission européenne - Communiqué de presse, « Union de la sécurité : adoption du système d'information Schengen renforcé », Bruxelles, le 19 novembre 2018.

Commission européenne, Communiqué de Presse « Intelligence artificielle », Bruxelles, le 7 décembre 2018.

Commission européenne - Communiqué de presse, « La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde », Bruxelles, le 23 janvier 2019.

Draft Council Resolution on New Technologies, Document 10951/1/98 Limite ENFOPOL Rev 1, Note et Document 10951/2/98 ENFOPOL rev 2 + cor 1, Bruxelles, 4 novembre 1998.

Draft Council Resolution on the lawful interception of telecommunications in relation to new technologies, Document 6715/99 Limite ENFOPOL 19, Bruxelles, 15 mars 1999.

Commission des libertés publiques et des affaires intérieures du Parlement européen, Rapport sur le projet de résolution du Conseil relative à l'interception légale des télécommunications compte tenu des nouvelles technologies (10951/2/98 - C40052/99 - 99/0906(CNS)), Document de séance A4-0243/99, par M. Gerhard SCHMID, du 23 avril 1999, 11 p.

Commission des libertés publiques et des affaires intérieures du Parlement européen, Interception Capabilities 2014 – State Interference with privacy on the internet, commissioned by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), Presentation in Session II, par M. Duncan CAMPBELL, Bruxelles, Octobre 2013, 29 p.

Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)), Document de séance A7-0139/2014, par M. Claude MORAES, du 21 février 2014, 69 p.

Commission temporaire sur le système d'interception ECHELON, Rapport Final du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI)), par Gerhard SCHMID, FINAL, document de séance A5-0264/2001 Partie 1, du 11 juillet 2001, 210 p.

EPRS - European Parliament's Science and Technology Options Assessment (STOA) Panel, “An Appraisal of technologies of political control”, par M. Steve WRIGHT, Scientific and Technological Options Assessment, PE 166.499, Luxembourg, janvier 1998, 97 p.

EPRS – Service de recherche du Parlement européen, « L’affaire ECHELON - Les travaux du Parlement européen sur le système global d'interception, 1998 – 2002 », par MM. Franco PIODI et Iolanda MOMBELLI, Étude Série sur l'histoire du Parlement européen, PE 538.877, Direction générale des services de recherche parlementaire - Unité Archives historiques, Luxembourg, Office des Publications de l'Union européenne, Octobre 2014, 81 p.

EPRS - Working document for the STOA Panel, “Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition”, par M. Duncan CAMPBELL, Interception Capabilities 2000 – IC 2000 Report, PE 168.184/Vol 2/5, Directorate General for Research, Luxembourg, octobre 1999, 39 p.

EPRS - Working document for the STOA Panel, “Development of Surveillance Technology and Risk of Abuse of Economic Information - Appraisal of Technologies of Political Control (Vol. 1 to 5)”, par MM. Peggy BECKER et Dick HOLDSWORTH (dir. et éd.), Scientific and Technological Options Assessment, PE 168.184/Vol 1/5/EN, Directorate General for Research, Luxembourg, décembre 1999, 135 p.

European Commission, “Review of Recent Studies on PSI Re-Use and Related Market Developments”, Report for the European Commission in the context of the forthcoming review of the PSI Directive, par M. Graham VICKERY, du 16 septembre 2011, 44 p.

European Commission, Factsheet “High Performance Computing PPP: Mastering the next generation of computing technologies for innovative products and scientific discovery”, Digital Agenda for Europe, Bruxelles, 2013, 2 p.

European Commission, “Final Report: Data and information collection for EU dual-use export control policy review”, par SIPRI et Ecorys, du 6 novembre 2015, 247 p.

Proposition de Règlement du Parlement européen et du Conseil instituant un régime de l’Union de contrôle des exportations, des transferts, du courtage, de l’assistance technique et du transit en ce qui concerne les biens à double usage (refonte), COM/2016/0616 final - 2016/0295 (COD), Bruxelles le 28 septembre 2016, 50 p.

Proposition de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM/2017/010 final - 2017/03 (COD), Bruxelles, le 10 janvier 2017, 39 p.

Testimony to the European Parliament – The Civil Liberties, Justice and Home affairs (LIBE) Committee, par M. Edward SNOWDEN, May 2014, 12 p.

* Des agences, comités et institutions européennes

Comité Européen pour les problèmes criminels (CDPC) - Conseil de coopération pénologique (PC-CP), « La condamnation, la gestion et le traitement des délinquants “dangereux” », Rapport final rédigé par Nicola PADFIELD, n° PC-CP (2010) 10 rév 5, Conseil de l’Europe, Strasbourg, 20 décembre 2010, 44 p.

ETSI Guide, “Telecommunications Security; Trusted Third Parties (TTP); Requirements for TTP services”, EG 201 057 V1.1.2 (1997-07), Reference DEG/SEC-003000 (9sc00ide.PDF), European Telecommunications Standards Institute, 1997, 44 p.

ETSI Technical Report, “Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD)”, ETSI TR 101 567 V1.1.1 (2016-01), Reference: DTR/LI-00084, European Telecommunications Standards Institute, 2016, 103 p.

European Union Agency for Fundamental Rights, Fundamental Rights Report 2017, FRA, Luxembourg, Publications Office of the European Union, 2017, 241 p.

Recommandation CM/Rec(2010)13, du Comité des Ministres aux États membres sur la protection des personnes à l’égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée par le Comité des Ministres le 23 novembre 2010, Recommandation n° 1, 10 p.

Recommandation CM/Rec(2016)6, du Comité des Ministres aux États membres sur la recherche utilisant du matériel biologique d’origine humaine, adoptée par le Comité des Ministres le 11 mai 2016, 6 p.

* Du CEPD et Groupe de travail « Article 29 »

CEPD, Avis n° 7/2015 « Relever les défis des données massives : Un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes », du 19 novembre 2015, Bruxelles, EDPS, 26 p.

CEPD, « Protection des données par défaut ».

CEPD, « Protection des données dès la conception ».

EDPB, « *EDPB Rules of procedure* » adoptées le 25 mai 2018, 20 p.

EDPS, Speech on "Privacy by design - Privacy engineering" given at the 11th International Computers, Privacy and Data Protection Conference (CPDP), par Giovanni BUTTARELLI, EDPS side event, Bruxelles, du 25 janvier 2018, 3 p.

G29, Document de travail : Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne », n° 5063/00/FR WP 37, du 21 novembre 2000.

G29, Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, n° 11639/02/FR WP 74, adopté le 3 juin 2003, 22 p.

G29, Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification), n° 10107/05/FR WP 105, du 19 janvier 2005, 24 p.

G29, Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, n° 2093-01/05/FR WP 114, adopté le 25 novembre 2005, 20 p.

G29, Avis 4/2007 sur le concept de données à caractère personnel, n° 01248/07/FR WP 136, adopté le 20 juin 2007, 29 p.

G29, Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), n° 00350/09/FR WP 159, adopté le 10 février 2009, 12 p.

G29, Avis 5/2009 sur les réseaux sociaux en ligne, n° 01189/09/FR WP 163, adopté le 12 juin 2009, 14 p.

G29, Avis 15/2011 sur la définition du consentement, n° 01197/11/FR WP 187, adopté le 13 juillet 2011, 43 p.

G29, Opinion 03/2013 on purpose limitation, n° 00569/13/EN WP 203, adopté le 2 avril 2013, 70 p.

G29, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, n° 538/14/EN WP 212, adopté le 27 février 2014, 62 p.

G29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, n° 844/14/FR WP 217, adopté le 9 avril 2014, 78 p.

G29, "Statement on the role of a risk-based approach in data protection legal frameworks", n° 14/EN WP218, adopté le 30 mai 2014, 4 p.

G29, Lignes directrices relatives au droit à la portabilité des données, n° 16/FR WP 242 rev.01, adoptées le 13 décembre 2016 - Version révisée et adoptée le 5 avril 2017, 24 p.

G29, Lignes directrices concernant les délégués à la protection des données (DPD), Adoptées le 13 décembre 2016 - Version révisée et adoptée le 5 avril 2017, 16/FR WP 243 rev.01, 30 p.

G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé

» aux fins du règlement (UE) 2016/679, n° 17/FR WP 248 rév. 01, adoptées le 4 avril 2017 - modifiées et adoptées en dernier lieu le 4 octobre 2017, 27 p.

G29, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, n° 17/FR WP251 rév.01, adoptées le 3 octobre 2017 - Version révisée et adoptée le 6 février 2018, 43 p.

G29, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (mis à jour), n° 18/EN WP 256 rev. 01, adopté le 29 novembre 2017 - Version révisée et adoptée le 6 février 2018, 19 p.

G29, Lignes directrices sur le consentement au sens du règlement 2016/679, n° 17/FR WP259 rév.01, adoptées le 28 novembre 2017 - Version révisée et adoptée le 10 avril 2018, 36 p.

G29, Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, n° 17/EN WP264, adoptée le 11 avril 2018, 19 p.

* Des Nations-Unies

Assemblée générale des Nations-Unies, Rapport du Comité des Droits de l'Homme, Documents officiels de l'Assemblée générale, quarante-troisième session, Supplément n° 40 (A/43/40), du 28 septembre 1988, New-York, Nations-Unies, 1er novembre 1988 (trad.), 289 p.

Assemblée générale des Nations-Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. Frank La Rue, n° A/HRC/17/27, Conseil des droits de l'homme, dix-septième session, 16 mai 2011, 24 p.

Assemblée générale des Nations-Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. Frank La Rue, n° A/HRC/23/40, Conseil des droits de l'homme, vingt-troisième session, 17 avril 2013, 25 p.

Assemblée générale des Nations-Unies, Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, M.

Ben Emmerson, n° A/HRC/25/59/Add.1, Conseil des droits de l'homme, vingt-cinquième session, 4 février 2014, 19 p.

Assemblée générale des Nations-Unies, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, Le droit à la vie privée à l'ère du numérique, , n° A/HRC/27/37, Conseil des droits de l'homme, Vingt-septième session, 30 juin 2014, 18 p.

Assemblée générale des Nations-Unies, Rapport de synthèse sur la réunion-débat du Conseil des droits de l'homme sur le rôle de la prévention dans la promotion et la protection des droits de l'homme, Rapport du Haut-Commissariat des Nations Unis sur le rôle de la prévention dans la promotion et la protection des droits de l'homme, n° A/HRC/28/30, Conseil des droits de l'homme, vingt-huitième session, 10 décembre 2014, 18 p.

Assemblée générale des Nations-Unies, Résumé de la réunion-débat d'experts du Conseil des droits de l'homme sur l'utilisation d'aéronefs téléguidés ou de drones armés dans le respect du droit international, Rapport du Haut-Commissariat des Nations Unis, n° A/HRC/28/38, Conseil des droits de l'homme, vingt-huitième session, 15 décembre 2014, 18 p.

Assemblée générale des Nations-Unies, Résumé de la réunion-débat du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique, Rapport du Haut-Commissariat des Nations Unis sur la promotion et la protection du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles, n° A/HRC/28/39, Conseil des droits de l'homme, vingt-huitième session, 19 décembre 2014, 19 p.

Commission des droits de l'hommes, État des Pactes internationaux relatifs aux droits de l'homme – Note verbale du 24 août 1984, adressée au secrétaire général par le représentant permanent des Pays-Bas auprès de l'office des Nations Unies à Genève, Doc. E/CN.4/1985/4, Quarante et unième session, Conseil économique et social des Nations Unies, 28 septembre 1984, 14 p.

Commission des droits de l'homme, Promotion et protection du droit à la liberté d'opinion et d'expression, Rapport du Rapporteur spécial, M. Abid Hussain, établi en application de la

résolution 1993/45 de la Commission des droits de l'homme, Doc. E/CN.4/1995/32, Cinquante et unième session, Conseil économique et social des Nations Unis, 17 décembre 1994, 47 p.

Comité des Droits de l'Homme, Communication N° 488/1992, Toonen c. Australie, U.N. Doc CCPR/C/50/D/488/1992 (1994), UN Human Rights Committee (HRC), 4 avril 1994.

Comité des Droits de l'Homme, Communication N° 903/1999, Antonius Cornelis Van Hulst c. Pays-Bas, U.N. Doc. CCPR/C/82/D/903/1999 (2004), UN Human Rights Committee (HRC), 5 novembre 2004.

Comité des Droits de l'Homme, General Comment No. 27: Art. 12 (Freedom of Movement), U.N. Doc. CCPR/C/21/Rev.1/Add.9, UN Human Rights Committee (HCR), Sixty-seventh session, 2 novembre 1999.

Comité des Droits de l'Homme, Observation générale n° 16 : Art. 17 (Droit au respect de la vie privée), U.N. Doc. CCPR/C/21/Add.6 (1988), UN Human Rights Committee (HRC), Trente-deuxième session, 23 mars 1988.

Comité des Droits de l'Homme, Observation générale n° 27 : Liberté de circulation (art.12), U.N. Doc. CCPR/C/21/Rev.1/Add.9 (1999), UN Human Rights Committee (HRC), soixante-septième session, 18 octobre 1999.

