Libertés publiques, libertés individuelles, risques et enjeux de la société numérique

Jean Harivel

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE
ÉCOLE DE DROIT
DE LA SORBONNE

École Doctorale de Droit de la Sorbonne (ED 565)

Libertés publiques, libertés individuelles
Risques et enjeux de la société numérique

Thèse de droit public

présentée par **Jean HARIVEL**

Sous la direction de **William GILLES**

soutenue à l'Université Paris 1 Panthéon Sorbonne
le 19 juin 2018

Jury composé de :

Antoine DELBLOND, Professeur à l'Université de Nantes, rapporteur

Grenfieth SIERRA CADENA, Professeur à l'Université du Rosaire (Colombie), rapporteur

William GILLES, Maître de conférences HDR à l'Université Paris 1 Panthéon Sorbonne, Directeur de thèse

Daniel WUNDER HACHEM, Professeur à l'Université fédérale du Parana (Brésil)

Jean-Jacques LAVENUE, Professeur émérite à l'Université de Lille

Francisco TORTOLERO, Professeur à l'Université Nationale Autonome du Mexique (UNAM) (Mexique)

Laurent VIDAL, Maître de conférences HDR à l'Université Paris 1 Panthéon Sorbonne, Directeur du département Droit public de l'économie de l'Institut de Recherche Juridique de la Sorbonne (IRJS)

École Doctorale de Droit de la Sorbonne (ED 565)

Libertés publiques, libertés individuelles
Risques et enjeux de la société numérique

Thèse de droit public

présentée par **Jean HARIVEL**

Sous la direction de **William GILLES**

soutenue à l'Université Paris 1 Panthéon Sorbonne

le 19 juin 2018

Jury composé de :

Antoine DELBLOND, Professeur à l'Université de Nantes, rapporteur

Grenfieth SIERRA CADENA, Professeur à l'Université du Rosaire (Colombie), rapporteur

William GILLES, Maître de conférences HDR à l'Université Paris 1 Panthéon Sorbonne, Directeur de thèse

Daniel WUNDER HACHEM, Professeur à l'Université fédérale du Parana (Brésil)

Jean-Jacques LAVENUE, Professeur émérite à l'Université de Lille

Francisco TORTOLERO, Professeur à l'Université Nationale Autonome du Mexique (UNAM) (Mexique)

Laurent VIDAL, Maître de conférences HDR à l'Université Paris 1 Panthéon Sorbonne, Directeur du département Droit public de l'économie de l'Institut de Recherche Juridique de la Sorbonne (IRJS)

Avertissement

L'École de droit de la Sorbonne, Université Paris 1 Panthéon-Sorbonne, n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse. Ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

Au terme de plusieurs années de recherche, je tiens à remercier M. William Gilles, mon directeur de recherche, qui m'a guidé dans ce travail ainsi que Mme Irène Bouhadana pour sa gentillesse et son attention durant cette période. Ils m'ont fait participer à des colloques internationaux, m'ayant ainsi permis d'échanger des réflexions avec des professeurs et chercheurs français et étrangers.

Je remercie également les étudiants du master 2 droit des données, des administrations numériques et des gouvernements ouverts qui m'ont fait confiance en me demandant de diriger leurs travaux de mémoire, me permettant ainsi personnellement d'approfondir certains aspects de cette thèse.

Je tiens aussi à remercier mon épouse Marie-Madeleine qui a dû savoir patienter et supporter les contraintes indirectes liées à ce travail, mais qui m'a toujours soutenu et encouragé à persévérer dans les moments de doute.

Sommaire

Principaux acronymes et sigles

AAI	Autorité administrative indépendante
ACLU	*American Civil Liberties Union*
ADN	Acide désoxyribonucléique
AFNIC	Association française pour le nommage Internet en coopération
ANSSI	Agence nationale de sécurité des systèmes informatiques
ARCEP	Autorité de régulation des communications électroniques et des postes
ARIANE	Application de Rapprochement, d'Identification et d'Analyse pour les Enquêteurs
BCR	*Binding Corporate Rules*
CADA	Commission d'accès aux documents administratifs
CD	*Compact Disc*
CEPD	Comité européen de la protection des données
CIL	Correspondant informatique et libertés
CNCIS	Commission nationale des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNIL	Commission nationale de l'informatique et des libertés
COPA	*Child Online Protection Act*
COPPA	*Children's Online Privacy Protection Act*
CPCE	Code des postes et des communications électroniques
DADVSI	Droit d'auteur et droits voisins dans la Société de l'Information
DARPA	*Defense Advanced Research Projects Agency*
DDHC	Déclaration des droits de l'homme et du citoyen
DGT	Direction générale des télécommunications
DINSIC	Direction interministérielle du numérique et du système d'information et de communication de l'État
DNRED	Direction nationale des recherches et enquêtes douanières
DNS	*Domain Name Server*
DRM	*Digital Right Management*
DUDH	Déclaration universelle des droits de l'homme
DVD	*Didital versatil disc*
EC3	*European Cybercrime Centre*
ESTA	*Electronic System for Travel Authorization*
FAI	Fournisseur d'accès Internet
FBI	*Federal Bureau of Investigation*
GCHQ	*Government Communication Headquarter*
GPS	*Global Positioning System*
GSM	*Global System for Mobile Communications*
HADOPI	Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet
INHESJ	Institut national des hautes études de la sécurité et de la justice
INRIA	Institut national de recherche en informatique appliquée
JUDEX	système judiciaire de documentation et d'exploitation
LCEN	Loi pour la confiance dans l'économie numérique
LOPSI	Loi d'orientation et de programmation pour la sécurité intérieure

LOPPSI	Loi d'orientation et de programmation pour la performance de la sécurité intérieure
NFC	*Near Field Communication*
NIR	Numéro d'Inscription au répertoire (INSEE)
NIRPP	Numéro d'Inscription au répertoire des personnes physiques (NIR)
NSA	*National Service Agency*
PESC	Politique étrangère et de sécurité commune
PHAROS	Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements
PIN	*Personal Identification Number*
PNR	*Passenger Name Record*
QPC	Question préjudicielle de constitutionnalité
RFID	*Radio Frequency Identification*
RGPD	Règlement général sur la protection des données
RNIAM	Répertoire national inter régimes des bénéficiaires de l'Assurance Maladie
RNIPP	Répertoire national d'Identification des personnes physiques
SAFARI	Système automatisé pour les fichiers administratifs et le répertoire des individus
SIS	Système d'information Schengen
SIS	*Secret Intelligence Service*
SIV	Système d'immatriculation des véhicules
SMS	Short Message Service
STAD	Système de traitement automatique de données
STIC	Système de traitement des infractions constatées
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TES	Titre électronique sécurisé
TFUE	Traité pour le fonctionnement de l'Union européenne
UE	Union européenne
URL	*Uniform Resource Locator*
VoIP	*Voice over IP*
VPN	*Virtual Private Network*
Wi-Fi	*Wireless Fidelity*