Comité des Droits de l'Homme, Observation générale n° 29 : États d'urgence (art. 4), U.N. Doc. CCPR/C/21/Rev.1/Add.11 (2001), UN Human Rights Committee (HRC), 1950e session, 24 juillet 2001.

Comité des Droits de l'Homme, Observation générale n° 31 : La nature de l'obligation juridique générale imposée aux États parties au Pacte (Quatre-vingtième session, 2004), U.N. Doc. CCPR/C/21/Rev.1/Add.13, HRI/GEN/1/Rev.7 (2004) et HRI/GEN/1/Rev.9 (Vol. I), UN Human Rights Committee (HRC), 2187e session, 29 mars 2004.

Comité des Droits de l'Homme, Observation générale n° 34 : Liberté d'opinion et liberté d'expression (art. 19), U.N. Doc. CCPR/C/GC/34, UN Human Rights Committee (HRC), cent-deuxième session, 12 septembre 2011.

Résolution 7/36, Mandat du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Conseil des droits de l'homme, Quarante-deuxième séance, n° A/HRC/RES/7/36, 28 mars 2008, 5 p.

Resolution 56/183, World Summit on the Information Society, adoptée par l'Assemblée générale le 21 décembre 2001, Cinquante-sixième session, n° A/RES/56/183, Assemblée générale des Nations-Unies, 31 janvier 2002, 3 p.

Résolution 68/167, Le droit à la vie privée à l'ère du numérique, adoptée par l'Assemblée générale le 18 décembre 2013, Soixante-huitième session, n° A/RES/68/167, Assemblée générale des Nations-Unies, 21 janvier 2014, 3 p.

Résolution 69/166, Le droit à la vie privée à l'ère du numérique, adoptée par l'Assemblée générale le 18 décembre 2014, Soixante-neuvième session, n° A/RES/69/166, Assemblée générale des Nations-Unies, 10 février 2015, 4 p.

* De l'OCDE – OECD

OCDE, « Algorithmes et ententes - Note d'information du Secrétariat », n° DAF/COMP(2017)4, Direction des affaires financières et des entreprises, Comité de la concurrence, 16 juin 2017, 80 p.

OCDE, « Définition statistique de la biotechnologie », Direction de la science, de la technologie et de l'innovation, Les technologies émergentes, mise à jour en 2005.

OCDE, « Investissement dans les TIC (indicateur) », OCDE Données (2020), Direction de la science, de la technologie et de l'innovation, Les technologies émergentes, mis à jour en 2021.

OCDE, « Statistiques des biotechnologies : Méthodologie », F. 0, Direction de la science, de la technologie et de l'innovation, 2005-2006, 2 p.

OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, Annexe à la recommandation du Conseil du 23 septembre 1980, parties 1-5.

OCDE, Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel du 23 septembre 1980, n° OECD/LEGAL/0188, instruments juridiques de l'OCDE, amendée le 11 juillet 2013.

OECD, "Biotechnology Statistics – 2006", par Brigitte van Beuzekom et Anthony Arundel, OECD Publishing, 2006, 157 p.

OECD, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", n° DSTI/ICCP/IE/REG(2011)2/FINAL, OECD Digital Economy Papers, N° 220, OECD Publishing, Paris, 2 avril 2013, 39 p.

OECD, "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", n° DSTI/ICCP(2012)9/FINAL, OECD Digital Economy Papers, N° 222, OECD Publishing, Paris, 18 juin 2013, 43 p.

* Internationaux

Department of Homeland Security of the United States, "2017 National Network of Fusion Centers - Final Report", October 2018, 27 p.

Department of Homeland Security of the United States, "National Network of Fusion Centers Fact Sheet", April 2019.

Executive Office of the President, "Smart Disclosure and consumer decision-making: Report of the Task force on smart disclosure", National science and technology Council, The White House, Washington, Mai 2013, 41 p.

Executive Office of the President, White House Report "Big Data: Seizing opportunities, preserving Values", The White House, Washington, Mai 2014, 79 p.

Federal Trade Commission, “Privacy Online: Fair Information Practices in the Electronic Marketplace”, A Federal Trade Commission Report to Congress, FTC, Mai 2000, 56 p.

Federal Trade Commission, “Start with Security: A Guide for Business”, Lessons learned from FTC cases, FTC, Juin 2015, 14 p.

Federal Trade Commission, “Protecting Personal Information: A Guide for Business”, FTC, Octobre 2016, 32 p.

Federal Trade Commission, “The FTC’s Endorsement Guides: What People Are Asking”, FTC, Septembre 2017, 12 p.

ICCT Report “Fusion Centres in Six European Countries: Emergence, Roles and Challenges”, par MM. Renske VAN DER VEER, Walle BOS et Liesbeth VAN DER HEIDE, International Centre for Counter-Terrorism – The Hague, Février 2019, 27 p.

Memorandum of Understanding between Department of Defense and Department of Justice on “Operations other than War and Law enforcement”, signed by Janet Reno - Attorney General & John Deutch - Secretary of Defense, 20 avril 1994, 4 p.

Ministeriet for By, Bolig og Landdistrikter, « Re-use of public sector information – Catalogue and highlights of studies, cases and key figures on economic effects of changing policies », par M. Marc De Vries, Report for Danish Ministry for Housing, Urban and Rural Affairs, Copenhagen, The Hague 11 août 2012, 20 p.

Necessary and Proportionate Coalition, “Necessary & Proportionate - International principles on the application of Human Rights to Communications Surveillance”, Final version May 2014, 14 p.

NSA - William F. Friedman, Report on the Potentialities of COMINT as a Source of Warning of the Eminence of Hostilities, par Carolyn J. Fox, Ref ID A39176, PL 86-36/50 USC 3605, 28 août 1953, 6 p.

« Silent weapons for quiet wars - Armes silencieuses pour guerres tranquilles/sans bruit », An introductory programming manual, Operations Research, Technical Manual, TM-SW7905.1 – document de Mai 1979, n° #74-1120, 27 p.

Sommet Mondial Sur la Société de l'Information (SMSI), Genève 2003 – Tunis 2005, « Qu'est-ce que la révolution numérique ? », ONU – UIT, Résolution 56/183 de l'Assemblée générale des Nations-Unies, Genève du 10 au 12 décembre 2003, Tunis du 16 au 18 novembre 2005.

Statewatch bulletin, EU & FBI launch global telecommunications surveillance system: "not a significant document" - UK Home Secretary, January-February 1997, Vol. 7 n° 1, 24 p.

Statewatch Report, European Union and the FBI launch global surveillance system, 10 février 1997, 14 p.

U.S. Department of Justice's Office of Privacy and Civil Liberties (OPCL), "Overview of the Privacy Act of 1974", The United States Department of Justice, 2015 Edition, 317 p.

World Bank Group, 2017 World Development Indicators, International Bank for Reconstruction and Development, The World Bank, 2017, 124 p.

World Business Council for Sustainable Development, "Collaboration, innovation, transformation: Ideas and inspiration to accelerate sustainable growth - A value chain approach", WBCSD Consumption & Value chain, 1 Décembre 2011, 40 p.

V. Législations

* Codes

Code civil, Art. 16-5
Code civil, Art. 16-6
Code civil, Art. 16-10
Code civil, Art. 16-11
Code civil, Art. 16-14
Code civil, Art. 73

Code civil, Art. 96-1

Code de commerce, Art. L 151-1

Code de la consommation, Art. L. 121-2

Code de la défense, Art. L. 1111-1
Code de la défense, Art. D. 3126-1 et s.

Code de la sécurité intérieure, Art. L 228-3
Code de la sécurité intérieure, Art. L 229-1
Code de la sécurité intérieure, Art. L 229-5
Code de la sécurité intérieure, Art. L. 232-1 à L. 232-8
Code de la sécurité intérieure, Art. L 851-1 à L 851-6.
Code de la sécurité intérieure, Art. L 852-2
Code de la sécurité intérieure, Art. L 853-2
Code de la sécurité intérieure, Art. L 853-1
Code de la sécurité intérieure, Art. L 854-1 et L 854-2

Code de procédure pénale, Art. 48-1
Code de procédure pénale, Art. 706-53-13
Code de procédure pénale, Art. 706-73 et 706-73-1

Code pénal, Art. 410-1
Code pénal, Art. 413-9 à 413-12
Code Pénal, Art. 433-19
Code Pénal, Art. 434-23,
Code pénal, Art. 511-1 à 511-28

Constitution de 1958, Art. 2
Constitution de 1958, Art. 34
Constitution de 1791, Art. 6

Déclaration des droits de l'homme et du citoyen du 26 août 1789

Préambule de la Constitution du 27 octobre 1946

U.S. Constitution, Passed by Congress September 25, 1789 (Ratified December 15, 1791) - The first 10 amendments: The Bill of Rights.

* Lois françaises

Loi du 6 Fructidor An II (23 août 1794) portant qu'aucun citoyen ne pourra porter de nom ni de prénom autres que ceux exprimés dans son acte de naissance, loi N° 240, Bulletin des lois de la République française de 1794, p. 5.

Loi 1810-02-19 promulguée le 1er mars 1810, modifiée par Loi n°70-480 du 8 juin 1970 tendant à réprimer certaines formes nouvelles de délinquance (1) - art. 5, JORF du 9 juin 1970, Abrogée par Loi n°81-82 du 2 février 1981 renforçant la sécurité et protégeant la liberté des personnes (1) - art. 25, JORF n° 0028 du 3 février 1981.

Loi n° 54-439 du 15 avril 1954 sur le traitement des alcooliques dangereux pour autrui, JORF n° 0092 du 21 avril 1954, p. 3827-3829.

Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence, JORF n° 0085 du 7 avril 1955, p. 3477-3479.

Loi n° 56-1327 du 29 décembre 1956 de finances pour 1957, JORF n°0304 du 30 décembre 1956, p. 12638-12671.

Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, JORF n° 0166 du 19 juillet 1970, p. 6751-6761.

Loi n° 77-1468 du 30 décembre 1977 instaurant la gratuité des actes de justice devant les juridictions civiles et administratives, JORF n° 0303 du 31 décembre 1977, p. 6359-6360.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 0006 du 07 janvier 1978, p. 227-231.

Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, JORF n° 0166 du 18 juillet 1978, p. 2851-2857.

Loi n° 81-82 du 2 février 1981 renforçant la sécurité et protégeant la liberté des personnes, JORF n° 0028 du 03 février 1981, p. 415-425.

Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions de nature sexuelle ainsi qu'à la protection des mineurs, JORF n° 0139 du 18 juin 1998, p. 9255-9263.

Loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999, JORF n° 300 du 27 décembre 1998, p. 19646-19663.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n° 0143 du 22 juin 2004, Texte n° 2 sur 108.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 182 du 7 août 2007, Texte n° 2 sur 92.

Loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales, JORF n° 289 du 13 décembre 2005, Texte n° 1 sur 113.

Loi n° 2006-1666 du 21 décembre de Finances pour 2007, JORF n° 299 du 27 décembre 2006, Texte n° 1 sur 108.

Loi n° 2008-174 du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, JORF n° 0048 du 26 février 2008, Texte n° 1 sur 150.

Loi constitutionnelle n° 2008-724 du 23 juillet 2008 de modernisation des institutions de la V^{e} République, JORF n° 0171 du 24 juillet 2008, Texte n° 2 sur 149.

Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n° 0135 du 13 juin 2009, Texte n° 2 sur 148.

Loi n° 2009-928 du 29 juillet 2009 relative à la programmation militaire pour les années 2009 à 2014 et portant diverses dispositions concernant la défense, JORF n° 0175 du 31 juillet 2009, Texte n° 1 sur 114.

Loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale, JORF n° 0059 du 11 mars 2010, Texte n° 2 sur 133.

Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n° 0062 du 15 mars 2011, Texte n° 2 sur 127.

Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, JORF n°0075 du 28 mars 2012, Texte n° 2 sur 102.

Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n° 0294 du 19 décembre 2013, Texte n° 1 sur 163.

Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF n° 0171 du 26 juillet 2015, Texte n° 2 sur 49.

Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, JORF n° 0278 du 1er décembre 2015, Texte n° 1 sue 113.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016, Texte n° 1 sur 96.

Loi n° 2017-257 du 28 février 2017 relative au statut de Paris et à l'aménagement métropolitain, JORF n° 0051 du 1er mars 2017, Texte n° 2 sur 137.

Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, JORF n° 0255 du 31 octobre 2017, Texte n° 1 sur 130.

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF n°0141 du 21 juin 2018, Texte n° 1 sur 111.

Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, JORF n° 0161 du 14 juillet 2018, Texte n° 1 sur 160.

Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, JORF n° 0174 du 31 juillet 2018, Texte n° 1 sur 138.

Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, JORF n° 0071 du 24 mars 2019, Texte n° 2 sur 65.

Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement (1), JORF n°0176 du 31 juillet 2021, Texte n° 1 sur 149.