Principales abréviations utilisées dans les citations

AFDI	*Annuaire français de droit international*
AJDA	*Actualité juridique - Droit administratif*
Ann. parl.	*Annales parlementaires*
aff.	Affaire soumise à la Cour de justice avant la création du Tribunal
aff. C-	Affaire soumise à la Cour de justice
aff. jtes	Affaires jointes
aff. T-	Affaire soumise au Tribunal
al.	Alinéa
art.	Article
AUE	Acte unique européen
Bull. CE	*Bulletin des Communautés européennes*
Bull. fisc.	*Bulletin fiscal*
Bull. UE	*Bulletin de l'Union européenne*
c/	Contre
Cass.	Cour de cassation
CCC	*Cahiers du Conseil constitutionnel*
CDE	*Cahiers de droit européen*
CE	Communauté européenne
CECA	Communauté européenne du charbon et de l'acier
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales
CEE	Communauté économique européenne
CEEA	Communauté européenne de l'énergie atomique
CEI	Communauté des États indépendants
Cf.	Comparez, rapprochez
Chron.	Chronique
CIG	Conférence intergouvernementale
CJAI	Coopération dans les domaines de la justice et des affaires intérieures
CJ	Cour de justice
CJUE	Cour de justice de l'Union européenne
Coll.	Collection
CML rev.	*Common market law review*
Comm.	Commentaire
Concl.	Conclusions
Cons. const.	Conseil constitutionnel
Cons. D'État	Conseil d'État
Cour const.	Cour constitutionnelle
Cour EDH	Cour européenne des droits de l'homme
CPJI	Cour permanente de justice internationale
CPJP	Coopération policière et judiciaire en matière pénale
CSCE	Conférence sur la sécurité et la coopération en Europe
D.	*Dalloz (revue)*
Décr.	Décret
Dir.	Direction ou Directeur(s)
DF	*Documentation française*

Doc. parl.	*Documents parlementaires*
Dr. adm.	*Droit administratif*
Dr. env.	*Droit de l'environnement*
Dr. fisc.	*Droit fiscal*
Dr. soc.	*Droit social*
e. a.	Et autres
Éd.	Éditions ou Éditeur(s)
égal.	Également
EL rev.	*European law review*
ELSJ	Espace de Liberté, de Sécurité et de Justice
EuGRZ	*Europaïsche grundrecht zeitschrift*
Ex.	Exemple
GACEDH	*Grands arrêts de la Cour européenne des droits de l'homme*
GAJA	*Grands arrêts de la jurisprudence administrative*
GAJUE	*Grands arrêts de la jurisprudence de l'Union européenne*
GDCC	*Grandes décisions du Conseil constitutionnel*
G. Pal.	*Gazette du palais*
Ibid.	Référence citée à la note de bas de page précédente
J.-Cl. Europe	*JurisClasseur Europe Traité*
JCP	*JurisClasseur périodique (La semaine juridique) JDI Journal du droit international*
JORF	*Journal officiel de la République française*
JO	*Journal officiel des Communautés européennes ou Journal officiel de l'Union européenne*
JT	*Journal des tribunaux*
JTDE	*Journal des tribunaux de droit européen*
Lamy - Proc. com.	*Lamy – Procédures communautaires*
LPA	*Les petites affiches*
Mél.	Mélanges
Mon. be	*Moniteur belge*
Nep	*Non encore publié (arrêt ou ordonnance)*
not.	Notamment
Obs.	Note d'observations
Ord.	Ordonnance
Op. cit.	Source (généralement doctrinale) citée précédemment
OPOCE	*Office des publications officielles des Communautés européennes*
p.	Page
pp.	Pages
§	Paragraphe
PAC	Politique agricole commune
PECO	Pays d'Europe centrale et orientale
PESC	Politique étrangère et de sécurité commune
PIB	Produit intérieur brut
PNB	Produit national brut
RCADI	*Recueil des cours de l'académie de droit international*
Rec.	*Recueil de la jurisprudence de la Cour de justice et du Tribunal*
Rec. FP	*Recueil de jurisprudence-Fonction publique*
Rec. Sirey	*Recueil Dalloz-Sirey des décisions du Conseil d'État*

Rép. Com. Dalloz *Encyclopédie Dalloz-Droit communautaire*
Req. *Requête*
Rev. *Revue*
Rev. adm. *Revue administrative*
Rev. aff. eur. *Revue des affaires européennes*
Rev. crit. dr. int. privé *Revue critique de droit international privé*
Rev. dr. fisc. *Revue de droit fiscal*
RDP *Revue du droit public et de la science politique*
RDUE *Revue du droit l'Union européenne*
Rev. eur. *Revue Europe - Actualité du droit de l'Union européenne (Les revues du JurisClasseur)*
Rev. eur. dr. env. *Revue européenne de droit de l'environnement*
Rev. eur. dr. pub. *Revue européenne de droit public*
RFAP *Revue française d'administration publique*
RFDA *Revue française de droit administratif*
RFDC *Revue française de droit constitutionnel*
Rev. fra. fin. pub *Revue française de finances publiques*
Rev. fra. sc. pol. *Revue française de science politique*
RGDIP *Revue générale de droit international public*
Rev. int. dr. comp. *Revue internationale de droit comparé*
RIDE *Revue internationale de droit économique*
Rev. int. pol. comp. *Revue internationale de politique comparée*
RJE *Revue juridique de l'environnement*
Rev. juris. fisc. *Revue de jurisprudence fiscale*
Rev. trésor *Revue du Trésor*
Rev. Marché Commun *Revue du marché commun*
Rev. Marché Commun UE *Revue du marché commun et de l'Union européenne*
Rev. Marché unique eur. *Revue du marché unique européen*
RRJ *Revue de recherche juridique et de droit prospectif*
RTD civ. *Revue trimestrielle de droit civil*
RTD eur. *Revue trimestrielle de droit européen*
RTD hom. *Revue trimestrielle des droits de l'homme*
RTDSS *Revue trimestrielle de droit sanitaire et social*
RUDH *Revue universelle des droits de l'homme*
RNB Revenu national brut
s. Suivants ou suivantes
s.n. Publié sans nom d'auteur
S. *Sirey (revue)*
spéc. Spécialement
Statut Statut de la Cour de justice de l'Union européenne
TC Eur. Traité établissant une Constitution pour l'Europe
TCE Traité instituant la Communauté européenne
TCECA Traité instituant la Communauté européenne du charbon et de l'acier
TCEE Traité instituant la Communauté économique européenne
TFPUE Tribunal de la fonction publique de l'Union européenne
TFUE Traité sur le fonctionnement de l'Union européenne
Trib. Tribunal
TUE Traité sur l'Union européenne
UE Union européenne
UEM Union économique et monétaire

Voy.	Voyez
Vol.	Volume
YEL	*Yearbook of European law*

« *Il n'y a point de liberté sans loi.* »

Jean-Jacques Rousseau

Lettre VIII *in Lettres écrites de la montagne* (1764).

« *Avoir des esclaves n'est rien.*

Ce qui est intolérable, c'est d'avoir des esclaves en les appelant citoyens. »

Denis Diderot

Supplément au voyage de Bougainville,

ou dialogue entre A et B sur l'inconvénient d'attacher des idées morales à certaines actions physiques qui n'en comportent pas (1772).

Introduction

L'informatique, initialement enseignée en France comme mathématiques appliquées[1], est de fait une technique de mise en œuvre d'algorithmes[2] pour traiter de l'information[3]. L'un des premiers scientifiques ayant travaillé sur les automates d'états finis, classe particulière d'algorithme, ayant contribué au développement des ordinateurs est Alan Turing, mathématicien anglais[4], considéré comme l'un des pères de l'informatique et co-inventeur de l'ordinateur. D'outil mathématique utilisé pour décrypter les messages codés par ENIGMA[5], l'ordinateur s'est révélé un outil polyvalent et a progressivement envahi tous les niveaux de la société devenant un outil universel et omniprésent[6].

La révolution informatique a fortement marqué la société moderne. En l'espace d'un demi-siècle, les habitudes héritées de la révolution industrielle du XIX^{e} siècle et de la mise à disposition de nouvelles énergies ont été remplacées. L'évolution de ces nouvelles techniques a affecté la société dès la fin du XX^{e} siècle et ses conséquences continuent de se faire ressentir au début de ce siècle. Jamais auparavant dans l'histoire de l'humanité, de nouveaux progrès

[11] L'une des premières écoles d'ingénieurs créée en 1960 à Grenoble s'appelait École Nationale Supérieure d'Ingénieurs en Mathématiques appliquées de Grenoble (ENSIMAG) et délivrait des diplômes d'ingénieurs Mathématiciens. Aujourd'hui, son nom est devenu École nationale supérieure d'informatique et de mathématiques appliquées (Lire le communiqué « 50 ans Grenoble INP – Ensimag : 60 diplômes oubliés ont été remis à leurs titulaires » en ligne à l'URL : http://www.grenoble-inp.fr/actualites/50-ans-grenoble-inp-ensimag-60-diplomes-oublies-ont-ete-remis-a-leurs-titulaires-375656.kjsp, consulté le 30 novembre 2017).

[2]Algorithme : nom masculin, (du latin médiéval Algorithmus, latinisation du nom d'un mathématicien de langue arabe, avec influence du grec arithmos, nombre), Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur. (source : dictionnaire Larousse à l'URL : http://www.larousse.fr/dictionnaires/francais/algorithme/2238.

[3] L'une des premières sociétés de service informatique en France s'appelait SoGeTI pour Société de Gestion et de Traitement de l'Information (créée à Grenoble en 1967 par Serge Kampf). Lire à ce sujet Tristan Gaston-Breton, *Serge Kampf Le plus secret des grands patrons français*, 2014, Éditions Tallandier.

[4] Alan Turing (1912-1954), mathématicien britannique. Il publie en 1950 un article intitulé « Computing machinery and intelligence » dans *Mind*, il se pose la question : un ordinateur peut-il tenir la place d'un être humain dans le jeu de l'imitation ? Peu connu du grand public, il a été révélé par le film « Imitation game », réalisé par Morten Tyldum, sorti en 2014.

[5] Durant la Seconde Guerre Mondiale, les armées allemandes utilisaient une machine électromécanique portative pour crypter les messages, appelée en allemand *Die Chiffriermaschine Enigma*. Le code changeait tous les jours en modifiant le positionnement des disques et en permutant dix paires de lettres sur un tableau de connexion. (Lire sur le sujet Gustave Bertrand, *Enigma ou la plus grande énigme de la guerre 1939-1945,* Plon, 1973).

[6] Isabelle Tellier, « Chapitre 4 L'histoire de l'informatique » in Isabelle Tellier, *Introduction à l'informatique*, *Cours de L1 Miashs,* Université de Lille 3, en ligne à http://www.lattice.cnrs.fr/sites/itellier/poly_intro_info/intro-info.pdf consulté le 30 mars 2018.

techniques ne sont apparus aussi rapidement, avec des répercussions quasi immédiates dans la vie des individus, créant parfois une véritable addiction.

Depuis 1946, date officielle de la présentation du premier calculateur électronique reprogrammable[7], les calculateurs électroniques ont progressivement envahi notre vie quotidienne. Sorti des laboratoires, l'ordinateur est devenu l'outil indispensable des entreprises avant de devenir un outil individuel et personnel. Dans les années 1980, de nombreuses techniques analogiques ont été digitalisées[8] et les moyens de transmission des données entre ordinateurs se sont développés grâce à l'invention du modem[9]. En France, à partir de 1975[10], le téléphone a vu les centraux analogiques remplacés progressivement par des centraux électroniques et la Direction générale des Télécommunications[11] a lancé le programme Télétel en 1980 avec la diffusion gratuite du Minitel. Ce petit terminal permettait d'accéder aux services vidéotex, dont l'annuaire électronique, aux messageries et aux premiers sites de commandes électroniques, marquant ainsi la fusion des télécommunications et de l'informatique[12]. Depuis, le Vidéotex a été remplacé par Internet[13] et le téléphone filaire par les téléphones GSM[14]. Les téléphones mobiles ont vu avec la miniaturisation des composants électroniques de nombreuses fonctions ajoutées à la fonction initiale de téléphonie, au point

[7] Le 14 février 1946, l'ENIAC (acronyme de l'expression anglaise *Electronic Numerical Integrator Analyser and Computer*), est dévoilé au public à l'Université de Pennsylvanie à Philadelphie. Il est le premier ordinateur entièrement électronique. Il peut être reprogrammé pour résoudre, en principe, tous les problèmes calculatoires.

[8] Des données analogiques ont été transformées en données numériques permettant une lecture directe de leur valeur, mais aussi un stockage sur support informatique et une transformation algorithmique.

[9] Modem pour modulateur-démodulateur, dispositif électronique qui permet de faire circuler (réception et envoi) des données numériques sur un canal analogique.