* Lois européennes et internationales

Loi fondamentale pour la République fédérale d'Allemagne du 23 mai 1949, Journal officiel fédéral, p. 1, BGBI. III 100-1.

The Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. 1681 et *sq*. and 16 CFR 1.73., public law 91-508, 91st United States Congress, October 26, 1970.

Loi du 11 mai 1973 sur la protection des données (Datalagen), entrée en vigueur le 1er juillet 1974, abrogée et remplacée le 24 octobre 1998 par la loi sur les données personnelles (Personuppgiftslagen), Suède.

The Privacy Act of 1974, 5 U.S.C. § 552a (2012), public law 93-579, U.S. Department of Justice, Office of Privacy and Civil Liberties December 31, 1974.

Loi fédérale du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement de données, modifiée par la loi fédérale de protection des données du 20 décembre 1990 et amendée par la loi du 14 septembre 1994, République fédérale d'Allemagne.

Loi n° 293 du 8 juin 1978 sur les registres privés et loi n° 294 du 8 juin 1978 sur les registres des pouvoirs publics, amendées en 1988 et en 1991, Danemark.

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510, public law 99-508, 99th United States Congress, October 21, 1986.

Loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant la police, Finlande.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), public law 104–191, 104th United States Congress, august 21, 1996.

Communications Decency Act of 1996, 47 U.S.C. §230, public law 104-104, 104th United States Congress, February 8, 1996 (declared unconstitutional by the US Supreme Court in 1997).

Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. 6501–6505, FTC, public law 105-277, 105th United States Congress, April 21, 2000.

Décret n° 14 sur les fichiers de renseignements personnels inconsultables (SCRS), Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21), DORS/92-688, C.P. 1992-2412, 26 novembre 1992, Canada.

Identity Documents Act, *Riigikogu*, Passed 15.02.1999, RT I 1999, 25, 365, Entry into force January 1, 2000, Estonia.

The USA Patriot Act - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism - of 2001, Public Law 107-56, 107th United States Congress, October 26, 2001.

The Austrian E-Government Act – Federal Act on Provisions Facilitating Electronic Communications with Public Bodies, entered into force on 1 March 2004, Austrian Federal Law Gazette (BGBl), part I, N° 10/2004.

* Arrêtés, circulaires, décrets et ordonnances français

Arrêté du 19 juillet 2006 portant homologation de la norme d'exercice professionnel relative aux principes applicables à l'audit des comptes mis en œuvre dans le cadre de la certification des comptes, JORF n°176 du 1er août 2006, texte n° 12 sur 151.

Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité, JORF n°0095 du 22 avril 2016, texte n° 1 sur 200.

Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », JORF n°0180 du 6 août 2015, texte n° 4 sur 94.

Circulaire de la DACG n° Crim 08-01/G1 du 3 janvier 2008 relative au secret de la Défense nationale, Bulletin Officiel du Ministère de la Justice n° 2008/1 du 29 février 2008, texte n° 13 sur 22 (NOR : JUSD0800121C).

Circulaire du 28 juillet 2011 relative à la présentation des dispositions de droit pénal général et de procédure pénale générale de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, Bulletin Officiel du Ministère de la Justice et des libertés n° 2011-08 du 31 août 2011 (NOR : JUSD1121169C).

Décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité, JORF n° 0254 du 27 octobre 1955, p. 10604.

Décret n° 77-127 du 11 février 1977 instituant une Commission chargée de favoriser la communication au public des documents administratifs, JORF n° 0036 du 12 février 1977, p. 859.

Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'intérieur, JORF n° 0084 du 09 avril 1987, p. 4046.

Décret n°2005-1726 du 30 décembre 2005 relatif aux passeports, JORF n° 304 du 31 décembre 2005, texte n° 15 sur 230.

Décret n° 2007-240 du 22 février 2007 portant création de l'Agence nationale des titres sécurisés, JORF n° 0047 du 24 février 2007, texte n° 8 sur 123.

Décret n° 2009-1118 du 17 septembre 2009 relatif au contrôle gouvernemental de la dissuasion nucléaire, JORF n° 0216 du 18 septembre 2009, texte n° 1 sur 106.

Décret du 2 décembre 2011 modifiant le décret n° 2007-255 du 27 février 2007 fixant la liste des titres sécurisés relevant de l'Agence nationale des titres sécurisés, JORF n°0280 du 3 décembre 2011, texte n° 26 sur 137.

Décret n° 2014-474 du 12 mai 2014 pris pour l'application de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires et portant désignation des services spécialisés de renseignement, JORF n°0111 du 14 mai 2014, texte n° 1 sur 95.

Décret n° 2014-1050 du 16 septembre 2014 instituant un administrateur général des données, JORF n° 0215 du 17 septembre 2014, texte n° 2 sur 83.

Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, JORF n° 0225 du 29 septembre 2015, texte n° 1 sur 97.

Décret n° 2017-1095 du 14 juin 2017 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme, JORF n° 0139 du 15 juin 2017, texte n° 1 sur 168.

Décret n° 2018-714 du 3 août 2018 relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire), JORF n° 0181 du 8 août 2018, texte n° 2 sur 142.

Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n° 0125 du 30 mai 2019, texte n° 16 sur 209.

Ordonnance n° 58-1298 du 23 décembre 1958 modifiant notamment certains articles du code pénal, JORF n° 0300 du 24 décembre 1958, p. 11761.

Ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense, JORF n° 0008 du 10 janvier 1959, p. 691.

Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, JORF n° 0197 du 26 août 2011, texte n° 49 sur 134.

Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF n° 0288 du 13 décembre 2018, texte n° 5 sur 146.

Ordonnance n° 2019-1015 du 2 octobre 2019 réformant la régulation des jeux d'argent et de hasard, JORF n° 0230 du 3 octobre 2019, texte n° 18 sur 129.

Ordonnance n° 2020-1733 du 16 décembre 2020 portant partie législative du code de l'entrée et du séjour des étrangers et du droit d'asile, JORF n°0315 du 30 décembre 2020, texte n° 41 sur 135.

* Directives et règlements européens

Décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (2002/475/JAI), JOUE n° L 164 du 22 juin 2002, p. 3-7, date de fin de validité : 19/04/2017, abrogé et remplacé par la Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme.

Décision n° 922/2009/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant des solutions d'interopérabilité pour les administrations publiques européennes (ISA), JOUE n° L 260 du 03 octobre 2009, p. 20-27, date de fin de validité : 31/12/2015.

Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs, JOUE n° L 95 du 21 avril 1993, p. 29-34.

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOUE n° L 281 du 23 novembre1995, p. 31-50, date de fin de validité : 24/05/2018.

Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999, portant sur un cadre communautaire pour les signatures électroniques, JOUE n° L 13 du 19 janvier 2000, p. 12-20, date de vin de validité : 30/06/2016.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JOUE n° L 201 du 31 juillet 2002, p. 37-47.

Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, JOUE n° L 345 du 31 décembre 2003, p. 90-96.

Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (dite directive API), JOUE n° L 261 du 06 août 2004, p. 24-27.

Directive européenne 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (Data Retention Directive), JOUE n° L 105 du 13 avril 2006, p. 54-63, date de fin de validité : 03/05/2006.

Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques, JOUE n° L 337 du 18 décembre 2009, p. 37-69.

Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, JOUE n° L 175 du 27 juin 2013, p. 1-8, date de fin de validité : 16/07/2021.

Directive UE 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JOUE n° L 119 du 04 mars 2016, p. 89-131.

Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, JOUE n° L 119 du 04 mars 2016, p. 132-149.

Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, JOUE n° L 88 du 31 mars 2017, p. 6-21.

Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, JOUE n° L 385 du 29 décembre 2004, p. 1-6.

Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JOUE n° L 381 du 28 décembre 2006, p. 4-23.

Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, JOUE n° L 218 du 13 août 2008, p. 30-47.

Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, (règlement eIDAS), JOUE n° L 257 du 28 août 2014, p. 73-114.

Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union, JOUE n° L 310 du 26 novembre 2015, p. 1-18.

Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données – RGPD), JOUE n° L 119 du 4 mars 2016, p. 1-88.

Règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), modifiant le règlement (CE) n° 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) n° 1077/2011, JOUE n° L 295 du 21 novembre 2018, p. 99-37.

Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006, JOUE n° L 312 du 7 décembre 2018, p. 14-55.

Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte), JOUE n° L 206 du 11 juin 2021, p. 1-461.

Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, Journal officiel n° C 329 du 04 novembre 1996 (96/C 329/01), p. 01-06.

Résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union (2013/2682(RSP)), P7_TA(2013)0322, Journal officiel n° C 75 du 26 février 2016 (2016/C 075/14), p. 105-108.

* Accords, conventions & pactes européens et internationaux

Accord Canada-États-Unis-Mexique (ACEUM), entré en vigueur le 1er janvier 1994, signé le 30 novembre 2018, remplacé par le nouvel Accord Canada-États-Unis-Mexique (ACEUM), entré en vigueur le 1er juillet 2020.

Accord économique et commercial global entre le Canada et l'Union européenne (AECG), ou Comprehensive Economic and Trade Agreement (CETA) signé le 30 octobre 2016 entrée en vigueur le 21 septembre 2017.

Accord de libre-échange Nord-américain (ALENA) ou North American Free Trade Agreement (NAFTA), du 1er janvier 1994, remplacé par Accord Canada-États-Unis-Mexique (ACEUM).

American Convention on Human Rights : "Pact of San José, Costa Rica", n° 17955, Adopted at the Inter-American Specialized Conference on Human Rights, San José, Costa Rica, 22 November 1969, UNTS Vol. n° 1144 (p. 123), Registered by the Organization of American States on 27 August 1979.

Charte des droits fondamentaux de l'Union Européenne, du 7 décembre 2000 (2000/C 364/01), JO n° C 364 du 18 décembre 2000, p. 1-22.

Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (Convention Européenne des droits de l'Homme), Telle qu'amendée par les Protocoles nos 11 et 14, complétée par le Protocole additionnel et les Protocoles nos 4, 6, 7, 12, 13 et 16, du 4 novembre 1950, Cour européenne des droits de l'homme, Conseil de l'Europe, STCE n° 005, p. 5-62.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (Convention 108), Conseil de l'Europe, STE n° 108, Strasbourg, 28 janvier 1981, p. 1-9.

Convention internationale des droits de l'enfant (CIDE) - Convention relative aux droits de l'enfant, adoptée et ouverte à la signature, ratification et adhésion par l'Assemblée générale des Nations-Unies dans sa résolution 44/25 du 20 novembre 1989, Entrée en vigueur le 2 septembre 1990, conformément à l'article 49 (ratifiée par 196 États).

Déclaration universelle des droits de l'homme du 10 décembre 1948, adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948 à Paris, palais de Chaillot, par la résolution 217 (III) A, JORF n° 0044 du 19 février 1949, p. 1859.

Interregional Framework Cooperation Agreement between the European Community and Mercosur (The EU-Mercosur), entered into force on 1 July 1999, JOUE n° L 175, 10 july 1999, p. 62.

Pacte international relatif aux droits civils et politiques, Adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale dans sa résolution 2200 A (XXI) du 16 décembre 1966 – Entrée en vigueur le 23 mars 1976, conformément aux dispositions de l'article 49, ONU.

Privacy Shield EU-US (EU-U.S. Privacy shield framework principles issued by the U.S. Department of commerce), ou Bouclier de protection des données UE-US entrée en vigueur le 1er août 2016, à la suite de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis [notifiée sous le numéro C(2016) 4176], JOUE n° L 207 du 1er août 2016, p. 1-112, date de fin de validité : 12/07/2016.

Traité sur le fonctionnement de l'Union Européenne, Versions consolidées du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne - Journal officiel n° C 326 du 26 octobre 2012, p. 0001 – 0390.

VI. Jurisprudences

* Du Conseil constitutionnel français

Conseil Constitutionnel, Décision n° 80-127 DC du 20 janvier 1981, Loi renforçant la sécurité et protégeant la liberté des personnes, JORF du 22 janvier 1981, p. 308.

Conseil Constitutionnel, Décision n° 94-352 DC du 18 janvier 1995, Loi d'orientation et de programmation relative à la sécurité, JORF n° 18 du 21 janvier 1995, p. 1154.

Conseil constitutionnel, Décision n° 99-416 DC du 23 juillet 1999, Loi portant création d'une couverture maladie universelle, JORF n° 172 du 28 juillet 1999, p. 11250.

Conseil Constitutionnel, Décision n° 99-419 DC du 9 novembre 1999, Loi relative au pacte civil de solidarité, JORF n° 265 du 16 novembre 1999, p. 16962.

Conseil Constitutionnel, Décision n° 2004-492 DC du 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité, JORF n° 59 du 10 mars 2004, p. 4637.

Conseil Constitutionnel, Décision n° 2007-557 DC du 15 novembre 2007, Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile, JORF n° 270 du 21 novembre 2007, p. 19001.

Conseil Constitutionnel, Décision n° 2008-562 DC du 21 février 2008, Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, JORF n° 0048 du 26 février 2008, p. 3272.