[10] Les premiers prototypes de commutateurs électroniques, SOCRATE (système organique de commutation rapide automatique à traitement électronique) et ARISTOTE (autocommutateur réalisant intégralement et systématiquement toutes les opérations de téléphonie électronique) ont été testés à Lannion en 1964 et 1965. Le premier commutateur E11 a été mis en service en 1976 à Athis-Mons puis en 1977 à Marseille (source personnelle de l'auteur).

[11] La Direction générale des télécommunications est renommée France Télécom le 1er janvier 1988, transformée en établissement de droit public par la loi n° 90-568 du 2 juillet 1990 *relative à l'organisation du service public de la poste et à France Télécom*, puis en société anonyme par la loi no 96-660 du 26 juillet 1996 *relative à l'entreprise nationale France Télécom*. Après l'ouverture au public de son capital en 1997 et le rachat d'ORANGE en 2000 puis 2003, le changement de nom du Groupe France Télécom en ORANGE est voté lors de l'assemblée générale du 28 mai 2013 et sera effectif au 1er juillet 2013.

[12] Fusion confirmée par le mot télématique obtenu en accolant le début du mot télécommunications à la fin du mot informatique (Simon Nora, Alain Minc, *L'informatisation de la société, rapport à M. le Président de la République*, janvier 1978, La Documentation française, p. 11).

[13] Les premiers accès à Internet étaient réalisés par utilisation d'un modem et d'une ligne téléphonique avec des vitesses de transmission de 2400 bps. En France, les premiers accès à Internet étaient disponibles à partir de 1994 pour le grand public. En avril 1999, Free, Freesurf et World Online proposent un accès à Internet par le réseau commuté sans abonnement ni numéro surtaxé.

[14] GSM ou Global System for Mobile Communications est une norme numérique pour la téléphonie mobile. La première norme GSM a été spécifiée et mise au point par l'ETSI (*European Telecommunications Standard Institut*) pour une gamme de fréquence de 900 MHz à partir de 1982.

qu'aujourd'hui, ces téléphones sont devenus des « *smartphones* » permettant de localiser leur position, de se connecter à Internet, de prendre des photographies ou de petits films. Le téléphone est devenu un microordinateur individuel pouvant être transporté dans une poche ou un sac à main. De nombreuses applications fournissent des services de proximité : localisation de restaurants, guides de parcours, etc. en utilisant des données à caractère personnel présentes dans la mémoire de ces smartphones, parfois, au détriment des libertés individuelles, voire publiques, en dévoilant des pans de la vie privée[15]. De centralisés et étatiques, les réseaux avec Internet sont devenus distribués et mondialisés.

Mais la numérisation de la société a aussi fondamentalement modifié les relations entre les individus, entre les individus et l'administration, et bouleversé nos habitudes en favorisant certaines libertés ou certains droits fondamentaux tout en les affaiblissant, montrant ainsi l'ambiguïté ou l'ambivalence de la transformation liée à la numérisation de la société[16].

Les libertés publiques sont celles que l'individu peut exercer au sein de la société et l'adjectif précise que ces libertés sont envisagées en tant qu'objets de la réglementation juridique[17]. Parmi ces libertés, les libertés individuelles sont celles qui touchent la vie privée et la personne d'un individu, et dont il use et abuse seul. La liberté individuelle est liée au respect de la vie privée de l'individu ou au respect de l'intimité de cette vie privée[18]. La sûreté et la liberté de se déplacer sont des libertés individuelles. À ces libertés, il y a lieu d'ajouter la protection de la vie privée, protection qui n'est apparue que tardivement dans la législation française. Issu de la loi n° 70-643 du 17 juillet 1970[19], l'article 9 du Code civil dispose : « chacun a droit au respect de sa vie privée », principe que l'on retrouve également à l'article 8 de la Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales[20] qui ajoute le droit au respect

[15] Caroline Vallet, « Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs », *Droit et société* 2012/1 (n° 80), pp. 163-188.

[16] Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014.

[17] Patrick Wachsmann, *Libertés publiques,* Dalloz, 6e édition 2009, p. 2.

[18] Formulation utilisée dans l'Article 9 du Code civil : « *Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée* ».

[19] Loi n° 70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens* publiée au JORF du 19 juillet 1970 page 6751.

[20] L'article 8 de la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales 1953 - droit au respect de la vie privée et familiale - dispose : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 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* ».

de la vie familiale, du domicile et de la correspondance, et à l'article 7 de la Charte des droits fondamentaux de l'Union européenne.

Jean Rivero[21], dans son cours sur les libertés publiques en France, ne retient, à l'origine, pour ces libertés que la sûreté, les libertés corporelles et de déplacement, la liberté d'opinion, la liberté religieuse, les libertés de la presse, la liberté d'enseignement, les libertés de réunion, de rassemblement et d'association. Toutes ces libertés relèvent du droit administratif et apparaissent comme des concessions ou des limites arrachées à l'administration par le Conseil d'État, marginalisant ainsi le juge judiciaire même lorsque la Constitution[22] lui confie expressément la sauvegarde de la liberté individuelle[23].

Déjà en 1906, sous la III^e^ République, Jean Cruet[24] écrivait : « *L'arbitraire, dans une certaine mesure, c'est la liberté de l'administration. Mais il ne convient pas que la liberté de l'administration puisse porter atteinte aux libertés des administrés* ». Avec la V^e^ République, le Conseil d'État, pour les actes règlementaires, et le Conseil constitutionnel, pour la loi, veillent au respect de la liberté des administrés et des individus, s'attachant à respecter une juste proportionnalité entre restriction des libertés et préservation ou sauvegarde des intérêts généraux[25].

Cet équilibre précaire peut être remis en cause par l'informatique, outil protéiforme et omniprésent dans notre société. Le développement de l'informatique et les possibilités supposées de rapprochement d'informations personnelles, en utilisant les connexions entre bases de données, ont été à l'origine de la première loi française associant l'informatique et la protection des libertés[26] dès 1978. Depuis, l'Union européenne s'est également dotée d'instruments juridiques pour protéger ces libertés[27]. Mais dans une société fortement

---

[21] Jean Rivero, Hugues Moutouh, *Libertés publiques*, Tome 1, 9^e^ édition mise à jour, juillet 2003, Presses universitaires de France, pp. 17-18.

[22] Constitution du 4 octobre 1958, Titre VIII : De l'autorité judiciaire, article 66 : « *Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi ».*

[23] D'après Louis Favoreu, *Droit des libertés fondamentales*, Précis Dalloz 5e édition, Introduction, pp. 1 et suivantes.

[24] Jean Cruet, *Étude juridique de l'Arbitraire Gouvernemental et Administratif, Des cas où l'autorité gouvernementale et administrative n'est pas tenue, sous des sanctions efficaces, de respecter les droits individuels et la légalité,* Librairie Nouvelle de Droit et de Jurisprudence, Arthur Rousseau, 1906.

[25] Lire à ce sujet Pierre Mazeaud, *La lutte contre le terrorisme dans la jurisprudence du Conseil constitutionnel*, Visite à la cour suprême du Canada, 24 au 26 avril 2006.

[26] Loi n^o^ 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, parue au journal officiel de la République française du 7 janvier 1978 p. 227.

[27] 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*, publiée au Journal officiel n^o^ L 281 du 23/11/1995 pp. 31-50, remplacée à partir de 2018 par le Règlement

influencée par les techniques numériques et la prolifération des acteurs internationaux sur ce secteur technique et commercial, les libertés publiques et les libertés privées acquises lentement depuis le XVIII[e] siècle en France, connaissent une pression importante et font l'objet d'un enjeu mondial et commercial, enjeu renforcé par la primauté des États-Unis d'Amérique[28] dans la gestion effective de l'Internet[29] ou de la fourniture des services associés[30]. Si certaines de ces libertés profitent des évolutions de la technique et peuvent mieux s'épanouir, d'autres sont remises en cause. Face à la pression et la progression de la technique, les protections développées progressivement par une société industrielle, centralisée et administrative, peuvent-elles défendre et protéger les individus et les États, dans une société en réseau, mondialisée et virtuelle ? Dans une société numérique en évolution constante, le droit, mais aussi l'individu, doivent évoluer pour continuer d'exister et ne pas être contraints à subir une complète remise en cause.

(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).*

[28] Charles Kupchan, *Comment l'Europe va sauver l'Amérique,* Éditions Saint-Simon, 2004 cité dans « Lectures signalées », *Politique américaine*, 2005/1 (N° 1), pp. 125-135. URL : https://www.cairn.info/revue-politique-americaine-2005-1-page-125.htm, consulté le 21 novembre 2017.
Jean-Jacques Lavenue, « Internalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberespace confronté à la notion d'ordre public », *Les Electronica,* vol 11, n° 2 (Automne / Fall 2006).
Jean-Jacques Lavenue, « Internet : efficacité des poursuites et ordre public international », Irène Bouhadana, Willliam Gilles (sous la direction de), *Cybercriminalité cybermenaces & cyberfraudes*, Les éditions IMODEV, mars 2012, pp.84-91.

[29] Au travers de *l'Internet Corporation for Assigned Names and Numbers* (ICANN), en français, la Société pour l'attribution des noms de domaine et des numéros sur Internet, société de droit californien à but non lucratif, ayant pour principales missions d'administrer les ressources numériques d'Internet, tels que l'adressage IP et les noms de domaines de premier niveau (*top level domain* ou TLD), et de coordonner les acteurs techniques.

[30] Les principaux acteurs et fournisseurs de services sur Internet sont des sociétés de droit américain : Google, YAHOO!, Facebook, Twitter, Amazon ou Microsoft pour ne citer que les plus importantes et omniprésentes, même si en Asie de nouveaux géants sont en cours de colonisation des pays occidentaux, les BAT (Baidu, Alibaba et Tencent). Lire à ce sujet Paul Pichot, Léa Desrayaud et Marianne Boyer, « Internet : les géants chinois se sont éveillés », *Le Monde.fr Entreprises,* 22 septembre 2017, URL : http://www.lemonde.fr/entreprises/visuel/2017/09/22/internet-les-geants-chinois-se-sont-eveilles_5189788_1656994.html, consulté le 30 novembre 2017.

Section 1. Le droit et la société numérique

À la fin du XX[e] siècle, avec l'apparition de la toile[31], les internautes ont découvert un nouvel espace de communication puissant et international, se jouant des frontières, mais cet espace ouvert, conçu par des universitaires libertaires[32], n'a pas été conçu comme un espace sécurisé et, à ce titre, son utilisation peut réduire, voire anéantir, certaines libertés (secret des correspondances, intimité, vie sexuelle, …). Il peut, à l'opposé, être utilisé pour contrer un État policier et organiser des réunions, voire des manifestations prérévolutionnaires, comme ce fut le cas en Tunisie et en Égypte au printemps 2011[33], par l'intermédiaire des réseaux sociaux et leur capacité de diffusion rapide. De plus, la généralisation de la dématérialisation de nombreux documents, la vidéosurveillance et la vulgarisation de certaines techniques, initialement militaires, comme le GPS[34], peuvent venir réduire cet espace de liberté individuelle.

Mais le cyberespace, l'espace numérique dématérialisé, n'est pas un espace de liberté[35] où le droit des États ne s'applique pas, comme le préconisaient les universitaires et chercheurs[36], premiers utilisateurs et concepteurs du réseau Internet. Le droit commun s'applique ou tente de s'appliquer à cet espace mouvant et international, et quelques particularités y ont incité le législateur à introduire des règles spéciales tenant compte de cette spécificité telles que la protection des données personnelles et de la vie privée, la sécurisation et l'adaptation des règles des transactions électroniques, la valorisation de la propriété intellectuelle, la lutte contre les contenus et les comportements illicites et l'adaptation de la réglementation des communications et des services en ligne à la convergence entre l'informatique, l'audiovisuel et les télécommunications[37]. Les droits fondamentaux protégés par les textes et les institutions mis en

---

[31] En anglais, *web. Spider web* correspond à la toile d'araignée, allusion au réseau Internet maillé et non hiérarchique.

[32] John Perry Barlow, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation,* February 8, 1996, URL : https://projects.eff.org/~barlow/Declaration-Final.html, consulté le 21 novembre 2017.

[33] Yves Gonzalez-Quijano, « Internet, le "Printemps arabe" et la dévaluation du cyberactivisme arabe », *Égypte/Monde arabe*, 2015/1 (n° 12), pp. 67-84. URL : https://www.cairn.info/revue-egypte-monde-arabe-2015-1-page-67.htm, consulté le 21 novembre 2017.

[34] Global Positioning System.

[35] Isabelle Falque-Pierrotin, « La Constitution et l'Internet », *Les Nouveaux Cahiers du Conseil constitutionnel*, 2012/3 (N° 36), pp. 31-44. DOI : 10.3917/nccc.036.0031. URL : https://www.cairn.info/revue-nouveaux-cahiers-conseil-constitutionnel-2012-3-page-31.htm, consulté le 21 novembre 2017.

[36] John Perry Barlow, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation,* February 8, 1996, Op. cit.

[37] Jean-François Théry, Isabelle Falque Pierrotin, *Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998,* Conseil d'État. Section du rapport et des études, Publié à la documentation française, décembre 1998.

place depuis la Révolution française restent protégés par ces mêmes textes[38] et institutions, mais certains organes, spécifiques au numérique, ont vu le jour et sont venus compléter cet arsenal de défense de nos libertés.