Conseil Constitutionnel, Décision n° 2009-580 DC du 10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet, JORF n° 0135 du 13 juin 2009, p. 9675.

Conseil Constitutionnel, Décision n° 2010-25 QPC du 16 septembre 2010, M. Jean-Victor C. [Fichier empreintes génétiques], JORF n° 0216 du 17 septembre 2010, p. 16847.

Conseil Constitutionnel, Décision n° 2010-613 DC du 7 octobre 2010, Loi interdisant la dissimulation du visage dans l'espace public, JORF n° 0237 du 12 octobre 2010, p. 18345.

Conseil Constitutionnel, Décision n° 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité, JORF n° 0075 du 28 mars 2012, p. 5607.

Conseil Constitutionnel, Décision n° 2013-675 DC du 9 octobre 2013, Loi organique relative à la transparence de la vie publique, JORF n° 0238 du 12 octobre 2013, p. 16838.

Conseil Constitutionnel, Décision n° 2013-357 QPC du 29 novembre 2013, Société Wesgate Charters Ltd [Visite des navires par les agents des douanes], JORF n° 0279 du 1er décembre 2013, p. 19603.

Conseil Constitutionnel, Décision n° 2013-684 DC du 29 décembre 2013, Loi de finances rectificative pour 2013, JORF n° 0303 du 30 décembre 2013, p. 22232.

Conseil Constitutionnel, Décision n° 2013-685 DC du 29 décembre 2013, Loi de finances pour 2014, JORF n° 0303 du 30 décembre 2013, p. 22188.

Conseil Constitutionnel, Décision n° 2014-420/421 QPC du 9 octobre 2014, M. Maurice L. et autre [Prolongation exceptionnelle de la garde à vue pour des faits d'escroquerie en bande organisée], JORF n° 0237 du 12 octobre 2014, p. 16578.

* Du Conseil d'État français

Conseil d'État, Assemblée, Décision n° 317827 du 26 octobre 2011, Association pour la promotion de l'image, Recueil Lebon, p. 505.

Conseil d'État, 10ème - 9ème chambres réunies, Décision n° 399922 du 19 juillet 2017, Google Inc., Mentionnée dans les tables du recueil Lebon.

* De la Cour de cassation française

Cour de Cassation (1ère ch. civ.), arrêt du 23 octobre 1990, pourvoi N° 89-13.163, Bulletin 1990 I, n° 222, p. 158.

Cour de Cassation (Ass. plén.), arrêt du 11 décembre 1992, pourvoi n° 91-11.900, Bulletin 1992, A.P. n° 13, p. 27.

Cour de Cassation (Ass. plén.), arrêt du 11 décembre 1992, pourvoi n° 91-12.373, Arrêt N°2 – Moyen annexé produit par la SCP Masse-Dessen, Georges et Thouvenin (avocats aux Conseils), Bulletin 1992, A.P. n° 13, p. 27.

Cour de Cassation (Ch. crim.), arrêt du 21 janvier 2009, pourvoi n° 08-83.492, Bulletin criminel 2009, n° 24.

Cour de Cassation (Ass. plén.), arrêt n° 589 du 15 avril 2011, pourvoi n° 10-17.049, Bulletin criminel 2011, A.P. n° 1.

Cour de Cassation (Ch. crim.), arrêt du 28 mars 2018, pourvoi n° 17-86.938, Bulletin criminel 2018, n° 827.

* De la Cour européenne des droits de l'homme

CEDH, Cour (Plénière), Affaire Engel et autres c. Pays-Bas du 8 juin 1976, requêtes n^{os} 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, série A n° 22.

CEDH, Cour (Plénière), Affaire Handyside c. Royaume-Uni du 7 décembre 1976, requête n° 5493/72, série A n° 24.

CEDH, Cour (Plénière), Affaire Irlande c. Royaume-Uni du 18 janvier 1978, requête n° 5310/71, série A n° 25.

CEDH, Cour (Plénière), Affaire Klass et autres c. Allemagne du 6 septembre 1978, requête n° 5029/71, série A n° 28.

CEDH, Cour (Chambre), Affaire Airey c. Irlande du 9 octobre 1979, requête n° 6289/73, série A n° 32.

CEDH, Commission (plénière), Affaire McFeeley et al. c. Royaume-Uni, décision de la Commission du 15 mai 1980 sur la recevabilité de la requête, requête n° 8317/78, DR 20, p. 44.

CEDH, Cour (Plénière), Affaire Dudgeon c. Royaume-Uni du 22 octobre 1981, requête n° 7525/76, série A n° 45.

CEDH, Cour (Plénière), Affaire Malone c. Royaume-Uni du 2 août 1984, requête n° 8691/79, série A n° 82.

CEDH Cour (Chambre), Affaire X et Y c. Pays-Bas du 26 mars 1985, requête n° 8978/80, série A no° 91.

CEDH, Cour (Chambre), Leander c. Suède du 26 mars 1987, requête n° 9248/81, série A n° 116.

CEDH, Cour (Plénière), Affaire Gaskin c. Royaume-Uni du 7 juillet 1989, requête n° 10454/83, série A n° 160.

CEDH, Cour (Plénière), Affaire Soering c. Royaume-Uni du 7 juillet 1989, requête n° 14038/88, série A n° 161.

CEDH, Cour (Plénière), Affaire B. c. France du 25 mars 1992, requête n° 13343/87, série A n° 232-C.

CEDH, Cour (Chambre), Affaire Niemietz c. Allemagne du 16 décembre 1992, requête n° 13710/88, série A n° 251-B.

CEDH, Cour (Chambre), Affaire Costello-Roberts c. Royaume-Uni du 25 mars 1993, requête n° 13134/87, série A n° 247-C.

CEDH, Cour (Chambre), Affaire Burghartz c. Suisse du 22 février 1994, requête n° 16213/90, série A n° 280-B.

CEDH, Cour (Chambre), Affaire Friedl c. Autriche du 31 janvier 1995, requête n° 15225/89, série A n° 305-B.

CEDH, Comité des ministres, Affaire Friedl c. Autriche, avis de la Commission du 04 mai 1995, requête n° 15225/89, résolution n° DH (95) 35, Res-54.

CEDH, Cour (Chambre), Affaire Buckley c. Royaume-Uni du 25 septembre 1996, requête n° 20348/92, Recueil 1996-IV.

CEDH, Cour (Chambre), Affaire Laskey, Jaggard et Brown c. Royaume-Uni du 19 février 1997, requête N° 21627/93, 21826/93 et 21974/93, Recueil 1997-I.

CEDH, Cour (Chambre), Affaire Z. c. Finlande du 25 février 1997, requête n° 22009/93, Recueil 1997-I.

CEDH, Cour (Chambre), Affaire Halford c. Royaume-Uni du 25 juin 1997, requête n° 20605/92, Recueil 1997-III.

CEDH, Cour (Chambre), Affaire Kopp c. Suisse, du 25 mars 1998, requête n° 23224/94, Recueil 1998-II.

CEDH, Cour (Grande Chambre), Affaire Amann c. Suisse du 16 février 2000, requête n° 27798/95, Recueil des arrêts et décisions 2000-II.

CEDH, Cour (3ème section), Affaire Bensaid c. Royaume-Uni du 6 février 2001, requête n° 44599/98, Recueil des arrêts et décisions 2001-I.

CEDH, Cour (1ère Section), Affaire Mikulić c. Croatie du 7 février 2002, requête n° 53176/99, Recueil des arrêts et décisions 2002-I.

CEDH, Cour (4ème Section), Affaire Pretty c. Royaume-Uni du 29 avril 2002, requête n° 2346/02, Recueil des arrêts et décisions 2002-III.

CEDH, Cour (Grande Chambre), Affaire Christine Goodwin c. Royaume-Uni du 11 juillet 2002, requête n° 28957/95, Recueil des arrêts et décisions 2002-VI.

CEDH, Cour (2ème section), Affaire M.M. c. Pays bas du 8 avril 2003, requête n° 39339/98, non publié.

CEDH, Cour (Grande Chambre), Affaire Hatton et autres c. Royaume-Uni du 8 juillet 2003, requête n° 36022/97, Recueil des arrêts et décisions 2003-VIII.

CEDH, Cour (3ème section), Affaire Weber et Saravia c. Allemagne du 29 juin 2006, requête n° 54934/00, Recueil des arrêts et décisions 2006-XI.

CEDH, Cour (3ème section), Affaire Jäggi c. Suisse du 13 juillet 2006, requête n° 58757/00, Recueil des arrêts et décisions 2006-X.

CEDH, Cour (Grande Chambre), Affaire S. et Marper c. Royaume-Uni du 4 décembre 2008, requêtes nos 30562/04 et 30566/04, Recueil des arrêts et décisions 2008.

CEDH, Cour (3ème section), Affaire Toma c. Roumanie du 24 février 2009, requête n° 42716/02, non publié.

CEDH, (Grande Chambre), Affaire Bykov c. Russie du 10 mars 2009, requête n° 4378/02, non publié.

CEDH, Cour (5ème section), Affaire M. *c*. Allemagne du 17 décembre 2009, requête n° 19359/04, Recueil des arrêts et décisions 2009.

CEDH, Cour (5ème section), Affaire Uzun c. Allemagne du 02 septembre 2010, requête n° 35623/05, Recueil des arrêts et décisions 2010 (extraits).

CEDH, (4ème section), Affaire Nurzyński c. Pologne du 21 décembre 2010, requête n° 46859/06, non publié.

CEDH, Cour (1ère section), Affaire Shimovolos c. Russie du 21 juin 2011, requête n° 30194/09, non publié.

CEDH, Cour (4ème section), Affaire Piechowicz c. Pologne du 17 avril 2012, requête n° 20071/07, non publié.

CEDH, Cour (Grande Chambre), Affaire Söderman c. Suède du 12 novembre 2013, requête n° 5786/08, Recueil des arrêts et décisions 2013.

CEDH, Cour (Grande Chambre), Affaire S.A.S. c. France du 1er juillet 2014, requête n° 43835/11, Recueil des arrêts et décisions 2014.

CEDH, Cour (3ème section), Affaire Tanda-Muzinga c. France du 10 juillet 2014, requête n° 2260/10, non publié.

CEDH, (Grande Chambre), Affaire Parrillo c. Italie du 27 août 2015, requête n° 46470/11, Recueil des arrêts et décisions 2015.

CEDH, Cour (3ème section), Affaire Vukota-Bojić c. Suisse du 18 octobre 2016, requête n° 61838/10, non publié.

CEDH, (Grande Chambre), Affaire Paradiso et Campanelli c. Italie du 24 janvier 2017, requête n° 25358/12, Recueil des arrêts et décisions 2017.

CEDH, Cour (4ème section), Affaire M. S. c. Ukraine du 11 juillet 2017, requête n° 2091/13, non publié.

CEDH (2ème section), Affaire Egill Einarsson c. Iceland du 7 novembre 2017, requête n° 24703/15, non publié.

CEDH, Cour (Grande Chambre), Affaire Ilnseher c. Allemagne du 4 décembre 2018, requêtes nos 10211/12 et 27505/14, non publié.

* De la Cour de justice des Communautés européennes – Cour de justice de l'Union européenne

CJCE, Arrêt Hoechst AG c. Commission des Communautés européennes, du 21 septembre 1989, Affaires jointes 46/87 et 227/88, Recueil de jurisprudence 1989, p. 02859.

CJCE, Arrêt Bernard Connolly c. Commission des Communautés européennes, du 6 mars 2001, Affaire C-274/99, Recueil de jurisprudence 2001, p. I-01611.

CJCE, Arrêt Rechnungshof c. Österreichischer Rundfunk et autres et Christa Neukomm et Joseph Lauermann c. Österreichischer Rundfunk, du 20 mai 2003, Affaires jointes C-465/00, C-138/01 et C-139/01, Recueil de jurisprudence 2003, p. I-04989.

CJCE, Arrêt Eugen Schmidberger, Internationale Transporte und Planzüge c. Republik Österreich (dit arrêt Schmidberger), du 12 juin 2003, Affaire C-112/00, Recueil de jurisprudence 2003, p. I-05659.

CJCE, Arrêt Procédure pénale contre Bodil Lindqvist (dit arrêt Lindqvist), du 6 novembre 2003, Affaire C-101/01, Recueil des arrêts et décisions 2003, p. I-12971.

CJCE, Arrêt Omega Spielhallen- und Automatenaufstellungs-GmbH c. Oberbürgermeisterin der Bundesstadt Bonn (dit arrêt Omega), du 14 octobre 2004, Affaire C-36/02, Recueil de jurisprudence 2004, p. I-09609.

CJCE, Arrêt International Transport Workers' Federation, Finnish Seamen's Union/Viking Line ABP, ou Viking Line Eesti (dit arrêt Viking), du 11 décembre 2007, Affaire C-438/05, JOUE n° C 51 du 23 février 2008, p. 11.

CJUE (Grande chambre), Arrêt eDate Advertising c. X et Olivier Martinez et Robert Martinez c. MGN Limited, du 25 octobre 2011, Affaires jointes C-509/09 et C-161/10, Recueil de jurisprudence 2011, p. I-10269.