La généralisation de l'informatique et la numérisation de la société accompagnée de la dématérialisation des documents courants voient aussi se propager une nouvelle délinquance : la cybercriminalité[39]. Les cyberattaques sont dirigées autant contre l'individu que contre la société, voire les États. En accédant à certaines informations confidentielles ou en rendant ces informations inaccessibles, les cyberattaquants peuvent agir sur des négociations économiques ou politiques, ou sur les individus ou les sociétés par pression, chantage ou diffamation, voire même affecter nos démocraties en interférant dans les processus électifs[40]. La société numérique a-t-elle les moyens et les capacités de préserver les libertés ainsi attaquées et fragilisées, ou doit-elle faire évoluer ses méthodes pour conserver un espace de liberté hérité d'un courant de pensée du XVIIIe siècle en provenance d'Europe et d'Amérique ?

Sous-section 1. Le droit commun, droit applicable à l'Internet et aux techniques numériques

Avec l'apparition du cyberespace, la question du droit applicable à cet espace nouveau, international et protéiforme s'est posée[41]. Les chercheurs, à l'origine de la construction d'Internet, militaient pour une auto-régulation du réseau hors des gouvernements[42]. Ils

---

[38] Comme l'écrivait Jean Rivero : « *Le statut des libertés publiques, tout d'abord, procède directement d'une idéologie qui s'intègre de plus en plus directement au droit positif national et international ». (*Cité par Hugues Moutouh, Préface, Jean Rivero, Hugues Moutouh, *Libertés publiques,* Tome 1, 9e édition mise à jour, juillet 2003, Presses universitaires de France,).

[39] Irène Bouhadana, William Gilles, « Introduction – cyberspace, cybercriminalité & libertés », Irène Bouhadana, William Gilles (sous la direction de), *Cybercriminalité, cybermenaces & cyberfraudes,* Les éditions IMODEV, Mars 2012, pp. 4-5.

[40] Les services secrets américains ont établi que la Russie avait tenté par des cyberattaques d'influencer le résultat des élections présidentielles de 2016. À ce sujet, « Piratages durant l'élection présidentielle : Barack Obama annonce des représailles contre la Russie » dans le *Huffington Post*, article du 16 décembre 2016, à http://www.huffingtonpost.fr/2016/12/16/piratages-election-presidentielle-americaine-etats-unis-barack-obama-represailles-russie-vladimir-poutine/, consulté le 16 janvier 2017.

[41] Marie-Charlotte Roques-Bonnet, *Le droit peut-il ignorer la révolution culturelle ?* Michalon éditions, 2010.

[42] "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*" (John Perry Barlow, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation*, February 8, 1996, déjà cite). En français : « Gouvernements du Monde Industriel, géants fatigués de chair et d'acier, je viens du Cyberespace, la nouvelle demeure de l'Esprit. Au nom de l'avenir, je vous demande du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté là où nous nous réunissons » (traduction de l'auteur).

souhaitaient pour le cyberespace, un monde sans privilèges liés au pouvoir économique, à la race ou à la puissance, un monde sans contraintes extérieures. Le législateur devait-il laisser cet espace s'autoréguler ou au contraire, cet espace devait-il être régi par une législation, ordinaire ou spéciale ?

Dès 1998, le Conseil d'État[43] précise que « *contrairement à ce que l'on entend parfois, l'ensemble de la législation existante s'applique aux acteurs d'Internet, notamment les règles de protection du consommateur et celles qui garantissent le respect de l'ordre public. Il n'existe pas et il n'est nul besoin d'un droit spécifique des réseaux* ». Ainsi, le Conseil d'État confirme que l'Internet n'est pas une zone de non-droit, que la législation communautaire ou nationale existante s'applique aux activités de l'Internet.

En 2004, lors de l'examen de la loi pour la confiance dans l'économie numérique[44], la prise en compte des spécificités de l'Internet s'est posée. Le délai de prescription en cas de diffamation commence à la date de la première publication de l'information diffamatoire[45], le Parlement souhaitait faire commencer ce délai à la date de cessation de la publication en cas d'utilisation d'Internet. Saisi sur ce point, le Conseil constitutionnel[46] a accepté la possibilité d'un traitement différent entre la chose écrite sur papier et la chose publiée électroniquement, mais ce traitement ne devait pas être manifestement disproportionné entre ces deux modes de publication[47]. Ainsi le droit positif et la jurisprudence s'appliquent à Internet[48] même si certains ajustements s'avèrent nécessaires.

Le rapport de 1998[49] du Conseil d'État ajoute cependant que : « *compte tenu des limites inhérentes à toute initiative purement nationale, la coopération internationale des États est*

---

[43] Jean-François Théry, Isabelle Falque Pierrotin, *Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998,* Conseil d'État. Section du rapport et des études, Publié à la documentation française, décembre 1998.

[44] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique*, publiée au JORF nº 143 du 22 juin 2004 p. 11168.

[45] Loi du 29 juillet 1881 *sur la liberté de la presse*, art. 65.

[46] Conseil constitutionnel, Décision nº 2004-496 DC du 10 juin 2004 - *Loi pour la confiance dans l'économie numérique*. Journal officiel du 22 juin 2004, p. 11182.

[47] *« par elle-même, la prise en compte de différences dans les conditions d'accessibilité d'un message dans le temps, selon qu'il est publié sur un support papier ou qu'il est disponible sur un support informatique, n'est pas contraire au principe d'égalité ; que, toutefois, la différence de régime instaurée, en matière de droit de réponse et de prescription, par les dispositions critiquées dépasse manifestement ce qui serait nécessaire pour prendre en compte la situation particulière des messages exclusivement disponibles sur un support informatique* » (Conseil constitutionnel, décision nº 2004-496 DC *Loi pour la confiance dans l'économie numérique,* considérant n° 14).

[48] Nicolas Brault, « Le droit applicable à Internet. De l'abîme aux sommets », *LEGICOM*, 1996/2 (N° 12), pp. 1-15. URL : https://www.cairn.info/revue-legicom-1996-2-page-1.htm, consulte le 24 novembre 2017.

[49] Jean-François Théry, Isabelle Falque Pierrotin, Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998, Op. cit.

nécessaire pour faire respecter l'intérêt public dans un espace largement dominé par l'initiative privée ». Une coopération internationale[50] est nécessaire pour légiférer concrètement et efficacement sur Internet. Elle est également nécessaire pour arbitrer entre l'intérêt général, défendu par les États, et l'intérêt particulier des sociétés privées souhaitant profiter d'une valeur ajoutée inhérente à ce cyberespace. Si notre législation sait protéger l'intérêt public à l'intérieur de nos frontières, cette législation n'a pas été conçue pour faire face à une pression mondiale due à un réseau pour lequel les frontières des États ne jouent pas leur rôle protecteur. Face à ce double défi, techniques nouvelles et réseau ouvert et mondial, des adaptations législatives spécifiques sont parfois nécessaires.