CJUE (Grande chambre), Arrêt Prokurator Generalny c. Łukasz Marcin Bonda, Demande de décision préjudicielle, introduite par Sąd Najwyższy, du 5 juin 2012, Affaire C-489/10, Recueil numérique (Recueil général).

CJUE (Grande chambre), Arrêt Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a. (dit arrêt Digital Rights Ireland), du 8 avril 2014, Affaires jointes C-293/12 et C-594/12, Recueil numérique (Recueil général).

CJUE (Grande chambre), Arrêt Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, du 13 mai 2014, Affaire C-131/12, JOUE n° C 212 du 7 juillet 2014, p. 4.

CJUE (Grande chambre), Arrêt Maximillian Schrems c. Data Protection Commissioner, en présence de Digital Rights Ireland Ltd, du 6 octobre 2015, Affaire C-362/14, JOUE n° C 398 du 30 novembre 2015, p. 5.

CJUE (Grande chambre), Arrêt Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson et autres, du 21 décembre 2016, Affaires jointes C-203/15 et C-698/15, Recueil numérique (Recueil général).

CJUE, Avis de la Cour (Grande chambre), Avis rendu en vertu de l'article 218, paragraphe 11, TFUE – Projet d'accord entre le Canada et l'Union européenne – Transfert des données des dossiers passagers aériens depuis l'Union vers le Canada, Avis 1/15 du 26 juillet 2017, Recueil numérique (Recueil général), 56 p.

CJUE, Avis de la Cour (Grande chambre) du 26 juillet 2017 — Parlement européen, Avis 1/15, JOUE n° C 309 du 18 septembre 2017, p. 3.

CJUE (Grande chambre), Arrêt Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems, du 16 juillet 2020, Affaire C-311/18 (Arrêt Schrems II), JOUE n° C 559, Recueil de jurisprudence 2020, p. 1-51.

* Internationales

U.S. Supreme Court, Katz *v.* United States, 389 U.S. 347 (1967), case n° 35, decided December 18, 1967.

Cour Constitutionnelle fédérale de l'Allemagne, arrêt du 13 décembre 1983 relatif à la loi de Recensement : BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats Vom 15 Dezember 1983 auf die mündliche Verhandlung Vom 18 und 19 Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden.

U.S. Supreme Court, Ruckelshaus *v.* Monsanto Co., 467 U.S. 986 (1984), case No. 83-196, decided June 26, 1984.

U.S. Supreme Court, Reno, Attorney General of the United States et al. *v.* American Civil Liberties Union et al., 521 U.S. 844 (1997), case No. 96-511, decided June 26, 1997.

Cour Interaméricaine des Droits de l'Homme, Affaire Escher et autres c. Brésil, Exceptions préliminaires, Fond, réparations et dépens, arrêt du 6 juillet 2009, case n° 12.353, série C n° 200.

Cour Interaméricaine des Droits de l'Homme, Affaire Escher et autres c. Brésil, Interprétation, du 20 novembre 2009, case n° 12.353, série C n° 208.

U.S. Court of Appeal – For the District of Columbia Circuit, Electronic Privacy Information Center (EPIC) *v.* National Security Agency, USCA Case No. 11-5233, decided May 11, 2012, (EPIC v. NSA 798 F. Supp. 2d 26 (D.D.C. July 8, 2011)), 12 p.

VII. Ressources numériques

* Ressources médiatiques et numériques

Académie du Renseignement, « La communauté française du renseignement » : http://www.academie-renseignement.gouv.fr/communaute.html

Académie du Renseignement, « La coordination nationale du renseignement et de la lutte contre le terrorisme » : http://www.academie-renseignement.gouv.fr/coordination.html

AFNOR Éditions, NF Z74-501, Avis en ligne de consommateurs - Principes et exigences portant sur les processus de collecte, modération et restitution des avis en ligne de consommateurs, Juillet 2013 – Annulée le 22/09/2018 : https://www.boutique.afnor.org/norme/nf-z74-501/avis-en-ligne-de-consommateurs-principes-et-exigences-portant-sur-les-processus-de-collecte-moderation-et-restitution-des-avi/article/808897/fa178349

Agence du numérique en santé, « Interopérabilité, Pierre angulaire de la croissance en e-santé », Ministère des solidarités et de la santé, AsipSanté, 2019 : https://esante.gouv.fr/interoperabilite

ANDERSON [C.], "The end of theory: The Data deluge makes the scientific method obsolete", Wired, June 23, 2008: https://www.wired.com/2008/06/pb-theory/

ASHFORD [W.], « Les députés européens appellent à suspendre le Privacy Shield », LeMagIT, du 6 juillet 2018 : https://www.lemagit.fr/actualites/252444356/Les-deputes-europeens-appellent-a-suspendre-le-Privacy-Shield

Association ProECA, Article (1/2) « L'organisation des services de renseignement français », Master 2 Pro ECA, 18 mai 2017 : https://proeca-pantheon-sorbonne.com/2017/05/18/article-lorganisation-des-services-de-renseignements-francais-12/

BABILON [T.] et DIAKITE [I.], « Le Quantified self », Université Paris-Est Marne-la-Vallée (UFR Sciences humaines et sociales), Les mondes numériques, 18 février 2017 : https://lesmondesnumeriques.wordpress.com/2017/02/18/le-quantified-self/

BALL [J.], HARDING [L.] et GARSIDE [J.], "BT and Vodafone among telecoms companies passing details to GCHQ", The Guardian, August 2, 2013: https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

BARBAUX [A.], « Identifiant numérique unique Idenum : NKM en a rêvé, Fleur Pellerin l'a fait », L'usine digitale, du 10 avril 2013 : https://www.usine-digitale.fr/article/identifiant-numerique-unique-idenum-nkm-en-a-reve-fleur-pellerin-l-a-fait.N194954

BARON [F.], « La Souveraineté nationale », Parole d'expert, du 7 juillet 2018 : https://www.vie-publique.fr/parole-dexpert/270252-la-souverainete-nationale

BATHELOT [B.], « Définition : Brand content », Définitions marketing, juin 2017 : https://www.definitions-marketing.com/definition/brand-content/

BATHELOT [B.], « Définition : Communication de crise », Définitions marketing, février 2018 : https://www.definitions-marketing.com/definition/communication-de-crise/

Biography.com Editors, "Chelsea Manning Biography", initialement publié le 2 avril 2014, Mis à jour le 12 avril 2019 : https://www.biography.com/activist/chelsea-manning

Biography.com Editors, “Daniel Ellsberg Biography”, initialement publié le 2 avril 2014, Mis à jour le 12 avril 2019 : https://www.biography.com/activist/daniel-ellsberg ; http://www.ellsberg.net/bio/

Bloomberg News, “Mannequins collect data on shoppers via facial-recognition software”, The Washington Post, November 22, 2012 : https://www.washingtonpost.com/business/economy/mannequins-collect-data-on-shoppers-via-facial-recognition-software/2012/11/22/0751b992-3425-11e2-9cfa-e41bac906cc9_story.html?utm_term=.a149cdea7ecd

BOUCHER [P.], « « Safari » ou la chasse aux français », Le Monde, 21 mars 1974 : http://bugbrother.blog.lemonde.fr/files/2010/12/le_monde_-_21_03_1974_009_800_px.1292949083.jpg

BRENNER [D.], “Net Neutrality: A Solution In Search Of A Problem”, Forbes, September 25, 2012 : https://www.forbes.com/sites/ciocentral/2012/09/25/net-neutrality-a-solution-in-search-of-a-problem/#29659ce93fc5

CAMPBELL [F. B. Jr.], “The Slow Death of ‘Do Not Track’”, The New York Times, december 26, 2014 : https://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html

CBS News, Famous Whistleblowers, “Dr. Daniel Ellsberg”, June 10, 2013 : https://www.cbsnews.com/pictures/famous-whistleblowers/

CEA, « Le CEA, acteur clef de la recherche technologique », Présentation générale publiée le 4 mai 2021 : https://www.cea.fr/Pages/le-cea/acteur-clef-de-la-recherche-technologique.aspx#/scene_lmj_1/

CENAS – centre du sommeil, « Organisation du sommeil (les phases) », dernière mise à jour le 12 juin 2018 : http://www.cenas.ch/le-sommeil/comprendre-le-sommeil/phases-du-sommeil/

CGI, “Patient Care & Insights to support patient-centered care”, CGI Group Inc. 2013: https://www.cgi.com/sites/default/files/brochures/cgi-ibm-patient-care-and-insights.pdf

CHAMPEAU [G.], « HealthKit, l’inquiétante base de données médicales d’Apple », Numerama – Sciences, du 2 juin 2014 : https://www.numerama.com/magazine/29561-healthkit-sante-apple-donnees-medecine-hopitaux-big-data.html

CHOMSKY [N.], “What Makes Mainstream Media Mainstream”, Z Magazine, October 1997: https://chomsky.info/199710__/

Clément [G.], « Bourse : tous ces tweets qui ont affolé les marchés financiers », Le Revenu, 14 mars 2018 : https://www.lerevenu.com/bourse/bourse-tous-ces-tweets-qui-ont-affole-les-marches-financiers

Collins [K.], “Why Net Neutrality Was Repealed and How It Affects You”, The New York Times, December 14, 2017 : https://www.nytimes.com/2017/12/14/technology/net-neutrality-rules.html?module=inline

Concordia, 2016 Concordia Summit Agenda, “Session Description - The Power of Big Data and Psychographics”, 2016 : https://www.concordia.net/the-summit-2016/2016-concordia-summit-agenda/#rdv-calendar

Conseil de l’Europe, État des signatures et ratifications du traité 108 - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Situation au 2 mars 2019 : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures

Conseil des Ministres - Communiqué de Presse, « Programmation Militaire pour les années 2019 à 2025 et dispositions intéressant la défense », du 8 février 2018 : https://www.gouvernement.fr/conseil-des-ministres/2018-02-08/programmation-militaire-pour-les-annees-2019-a-2025-et-dispo & https://circulaire.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000036584151/

Courant philosophique, Lexique « Intelligence », du 9 mars 2010 : http://www.histophilo.com/intelligence.php#cite_ref-2

Criteo, "How Criteo Dynamic Retargeting Works for You": https://www.criteo.com/for-marketers/products/criteo-dynamic-retargeting/

CURTIS [A.], "What the Fluck! The point at which journalism fails and modern power begins", BBC UK, BBC Blog, December 5, 2013: https://www.bbc.co.uk/blogs/adamcurtis/entries/44122901-c2e8-34f5-93e0-d4402c163966

Déclaration de Montréal – IA Responsable, une initiative de l'Université de Montréal : https://www.declarationmontreal-iaresponsable.com/la-declaration

DELUZARCHE [C.], « La chute vertigineuse du coût du séquençage ADN », JDN, du 4 juin 2014 : https://www.journaldunet.com/economie/sante/1139340-le-sequencage-adn-a-bas-cout-une-revolution-fabuleuse-et-dangereuse/1139341-chute-des-couts

DHOLAKIA [U. M.], "Uber's Surge Pricing: 4 Reasons Why Everyone Hates It", government technology, January 27, 2016 : https://www.govtech.com/applications/Ubers-Surge-Pricing-4-Reasons-Why-Everyone-Hates-It.html

DHOLAKIA [U. M.], "Why Do Consumers Hate Uber's Surge Pricing?", Rice-Kinder Institution for Urban Research, The Urban Edge, January 27, 2016: https://kinder.rice.edu/2016/01/27/uberhatesurgepricing/#.Vqkf5_krLct

Direction générale de l'armement, « COMSAT NG (Communication par satellite de nouvelle génération) », Ministère des armées, 24 mars 2016 : https://www.defense.gouv.fr/dga/equipement/information-communication-espace/comsat-ng-communication-par-satellite-de-nouvelle-generation

Direction générale de l'armement, « Le programme CERES (capacité de renseignement électromagnétique spatiale) », Ministère des armées, du 24 mars 2016 : https://www.defense.gouv.fr/dga/equipement/information-communication-espace/le-programme-ceres-capacite-de-renseignement-electromagnetique-spatiale

Direction générale de l'armement, « Le programme Musis », Ministère des armées, du 24 mars 2016 : https://www.defense.gouv.fr/dga/equipement/information-communication-espace/musis

Direction générale de l'armement, « Le système de drone tactique (SDT) », Ministère des armées, du 24 mars 2016 : https://www.defense.gouv.fr/english/dga/equipement/missiles-et-drones/le-systeme-de-drone-tactique-sdt

Direction générale de l'armement, « Système de Lutte Anti-mines Marines Futur (SLAMF) », Ministère des armées, du 24 mars 2016 : https://www.defense.gouv.fr/dga/equipement/naval/le-systeme-de-lutte-anti-mines-marines-futur-slamf

ECC, "Vendor RelationShip Management (VRM)", Enriched cloud computing LLC, 2016: http://www.enrichedcloud.com/ECC/jsp/VRM.jsp

EGGEN [D.] et THOMPSON [C. W.], "INS to monitor foreign students", The Washington Post, may 11, 2002: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiW8PKCvuvhAhUHUBoKHf-ADgEQFjAAegQIARAB&url=https%3A%2F%2Fwww.washingtonpost.com%2Farchive%2Fpolitics%2F2002%2F05%2F11%2Fins-to-monitor-foreign-students%2Fe29d277e-bbc3-4ba9-9db7-59c995e585ce%2F&usg=AOvVaw1MI3HpXYOwydtOlQxzFHJV

Electronic Frontier Foundation (EFF), "NSA Spying – How it works", 2017: https://www.eff.org/nsa-spying/how-it-works ou http://www.acamedia.info/politics/surveillance/references/eff/How_the_NSAs_Domestic_Spying_Program_Works.pdf

Encyclopédie de l'Agora, « Intelligence », du 12 avril 2013 : http://agora.qc.ca/Dossiers/intelligence

ENJALBERT [C.], « L'Université de la Singularité arrive en France », Philosophie magazine, du 28 juillet 2015 : https://www.philomag.com/lactu/breves/luniversite-de-la-singularite-arrive-en-france-11947

European data protection supervisor, "Personal Information Management System (PIMS)": https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en

FALQUE-PIERROTIN [I.], « Quelle protection européenne pour les données personnelles ? », Question d'Europe n° 250, publié sur le site de la Fondation Robert Schuman, 3 septembre 2012 : https://www.robert-schuman.eu/fr/doc/questions-d-europe/qe-250-fr.pdf

Federation of American Scientists, "FAPSI History", FAS, November 26, 1997 : https://fas.org/irp/world/russia/fapsi/history.htm

FERNANDEZ [A.], "10 Neurotechnologies About to Transform Brain Health and Brain Enhancement", SharpBrains, November 10, 2015 : https://sharpbrains.com/blog/2015/11/10/10-neurotechnologies-about-to-transform-brain-enhancement-and-brain-health/

FILEV [A.], « L'économie à la demande : un défi pour l'efficacité opérationnelle », Journal Du Net, du 7 décembre 2017 : https://www.journaldunet.com/management/expert/68119/l-economie-a-la-demande---un-defi-pour-l-efficacite-operationnelle.shtml

FILLOUX [F.], "Google News: The secret sauce", The Guardian, February 25, 2013: https://www.theguardian.com/technology/2013/feb/25/1

FIORETTI [J.], "EU seeks to expedite police requests for data from tech firms", Reuters, June 8, 2018 : https://www.reuters.com/article/us-eu-data-security-idUSKBN18Z0H0?feedType=RSS&feedName=technologyNews

FONTAINE [P.], « Google crée un cerveau informatique capable de reconnaître un chat », 01net.com, du 26 juin 2012 : https://www.01net.com/actualites/google-cree-un-cerveau-informatique-capable-de-reconnaitre-un-chat-569065.html

Forbes, “10 Charts That Will Change Your Perspective Of Big Data's Growth”, May 2018: https://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/#c1f8ed029268

France diplomatie - Dossiers, « L’APEC », juin 2018 : https://www.diplomatie.gouv.fr/fr/dossiers-pays/asie-oceanie/les-dynamiques-d-integration-regionale/les-enceintes-de-cooperation-economique/article/l-apec

GALLAGHER [S.], “Porn Block: New Start Date Announced As 15 July Following Delay - Users will have to prove they are over 18 with a passport or driving licence”, HuffPost UK, April 17, 2019: https://www.huffingtonpost.co.uk/entry/porn-block-new-start-date-announced_uk_5cb6fef0e4b082aab08f084c

GALLAGHER [S.], “Porn Block: You'll Soon Be Able To Verify Your Age With A Selfie - But would you want to?”, HuffPost UK, April 18, 2019: https://www.huffingtonpost.co.uk/entry/porn-block-verify-your-age-with-a-selfie_uk_5cb8330be4b081fd1693593c?guccounter=1

Gartner, IT Glossary, “social publishing”: https://www.gartner.com/it-glossary/social-publishing

GEERE [D.], “How deep packet inspection works”, Wired, April 27, 2012: https://www.wired.co.uk/article/how-deep-packet-inspection-works

GLANZ [J.] et LEHREN [A. W.], “N.S.A. Spied on Allies, Aid Groups and Businesses”, The New York Times, December 20, 2013: : https://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html

Glossaire de l’UE, « Interoperability » : https://eur-lex.europa.eu/eli-register/glossary.html?locale=fr

GRASSEGGER [H.] et KROGERUS [M.], “Ich habe nur gezeigt, dass es die Bombe gibt”, Das Magazin, December 3, 2013: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

GRASSEGGER [H.] et KROGERUS [M.], “The Data That Turned the World Upside Down”, Motherboard Vice, January 28, 2017: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

GRAHAM [M.], “Big data and the end of theory?”, The Guardian, March 9, 2012: https://www.theguardian.com/news/datablog/2012/mar/09/big-data-theory

GREENWALD [G.] et MACASKILL [E.], “NSA Prism program taps into user data of Apple, Google and others”, The Guardian, June 6, 2013: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data & https://www.pulitzer.org/files/2014/public-service/guardianus/02guardianus2014.pdf

GREENWALD [G.], “XKeyscore: NSA tool collects 'nearly everything a user does on the internet'”, The Guardian, July 31st, 2013: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

GUIBERT [N.], « La France a vendu des armes pour 9,1 milliards d’euros en 2018 », Le monde, du 4 juin 2019 : : https://www.lemonde.fr/international/article/2019/06/04/la-france-a-vendu-des-armes-pour-9-1-milliards-d-euros-en-2018_5471354_3210.html

GUYONNET [P.], « Melania Trump choque aux États-Unis en portant cette veste Zara lors d'une visite à des migrants » Huffpost International, du 21 juin 2018 : https://www.huffingtonpost.fr/2018/06/21/melania-trump-choque-aux-etats-unis-en-portant-cette-veste-zara-lors-dune-visite-a-des-migrants_a_23465143/

Harris-Interactive, Baromètre 2017 « La confiance des Français dans le numérique », 6ème vague, 18 décembre 2017 : http://harris-interactive.fr/opinion_polls/barometre-la-confiance-des-francais-dans-le-numerique-6e-vague/

HEIMBER [C.], « Gênes, Italie, G8. Résurgences des années noires », Mediapart, Blog : Chroniques pour mémoires, Genève, août 2001 : https://blogs.mediapart.fr/heimbergch/blog/200718/genes-italie-g8-en-2001-resurgences-des-annees-noires-pour-carlo-giuliani

HILL [K.], "'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything", Gizmodo, October 15, 2018 : https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324

Human Rights Watch, "The Guantanamo Trials", August 9, 2018: https://www.hrw.org/guantanamo-trials

HYDE [K.], "What Is Data Exhaust? Cutting Through the Fumes", Capture Higher Ed, June 13, 2017: https://capturehighered.com/predictive-modeling/data-exhaust-cutting-fumes/

IBM Software Solution Brief, "IBM Patient Care and Insights - Identify new intervention and treatment opportunities and deliver coordinated, personalized care to help improve patient outcomes and lower costs", IBM Corporation, October 2012: https://dsimg.ubm-us.net/envelope/119833/305432/1361139266_IBM_Patient_Care_and_Insights.pdf

IC Off The Record, "NSA Tool Collects 'Nearly Everything a User Does on the Internet'", July 31st, 2013: https://nsa.gov1.info/dni/xkeyscore.html

Illumina, Specification Sheet: Illumina® Sequencing, "Genome Analyzer$_{IIx}$ System - The most proven, widely adopted next-generation sequencing platform", Pub. No. 770-2009-017 Current as of April 27, 2011: https://www.illumina.com/content/dam/illumina-marketing/documents/products/datasheets/datasheet_genome_analyzeriix.pdf

INGRAHAM [N.], "False tweet sent a company's stock plummeting more than 25 percent", The Verge, January 29, 2013 : https://www.theverge.com/2013/1/29/3930010/false-tweet-sent-a-companys-stock-plummeting-25-percent

ISM, « Formation – Datavisualisation : visualiser ses données pour mieux piloter », ISM organisme de formation : https://www.ism.fr/formation/datavisualisation-visualiser-ses-donnees-pour-mieux-piloter

ISO 31000:2018, Management du risque – Lignes directrices, Organisation internationale de normalisation-ISO, 2018 : https://www.iso.org/obp/ui/fr/#iso:std:iso:31000:ed-2:v1:fr

JOHNSON [K.], "Dangerous Side Effects Reported from Popular Fitness Trackers", New York CBS local news, May 21, 2018: https://newyork.cbslocal.com/2018/05/21/fitbit-fitness-fail/

JOIGNOT [F.], « Les 30 ans du Web : de l'utopie à un capitalisme de surveillance », Le Monde – Enquête, du 14 février 2019 : https://www.lemonde.fr/pixels/article/2019/02/14/les-30-ans-du-web-de-l-utopie-a-un-capitalisme-de-surveillance_5423578_4408996.html#xtor=AL-32280270

JOVIN [I.], "Some Fitbit users are reporting "shocking" side-effects", Gadgets & Wearables, May 23, 2018: https://gadgetsandwearables.com/2018/05/23/fitbit-shock/

KANG [C.], "F.C.C. Repeals Net Neutrality Rules", The New York Times, December 14, 2017 : https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html

KPMG, « Healthcare Insights - Turning data into patient value», Foreword by S. Murphy, KPMG's Creative Services, December 2015 (21 p.) : https://assets.kpmg.com/content/dam/kpmg/pdf/2016/01/healthcare-insights-dec-2015-2.pdf

La Quadrature du Net, « Privacy Shield : Un « bouclier » troué à refuser ! », du 8 juillet 2016 : https://www.laquadrature.net/2016/07/08/privacy-shield-bouclier-a-refuser/

La Quadrature du Net, « Lettre ouverte internationale des ONG demandant la suspension du Privacy Shield », du 3 mars 2017 : https://www.laquadrature.net/2017/03/03/appel_suspension_privacy_shield/

La Rédaction de Vie-publique.fr, « La réécriture de la loi “Informatique et libertés” du 6 janvier 1978 », du 2 août 2019 : https://www.vie-publique.fr/eclairage/268790-la-reecriture-de-la-loi-informatique-et-libertes-du-6-janvier-1978-cnil

LAUSSON [J.], « Privacy Shield : Le Parlement européen appelle les USA à protéger correctement ses citoyens », Numerama, du 12 juin 2018 : https://www.numerama.com/politique/384867-privacy-shield-le-parlement-europeen-appelle-les-usa-a-proteger-correctement-ses-citoyens.html

LAVRUSIK [V.] et TRAN [T.], “Introducing Live Video and Collages”, Facebook Newsroom, December 3, 2015 : https://newsroom.fb.com/news/2015/12/introducing-live-video-and-collages/

Le Big Data, « Le Dataviz, Qu’est-ce que c’est ? – Définition, outils essentiels », Le Magazine I.A., Cloud et Big data, du 26 octobre 2017 : https://www.lebigdata.fr/dataviz-qu-est-ce-que-c-est

LE CORRE [B.], « Bientôt à Paris, une très singulière « université » », Nouvel Obs, du 8 juillet 2015 : https://www.nouvelobs.com/rue89/rue89-nos-vies-connectees/20150708.RUE9807/bientot-a-paris-une-tres-singuliere-universite.html

Le Monde, « De nouveaux documents publiés par WikiLeaks montrent que la CIA a pu pirater des MacBook », du 23 mars 2017 : https://www.lemonde.fr/pixels/article/2017/03/23/de-nouveaux-documents-publies-par-wikileaks-montrent-que-la-cia-a-pu-pirater-des-macbook_5099828_4408996.html

Le Monde, « Provocation ou gaffe ? La veste « je m’en fiche » de Melania Trump agite l’Amérique », Lemonde – BigBrowser, du 22 juin 2018 : https://www.lemonde.fr/big-browser/article/2018/06/22/provocation-ou-gaffe-la-veste-je-m-en-fiche-de-melania-trump-agite-l-amerique_5319265_4832693.html

Le Monde, « Jean-Marie Delarue : « Au nom de la sécurité, toutes nos libertés sont menacées » », Propos recueilli par L. Couvelaire, du 29 avril 2019 :

https://www.lemonde.fr/societe/article/2019/04/29/jean-marie-delarue-au-nom-de-la-securite-toutes-nos-libertes-sont-menacees_5456075_3224.html

Le portail de l'économie, des finances, de l'action et des comptes publics, « Mise en place de l'identité numérique IDENUM », du 30 mai 2011 : https://www.economie.gouv.fr/mise-place-lidentite-numerique-idenum

Le portail de l'économie, des finances, de l'action et des comptes publics, « Faire du numérique un espace de confiance », du 21 juin 2013 : https://www.economie.gouv.fr/le-numerique-espace-de-confiance

Le portail de la transformation de l'action publique, « Une nouvelle organisation pour la transformation publique et numérique de l'État - Décrets du 20 novembre 2017 », du 21 novembre 2017 : http://www.modernisation.gouv.fr/etudes-et-referentiels/decrets/une-nouvelle-organisation-pour-la-transformation-publique-et-numerique-de-letat-decrets-du-20-novembre-2017