Sous-section 2. Le droit spécial, droit adapté aux spécificités du numérique

La France, dès 1978, avec la loi informatique et libertés[51], a développé un droit spécial concernant la sphère informatique en cours d'élaboration, et a créé une autorité administrative indépendante[52], la Commission nationale de l'informatique et des libertés ou CNIL, chargée de proposer des règles concernant cette activité. La loi informatique et libertés a aussi donné à la CNIL un pouvoir de sanction.

En 1995, l'Union européenne généralise le besoin d'une telle autorité de contrôle dans tous les pays de l'Union[53]. L'ensemble des autorités de protection des données personnelles forme le groupe de travail « article 29 » ou G29, du nom de l'article qui prévoit cette coordination. En 2016, l'Union européenne adopte le Règlement général sur la protection des données[54]. Le groupe de travail G29 devient le Comité européen de la protection des données. Il est institué en tant qu'organe de l'Union avec personnalité juridique[55].

---

[50] Grant Gross, « International Cooperation Needed to Create an "Increasingly Beneficial Internet" », 27 février 2018, *Global Internet And Jurisdiction Conference 2018,* URL: https://www.internetsociety.org/blog/2018/02/international-cooperation-needed-create-increasingly-beneficial-internet/ consulté le 30 mars 2018.

[51] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* publiée au JORF du 7 janvier 1978 p. 227.

[52] CNIL Commission nationale de l'informatique et des libertés créée par la loi du 6 janvier 1978, articles 11 à 21.

[53] Avec la 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.*

[54] 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).

[55] Règlement (UE) 2016/679, art. 68 al.1.

En 1978, est aussi promulguée une loi qui tente d'améliorer les relations entre l'administration et le public et qui définit la liberté d'accès aux documents administratifs et la réutilisation des informations publiques[56]. Cette loi nº 78-753 du 17 juillet 1978[57] crée aussi une autre autorité administrative : la commission d'accès aux documents administratifs, ou CADA, chargée de statuer sur les refus de l'Administration de communiquer des documents administratifs. Cette communication de documents administratifs prend une nouvelle dimension[58] avec la dématérialisation desdits documents et l'accès à de nombreux documents directement par Internet sans demande spéciale aux administrations productrices[59]. L'interconnexion avec Internet des bases de données administratives a rendu effectivement possible l'accès aux données publiques par le plus grand nombre de citoyens[60] et a entraîné une transformation des pratiques administratives[61]. En 2016, la loi pour une République numérique[62] prévoit un rapprochement de la CNIL et de la CADA par une réunion à l'initiative de leurs présidents[63]. D'autres textes sont adoptés en France, concernant exclusivement le monde numérique : une loi sur le commerce électronique[64], une loi sur la signature électronique[65], une loi sur les noms

[56] Joumana Boustany, « Accès et réutilisation des données publiques. État des lieux en France », *Les Cahiers du numérique*, 2013/1 (Vol. 9), pp. 21-37.
[57] Loi nº 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*, publiée au JORF du 18 juillet 1978 p. 2851.
[58] Marcel Moritz, « Entre idéal de neutralité technologique et réalité d'une mutation sémantique : analyse des catégories juridiques du droit français de la communication ». Irène Bouhadana, William Gilles (dir.), *Revue Internationale de droit des données et du numérique*, volume 1, mars 2017, pp. 31-42, URL : http://ojs.imodev.org/index.php/RIDDN/article/view/148 consulté le 29 mars 2018.
[59] Cornu Marie, « Le statut des archives publiques dans le discours d'ouverture des données : de la formalisation d'un droit d'accès à l'émergence d'un droit d'exploiter la donnée », *LEGICOM*, 2016/1 (N° 56), pp. 41-49.
[60] Samuel Goëta, Clément Mabi, « L'open data peut-il (encore) servir les citoyens ? », *Mouvements*, 2014/3 (n° 79), pp. 81-91. URL : https://www.cairn.info/revue-mouvements-2014-3-page-81.htm consulté le 24 novembre 2017.
[61] Yann Algan, Maya Bacache-Beauvallet, Anne Perrot, « Administration numérique », *Notes du conseil d'analyse économique*, 2016/7 (n° 34), pp. 1-12. URL : https://www.cairn.info/revue-notes-du-conseil-d-analyse-economique-2016-7-page-1.htm consulté le 24 novembre 2017.
[62] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique* publiée au JORF n°0235 du 8 octobre 2016.
[63] Loi n° 2016-1321 du 7 octobre 2016, art. 26 et 28.
[64] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique,* Titre II Du commerce électronique, publiée au JORF nº143 du 22 juin 2004 p. 11168
[65] Loi nº 2000-230 du 13 mars 2000 *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* publiée au JORF nº62 du 14 mars 2000 p. 3968

de domaine[66], les lois protégeant la création sur Internet HADOPI 1 et HADOPI 2[67], elles-mêmes précédées d'une loi DADVSI[68].

L'Union européenne a elle-même légiféré sur le domaine : directive sur la signature électronique[69], directive sur le commerce électronique[70], directive sur les données personnelles[71]. Ces directives ayant été transposées dans la législation des pays membres ont abouti à une certaine harmonisation des législations au sein des pays membres de l'Union européenne.

Ces textes spéciaux ont tous pour but de limiter et restreindre les conséquences de l'utilisation de l'Internet, ou des techniques numériques, afin de protéger des droits préexistants à l'expansion des techniques numériques, droits remis en cause par ces nouvelles technologies : droit d'auteur, propriété intellectuelle, et aussi droits de la personne et libertés fondamentales. Mais, ces textes ont aussi pour but d'introduire, dans le droit commun, certaines spécificités du numérique. Le Code civil est ainsi modifié pour assurer la validité de la signature électronique et son équivalence avec la signature papier[72].

Avec la généralisation des techniques numériques, le droit, les pratiques administratives évoluent. L'individu doit être protégé face à une technologie invasive dans sa vie privée, mais les transformations de l'État lui offrent de nouvelles possibilités de participation citoyenne.

---

[66] Loi n° 2011-302 du 22 mars 2011 *portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques,* Chapitre III : Dispositions relatives aux communications électroniques publiée au JORF n°0069 du 23 mars 2011 p. 5186.