LEBLAL [S.], « Un petit cloud personnel avec Lima Ultra », Le monde informatique, 10 Avril 2017 : https://www.lemondeinformatique.fr/actualites/lire-un-petit-cloud-personnel-avec-lima-ultra-67887.html

LEDIT [G.], « La Singularity University débarque à Bordeaux : « On est là pour animer une communauté locale », Usbek & Rica, du 2 septembre 2017 : https://usbeketrica.com/article/la-singularity-university-debarque-a-bordeaux-on-est-la-pour-animer-une-communaute-locale

LEE [M.], "The Unofficial XKeyscore User Guide", E92 – ADET, Booz Allen Hamilton – Consultant, January 8, 2007 : https://www.documentcloud.org/documents/2116191-unofficial-xks-user-guide.html#document/p1

L'histoire de France, « La Révolution française » : http://www.histoire-france.net/epoque/revolution-francaise

L'Homme Numérique, « Le Privacy Shield remis en cause », du 13 juin 2018 : https://lhommenumerique.wordpress.com/2018/06/13/le-privacy-shield-remis-en-cause/

LIEBER [C.], «Your Favorite Stores Could Be Tracking You With Facial Recognition », Racked, May 22, 2018: https://www.racked.com/2018/5/22/17380410/facial-recognition-technology-retail

LIPOWICZ [A.], "Boeing to staff FBI Fusion Center", Washington Technology, June 1st, 2007: https://washingtontechnology.com/articles/2007/06/01/boeing-to-staff-fbi-fusion-center.aspx

LUPIERI [S.], « Big data : devant nous le déluge », Enjeux, Les Échos, du 1er octobre 2012 : http://archives.lesechos.fr/archives/2012/Enjeux/00294-036-ENJ.htm#

MACASKILL [E.], THIELMAN [S.] et OLTERMANN [P.], "WikiLeaks publishes 'biggest ever leak of secret CIA documents'", The Guardian, March 7, 2017 : https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance

Management Dictionary, Marketing and strategy terms, "What is Buzz Marketing?", Published by MBA Skool Team, January 22, 2018 https://www.mbaskool.com/business-concepts/marketing-and-strategy-terms/2030-buzz-marketing.html

MARTIN [A. J.], "Bletchley Park remembers 'forgotten genius' Gordon Welchman", The Register UK, September 27, 2015: https://www.theregister.co.uk/2015/09/27/gordan_welchman_bletchley_park_remembers/

MesInfos – Fing, « Dataccess – Data-responsible Enterprises: User Experience and Technical Specifications » (En Anglais) – V.1, Fing, February 2018 : http://mesinfos.fing.org/wp-content/uploads/2018/03/PrezDataccess_EN_V1.21.pdf

Myhealthapps Blog, "mHealth App Economics 2017 – Current Status and Future Trends in Mobile Health, Health Apps Market Update", Research2Guidance, May 2, 2018 : http://www.myhealthappsblog.com/mhealth/research2guidance-market-update/

MILLER [J.-A.], « L'invention du partenaire », École de la cause freudienne, Orientations lacanienne, 16 juin 2005 : http://www.causefreudienne.net/linvention-du-partenaire/

Ministère des armées – Actualités, « La DGA commande des avions légers de surveillance et de reconnaissance (ALSR) », DICoD, du 24 juin 2016 : https://www.defense.gouv.fr/espanol/actualites/communaute-defense/la-dga-commande-des-avions-legers-de-surveillance-et-de-reconnaissance-alsr

Ministère des armées – Actualités, « Communiqué de Florence Parly, ministre des Armées : Capacité universelle de guerre électronique – CUGE, Lancement d'un nouveau programme d'avions de renseignement », DICoD, du 28 février 2018 : https://www.defense.gouv.fr/actualites/economie-et-technologie/cp-florence-parly_lancement-d-un-nouveau-programme-d-avions-de-renseignement_cuge

Ministère des armées, « La Division Surveillance de l'Espace du Commandement de la Défense Aérienne et des Opérations Aériennes », DICoD, du 20 mars 2012 : https://www.defense.gouv.fr/portail/dossiers/l-espace-au-profit-des-operations-militaires/fiches-techniques/dse-cdaoa

Ministère des armées, « La Loi de programmation militaire de A à Z », DICoD, du 08 février 2018 : https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/le-lexique/la-loi-de-programmation-militaire-de-a-a-z#S

Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation, *Le programme Horizon 2020* « Technologies de l'information et de la communication – T.I.C. » : https://www.horizon2020.gouv.fr/cid72685/technologies-de-l-information-et-de-la-communication-t.i.c.html

Mkomo.com, "A history of storage cost" (update), March 9, 2014 : http://www.mkomo.com/cost-per-gigabyte-update

National Human Genome Research Institute, “An Overview of the Human Genome Project”, NIH, October 28, 2018 : https://www.genome.gov/12011238/an-overview-of-the-human-genome-project/

Naval Group, « Le futur système de drone aérien », du 1er mars 2019 : https://www.naval-group.com/fr/episode/le-futur-systeme-de-drone-aerien/

NEZOSI [G.], « Comment la France se situe-t-elle entre le modèle bismarckien et le modèle beveridgien ? », Vie-publique, du 29 février 2016 : https://www.vie-publique.fr/decouverte-institutions/finances-publiques/approfondissements/comment-france-situe-t-elle-entre-modele-bismarckien-modele-beveridgien.html

NORVIG [P.], “Practice Makes Perfect: How Billions of Examples Lead to Better Models”, 2008 O'Reilly Emerging Technology Conference, March 2008: https://conferences.oreilly.com/et2008/public/schedule/detail/1778

NOYES [K.], “5 things you need to know about Data exhaust”, Computerworld – IDG News Service, May 13, 2016 : https://www.computerworld.com/article/3070475/5-things-you-need-to-know-about-data-exhaust.html

O’CONNOR [M. C.], “IBM patent sees sensors as high-tech floor boards”, ZDNet, April 23, 2012: https://www.zdnet.com/article/ibm-patent-sees-sensors-as-high-tech-floor-boards/

Onera, Communiqué de Presse, « GRAVES : vers une surveillance spatiale française plus performante », Onera et Degreane Horizon, du 12 décembre 2016 : https://www.onera.fr/sites/default/files/communiques/pdf/2017-06/20161212-CP-Graves-ONERA.pdf

Open Data Handbook Glossary, « Machine readable », Open Knowledge foundation : http://opendatahandbook.org/glossary/en/terms/machine-readable/

ORLIN [J.], « Sleep Tracking Startup Zeo Says Goodnight », Techcrunch.com, March 2013 : https://techcrunch.com/2013/05/22/sleep-tracking-startup-zeo-says-

goodnight/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=TJ4V83HjVbblRHpfVSisjQ

ORSINI [A.], « Terrorisme : Bruxelles veut faciliter l'accès de la police aux données personnelles sur Facebook et Google en Europe », numerama, du 8 juin 2017 : https://www.numerama.com/politique/264933-terrorisme-bruxelles-veut-faciliter-lacces-de-la-police-aux-donnees-personnelles-sur-facebook-et-google-en-europe.html

PACKER [G.], "Amazon and the Perils of Non-disclosure," The New Yorker, February 11, 2014 : https://www.newyorker.com/books/page-turner/amazon-and-the-perils-of-non-disclosure

Patent nº 8138882, "Securing premises using surfaced-based computing technology", Patents Google: https://patents.google.com/patent/US8138882B2/en#patentCitations

Patent n° 7983452, "Using a surface-based computing device for verification of an identification document", JUSTIA Patents, Date of Patent: July 19, 2011: https://patents.justia.com/inventor/kathryn-j-lemanski

PHILLIPS [D.], "JetBlue apologizes for use of Passenger Records", The Washington Post, September 20, 2003: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjKpaSHv-vhAhVCRBoKHfT1BtsQFjAAegQIAxAB&url=https%3A%2F%2Fwww.washingtonpost.com%2Farchive%2Fbusiness%2F2003%2F09%2F20%2Fjetblue-apologizes-for-use-of-passenger-records%2F207e5529-db29-40f3-9e27-6195faed2bff%2F&usg=AOvVaw1Pbh23KrqFfeqpxaEgoeHl

POPE [S.], "Why a Fitbit Harms More Than Helps Your Healt", The healthy home economist, May 29, 2019: https://www.thehealthyhomeeconomist.com/fitbit-health-concerns/

Privacy International, Topic « Communications surveillance », February 8, 2018 : https://privacyinternational.org/explainer/1309/communications-surveillance

Privacy International, “UK mass interception law violates human rights - but the fight against mass surveillance continues”, September 13, 2018 : https://privacyinternational.org/feature/2267/uk-mass-interception-law-violates-human-rights-fight-against-mass-surveillance

Privacy International, Topic “Communications Surveillance: Distinctions and Definitions”, 2019 : https://privacyinternational.org/course-section/2088/communications-surveillance-distinctions-and-definitions

Relative Home Systems, “Future Automation of Multi-Touch Floor From IBM”, April 10, 2012: https://www.relativehomesystems.com/blog/item/future-automation-of-multi-touch-floor-from-ibm

RENOUARD [G.], « Comment l’économie à la demande remodèle la société », L’Atelier BNP Paribas, Archive, Mars 2016 : https://atelier.bnpparibas/smart-city/article/economie-demande-remodele-societe

Research Briefs, “21 Neurotech Startups to Watch: Brain-Machine Interfaces, Implantables, and Neuroprosthetics”, CBInsights, January 28, 2019 : https://www.cbinsights.com/research/neurotech-startups-to-watch/

ROZIÈRES [G.], « Pour 999 dollars, le séquençage de votre génome disponible sur une app », Le HuffPost, du 10 mars 2016 : https://www.huffingtonpost.fr/2016/03/08/sequencage-genome-999-dollars-veritas-genetics-application_n_9408484.html

RTL, "Je m'en fiche complètement": la veste de Melania Trump qui suscite la stupéfaction (vidéo), Rtl Info, du 22 juin 2018 : https://www.rtl.be/people/buzz/-je-m-en-fiche-completement-la-veste-de-melania-trump-qui-suscite-la-stupefaction-1033573.aspx

RUSSELL [K.], “Basis Unveils The Peak, A Smarter Fitness Tracker”, Techncrunch.com, September 30, 2014: https://techcrunch.com/2014/09/30/basis-unveils-the-peak-a-smarter-fitness-tracker/

RUSSEL [K.], “Basis Launches A Limited Edition Titanium Peak, Updates Bands And App”, Techncrunch.com, May 19, 2015 : https://techcrunch.com/2015/05/19/basis-launches-a-limited-edition-titanium-peak-updates-bands-and-app/

SAS, “Data vizualisation - What it is and why it matters”, SAS Insights : https://www.sas.com/en_us/insights/big-data/data-visualization.html

SAS Communiqué, « Assurance maladie : la biostatistique au cœur du pilotage du système de santé » : https://www.sas.com/fr_ma/customers/temoignages-clients/cnamts-pilotage-du-systeme-de-sante.html

SCHWARTZ [B.], “Google’s search knows about over 130 trillion pages”, Search Engine Land, November 14, 2016: https://searchengineland.com/googles-search-indexes-hits-130-trillion-pages-documents-263378

SHENON [P.], “JetBlue Chief Says He Wasn't Told About Release of Data”, The New York Times, September 25, 2003: https://www.nytimes.com/2003/09/25/business/jetblue-chief-says-he-wasn-t-told-about-release-of-data.html

SNOWDEN [E.], “XKeyscore presentation”, February 25, 2008 : https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf

Sommet du G8 - Gleaneagles, Écosse, Royaume-Uni, 6-8 Juillet 2005 : http://www.jacqueschirac-asso.fr/archives-elysee.fr/elysee/elysee.fr/francais/actualites/deplacements_a_l_etranger/2005/juillet/sommet_du_g8_de_gleneagles_en_ecosse.30502.html; http://www.g8.utoronto.ca/francais/2005gleneagles/sommaire.pdf

SRI, 19ème édition de l’Observatoire de l’e-pub du SRI, réalisé par PwC, en partenariat avec l’UDECAM, Bilan 2017 - janvier 2018 (44 p.) : http://www.sri-france.org/etudes-et-chiffre-cles/observatoire-de-le-pub-sri/19eme-observatoire-de-pub-sri/

Statista, “Forecast of Big Data market size, based on revenue, from 2011 to 2027 (in billion U.S. dollars)” (Survey period: 2011-2018), March 2018 : https://www.statista.com/statistics/254266/global-big-data-market-forecast/

STRAW [J.], “Smashing Intelligence Stovepipes”, Security Management – A publications of ASIS International, March 1st, 2008: https://sm.asisonline.org/Pages/Smashing-Intelligence-Stovepipes.aspx

STUPP [C.] – Trad. de CANDAU [M.], « Bruxelles veut faciliter l’accès de la police aux données chiffrées », Euractiv, du 19 octobre 2017 : https://www.euractiv.fr/section/economie/news/brussels-promises-more-police-access-to-encrypted-data-but-no-backdoors/

« Tag Suggest » : « Comment fonctionne la reconnaissance faciale de Facebook ? » : https://www.facebook.com/help/122175507864081

Talend, « Talend’s Big Data Solutions Receive Commitment from Partner Community », Los Altos (CA), September 27, 2012 : https://www.talend.com/about-us/press-releases/talends-big-data-solutions-receive-commitment-partner-community/

Télécoms-infoconso, Arcep, « Arrêt du RTC et transition vers les réseaux téléphoniques de nouvelle génération », du 2 novembre 2018 : https://www.telecom-infoconso.fr/arret-du-rtc-et-transition-vers-les-reseaux-telephoniques-de-nouvelle-generation/

The Economist, « Clicking for gold – How the internet companies profit from data on the Web », *In* Special Report: Data, Data everywhere, February 27, 2010: https://www.economist.com/special-report/2010/02/27/clicking-for-gold & https://www.economist.com/sections/special-reports?page=67

The Europan, Conversation with George Dyson – auteur de l’ouvrage *Turing’s Cathedral* (2011), The Europan Magazine, October 17, 2011 : https://www.theeuropean-magazine.com/352-dyson-george/353-evolution-and-innovation

The National Archives, “Highlights Guide”, (10 p.) : https://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf

The National Archives, “Newly released GCHQ files: UKUSA Agreement”, June 2010 : https://www.nationalarchives.gov.uk/ukusa/

The Wharton School, “How to Turn ‘Data Exhaust’ into a Competitive Edge”, Knowledge@Wharton, University of Pennsylvania, march 1st, 2018: https://knowledge.wharton.upenn.edu/article/turn-iot-data-exhaust-next-competitive-advantage/

Think Tank "Génération libre", Rapport « Mes data sont à moi. Pour une patrimonialité des données personnelles », janvier 2018 : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf

Think Tank "Génération libre", Rapport « Aux data, citoyens ! pour une patrimonialité des données personnelles », septembre 2019 : https://www.generationlibre.eu/wp-content/uploads/2019/09/Rapport-Data-II-_-GL_Web.pdf

TÜRK [P.], « Définition et enjeux de la souveraineté numérique », Parole d’expert, du 14 septembre 2020 : https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique

Uber, « How surge pricing works »: https://www.uber.com/en-FR/drive/partner-app/how-surge-works/

UNESCO Institute of Statistics, Glossary “ Information and communication technologies (ICT)” : http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict

UNTERSINGER [M.], « L’incertaine mais nécessaire "souveraineté numérique" », Le Monde, du 20 novembre 2019 : https://www.lemonde.fr/idees/article/2019/11/20/l-incertaine-mais-necessaire-souverainete-numerique_6019810_3232.html

Vie-publique, « La loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales », du 14 décembre 2005 : https://www.vie-publique.fr/actualite/panorama/texte-vote/loi-du-12-decembre-2005-relative-au-traitement-recidive-infractions-penales.html

Vie-Publique.fr, « État d'urgence et autres régimes d'exception », du 10 novembre 2018 : https://www.vie-publique.fr/actualite/faq-citoyens/etat-urgence-regime-exception/

VITT [R.], « Témoignage : un mois avec une montre connectée c'est effrayant », Phonandroid, du 26 octobre 2015 : https://www.phonandroid.com/temoignage-mois-avec-montre-connectee-effrayant.html

Wikipédia, « série télévisée Black Mirror », article du 1er avril 2021 : https://fr.wikipedia.org/wiki/Black_Mirror_(série_télévisée)

Wikileaks, « Vault 7: CIA Hacking Tools Revealed », March 7, 2017 : https://wikileaks.org/ciav7p1/

World Economic Forum, Global Risks 2018, The Global Risks Report 2018, 13th edition, Genève: https://www.weforum.org/reports/the-global-risks-report-2018; http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

WU [T.], « Attention Brokers », NYU Law, September 2015 : http://www.law.nyu.edu/sites/default/files/upload_documents/Tim%20Wu%20-%20Attention%20Brokers.pdf

ZASLAVSKY [A.], « September 2013 Theme: Internet of Things and Ubiquitous Sensing », Tech News – Computing now, IEEE Computer Society, 2014 : https://www.computer.org/publications/tech-news/computing-now/internet-of-things-and-ubiquitous-sensing

* Bases de données

academy.visiplus.com
acxiom.com
aclu.org
ai.google
allaboutdnt.com
allistene.fr
almax-italy.com
ameli.fr
amazon.fr/gp/help
analytics.google.com
apec.org
api.gouv.fr
apple.com/fr
arcep.fr
archive.org
archives.assemblee-nationale.fr
archiv.digitales.oesterreich.gv.at
archives.libreblancdefenseetsecurite.gouv.fr
assemblee-nationale.fr
audralawson.com
autoritedelaconcurrence.fr
aws.amazon.com
bis.lexisnexis.fr
blog.archive.org
blogrecherche.wp.imt.fr
bloomberg.com
bnd.bund.de/EN
books.openedition.org
boozallen.com
bu.edu
buffer.com
heise.de
hhs.gov
hks.harvard.edu
home.cern/fr
horizon2020.gouv.fr
hrlibrary.umn.edu
hsdl.org
hudoc.echr.coe.int
huffingtonpost.fr
hugavenue.com
humanmetrics.com
icct.nl
ifop.com
illumina.com
inria.fr
insee.fr
international.gc.ca
internetlivestats.com
interpol.int
iplocation.net
ip2location.com
irep.asso.fr
irks.at
itu.int
journals.openedition.org
justice.gov
kurzweilai.net
kurzweiltech.com
ladocumentationfrancaise.fr
lannuaire.service-public.fr
larousse.fr

bundesregierung.de
cairn.info.htm
carthoris.free.fr
cc.europa.eu
cerna.org
cerna-ethics-allistene.org
cgi.fr
citeseerx.ist.psu.edu
classics.mit.edu
classiques.uqac.ca
claudinelepage.eu
cnil.fr
cnle.gouv.fr
cnpd.public.lu
cnrs.fr
cnrtl.fr
coe.int
communaute.ebay.fr
communication.oxfordre.com
concordia.net
conseil-constitutionnel.fr
conseil-etat.fr
controverses.mines-paristech.fr
coppa.org
core.ac.uk
corteidh.or.cr
criteo.com
courdecassation.fr
cs.stanford.edu
curia.europa.eu
datacatalog.worldbank.org
data.gov
data.oecd.org
law.yale.edu
laws-lois.justice.gc.ca
lecese.fr
legifrance.gouv.fr
legroupe.laposte.fr
lemonde.fr
lexico.com
1libertaire.free.fr
linkedin.com
linternaute.fr
marketingplatform.google.com
marketpsych.com
mesinfos.fing.org
meetic.fr
modernisation.gouv.fr
mydata.org
mydatachoices.co.uk
myerbriggs.com
myfitnesspal.com
nafta-sec-alena.org
namebase.net
ncbi.nlm.nih.gov
necessaryandproprotionate.org
news.adidas.com
nexatech.fr
nike.com
nsa.gov
obamawhitehouse.archives.gov
oecd.org
ohchr.org
osp.revues.org
oxfordlearnersdictionaries.com
paris-singularity.fr

data.worldbank.org
deeplearningbook.com
defense.gouv.fr
definitions-marketing.com
developer.apple.com
developers.google.com
dhs.gov
dicolatin.com
dictionnaire-academie.fr
dictionary.com
digitalcommons.wcl.american.edu
digital-strategy.ec.europa.eu
digitude.fr
dimsung.free.fr
diplomatie.gouv.fr
doctrine.fr
documents-dds-ny.un.org
doi.org
dougengelbart.org
drumup.io
duncancampbell.org
dx.doi.org
ec.europa.eu
echr.coe.int
econ.ucsb.edu
economie.gouv.fr
edarling.fr
edpb.europa.eu
edps.europa.eu
en.oxforddictionaries.com
epic.org
equifax.com
ercom.fr
pde.cc
pds.mydex.org
persee.fr
16personalities.com
philosophie.cegeptr.qc.ca
piaf-archives.org
pipl.com
plato.stanford.edu
plosbiology.org
privacyshield.gov
publications.parliament.uk
quantifiedself.com
references.modernisation.gouv.fr
refworld.org
remacle.org
repository.law.indiana.edu
reputation.com
reputationvip.com
riigiteataja.ee
rm.coe.int
runkeeper.com
schneier.com
scl.us.com
seagate.com
search.coe.int
search.google.com
securite-sociale.fr
semantic-web.com
senat.fr
sirs-fr.com
socialmention.com
sop.inria.fr
statewatch.org

espace-ethique-poitoucharentes.org
etic-data.com
etsi.org
eur-lex.europa.eu
europa.eu
europarl.europa.eu
europol.europa.eu
experian.co.uk
experian.com
facebook.com/help
fipr.org
fitbit.com
fnlondon.com
fr.reputationdefender.com
fr.statista.com
fra.europa.eu
fra.se
francearchives.fr
franceconnect.gouv.fr
frontiersin.org
ftc.gov
gallica.bnf.fr
galton.org
gchq.gov.uk
gendarmerie.interieur.gouv.fr
gouvernement.fr
govinfo.gov
gst.dk
hackingteam.it
hal.archives-ouvertes.fr
su.org
support.google.com
supreme.justia.com
swisslife.fr
systancia.com
syti.net
target.com
techopedia.com
textes.justice.gouv.fr
trade.ec.europa.eu
travail-emploi.gouv.fr
treaties.un.org
trends.google.com
truity.com
twitter.com
uber.com
un.org
undocs.org
unesco.org
unicef.fr
veille-strategique.org
vie-publique.fr
votre-reputation.com
w3.org
web02.gonzaga.edu
weborama.fr
wired.com
withings.com
zz.isommeil.net

Table des matières

L'émergence de l'identité numérique. L'influence de la révolution numérique sur l'environnement juridique

Recherche en droits et libertés fondamentales, en droit comparé et en politique criminelle, l'analyse contribue à l'étude de l'émergence de l'identité numérique à l'ère de la révolution numérique. Celle-ci a entraîné l'élaboration de l'environnement numérique, fondé sur les TIC, Big data, traitements de données à caractère personnel, code, surveillance, objets et dispositifs numériques et intelligents, qui imprègne et influence l'environnement juridique dans sa globalité et, à terme, l'individu dans sa singularité, l'identité dans sa dimension physique ou numérique. En analysant les interprétations sociojuridiques du concept d'identité numérique puis la réalité des enjeux l'affectant au regard des innombrables opérations de traitement dont il fait l'objet, l'étude montre que cet écosystème se développe au nom de la sécurité, la défense, la liberté, l'économie, l'innovation, la prévention, pour le bien-être de l'humanité, et ce au détriment de la liberté, des droits et libertés fondamentales, du respect de la vie privée et de la dignité, de la protection des données et des personnes concernées par les traitements entrepris couramment dans différents secteurs privés comme publics. Cette recherche propose une description de ce contexte, des relations dynamiques et interconnectées existant entre données, vie privée, liberté, autonomie dans la construction de soi, sécurité, TIC, cyberespace, RGPD et loi informatique et libertés, ainsi que des effets et enjeux que ces relations peuvent induire à l'échelle de la société, de l'humanité et, notamment, de l'identité numérique, le soi connecté, le prolongement technologique de l'identité, à l'époque de la numérisation de la société.

Mots-clés : Identité, Big data et révolution numérique, Données à caractère personnel, RGPD et Loi informatique et libertés, vie privée, surveillance, économie des données, cyberespace, TIC, liberté, sécurité.

Title: The emergence of the digital identity. The influence of the digital revolution on the legal environment

Research in fundamental rights and freedoms, comparative law and criminal policy, the analysis contributes to the study of the emergence of the digital identity in the era of the digital revolution. An era that has led to the development of the digital environment, founded on ICT, Big data, personal data processing, code, surveillance, digital and intelligent objects and devices, that permeates and influences the legal environment as a whole and, ultimately, the individual in its singularity, the identity in its physical or digital dimension. By analysing the socio-legal interpretations of the concept of digital identity and then the reality of the issues affecting it with regard to the countless processing operations it is subject to, the study shows that this ecosystem develops in the name of security, defence, freedom, economy, innovation, prevention, for the well-being of humanity, at the expense of freedom, fundamental rights and freedoms, respect for privacy and dignity, data protection and the data subjects concerned by the processing routinely undertaken in different private and public sectors. This research provides a description of this context, the dynamic and interconnected relations between data, privacy, freedom, autonomy in the construction of self, security, ICT, cyberspace, GDPR and the French data protection law, as well as the effects and concerns that these relations can induce at the scale of society, humanity, and, in particular, digital identity, the connected self, the technological extension of identity, in the era of the digitalisation of society.

Keywords: Identity, Big data and digital revolution, personal data, GDPR and French data protection law, privacy, surveillance, data economy, cyberspace, ITC, liberty, security.