[67] Loi n° 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur Internet,* publiée au JORF n°0135 du 13 juin 2009 p. 9666.
Loi n° 2009-1 311 du 28 octobre 2009 *relative à la protection pénale de la propriété littéraire et artistique sur Internet* publiée au JORF n°0251 du 29 octobre 2009 p. 18290.

[68] Loi n° 2006-961 du 1 août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information* publiée au JORF n°178 du 3 août 2006 p. 11529.

[69] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999*, sur un cadre communautaire pour les signatures électroniques* publiée au JO L 13 du 19.1.2000, pp. 12–20.

[70] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000, *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« directive sur le commerce électronique ») publiée au Journal officiel n° L 178 du 17/07/2000 pp. 1-16.

[71] 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* publiée au Journal officiel n° L 281 du 23/11/1995 pp. 31-50.

[72] Code civil, Article 1316-4 créé par la loi no 2000-230 du 13 mars 2000 *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, publiée au JORF n°62 du 14 mars 2000 p. 3968.

Section 2. Les adaptations des individus et de l'État la société numérique

Les atteintes aux libertés peuvent provenir des atteintes à la vie privée des individus, atteintes liées à la divulgation de données à caractère personnel. Comme en matière de protection des ordinateurs contre les virus ou autres vers informatiques, l'individu est souvent lui-même le « maillon faible » de la protection de ses données à caractère personnel et de sa sécurité. Cette faille de protection est due à un comportement et une exposition non contrôlés[73].

L'exposition de la vie privée est réalisée au travers des données fournies par les utilisateurs des applications proposées sur Internet, soit lors de l'inscription, soit ultérieurement, lors de l'utilisation de ces applications, par exemple par une inscription sur le mur de Facebook. Les réseaux sociaux, mais également de manière croissante tout un ensemble de services, reposent aujourd'hui sur l'exploitation de ces informations, générées involontairement, mais aussi très largement « données » volontairement, et leur restitution aux usagers reste souvent partielle sous des formes diversement travaillées et enrichies. Cette transformation et la restitution de la transformation confèrent à ces services sens et valeur pour les individus eux-mêmes[74].

Face à cette exposition de la vie privée par la fourniture volontaire ou la collecte insidieuse des données à caractère personnel, de nombreux organismes, le Conseil de l'Europe, la Commission nationale de l'informatique et des libertés, fournissent des conseils et des manuels de bonne conduite à respecter pour éviter l'exposition involontaire de la vie privée[75]. Mais, comme pour

---

[73] « *Lors de ses travaux, la mission d'information a été frappée à plusieurs reprises par le fait que, de plus en plus, les citoyens exposent leur vie privée sur Internet, notamment les plus jeunes, et qu'ils le font sans en avoir toujours conscience. Quand ils en prennent conscience et souhaitent mieux protéger leurs droits, ces internautes sont confrontés à des difficultés techniques et juridiques et se retrouvent alors relativement isolés face aux grands groupes de l'Internet, que sont Google, Facebook ou Twitter* » (extrait de Patrick Bloche, Patrick Verchère, *Rapport d'information déposé par la mission d'information commune sur les droits de l'individu dans la révolution numérique*, enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011, p.123).

[74] Viktor Mayer-Schönberger, « La révolution Big Data », *Politique étrangère*, 2014/4 (Hiver), pp. 69-81. URL : https://www.cairn.info/revue-politique-etrangere-2014-4-page-69.htm consulté le 30 mars 2018.

[75] CNIL, *Maîtriser mes données,* à https://www.cnil.fr/fr/maitriser-mes-donnees, consulté le 25 novembre 2017 ; CNIL, *Protéger ses données personnelles sur Facebook : les conseils pour agir,* 28 janvier 2014, à https://www.cnil.fr/fr/proteger-ses-donnees-personnelles-sur-facebook-les-conseils-pour-agir, consulté le 25 novembre 2017 ; CNIL, *10 conseils pour rester net sur le Web,* 7 mars 2016, à https://www.cnil.fr/fr/10-conseils-pour-rester-net-sur-le-web, consulté le 25 novembre 2016 ; CNIL, « Guide La sécurité des données personnelles », *Les guides de la CNIL,* 2010.
Council of Europe, "Protecting private life" In *Council of Europe Data Protection website,* URL : https://www.coe.int/en/web/data-protection/home consulté le 30 mars 2018.
Clémence Jost et Bruno Texier, « Comment mieux protéger vos données personnelles ? », *archimag*, 19 janvier 2017, URL : http://www.archimag.com/univers-data/2017/01/19/10-conseils-outils-indispensables-proteger-donnees-personnelles, consulté le 25 novembre 2017.

la protection des ordinateurs personnels contre les vers, virus ou chevaux de Troie, ces conseils sont peu ou prou respectés, voire mal connus. La Commission de l'informatique et des libertés a publié en 2014, une fiche pratique concernant la publication de photos sur le réseau[76] et la gendarmerie nationale met en garde les parents publiant des photos de leurs enfants sur les réseaux sociaux[77]. Ces recommandations visent à modifier l'attitude des individus face à un moyen de publication puissant et mal contrôlé.

Aujourd'hui, avec l'Internet des objets, ce sont des données relatives à la santé et à la condition physiques des individus qui vont se retrouver sur Internet[78] et faire l'objet d'enjeux mercantiles. Cette migration technologique qui met en relation les objets de la vie courante, va rendre prioritaire la protection de la vie privée[79].

La sensibilisation des individus devient nécessaire tant au niveau des adultes que des enfants dans les écoles pour améliorer la protection des libertés[80]. L'individu doit être capable d'évaluer les risques liés à son attitude et pouvoir décider en fonction des avantages obtenus en retour quels pans de sa vie privée et intime il souhaite ou accepte d'exposer.

Dès 1978 le Parlement a régulé la protection des données personnelles avec la loi informatique et libertés[81]. La protection des données à caractère personnel, mise en place initialement à cause d'une prémonition de risques administratifs, a vu avec l'apparition et le développement d'Internet son centre de gravité se mouvoir vers des entreprises privées avec la loi pour la confiance dans l'économie numérique[82] et récemment avec le Règlement général sur la protection des données[83].

---

[76] CNIL, *Les conseils de la CNIL pour mieux maîtriser la publication de photos*, 13 octobre 2014, à https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mieux-maitriser-la-publication-de-photos-0, consulté le 7 juillet 2016.

[77] Lire à ce sujet Hortense Nicolet, « Poster des photos de ses enfants sur Facebook n'est pas sans danger », *Le Figaro.fr madame*, 15 février 2015, URL : http://madame.lefigaro.fr/societe/pourquoi-il-faut-cesser-de-poster-des-photos-de-ses-enfants-mineurs-sur-facebook-011215, consulté le 25 novembre 2017.

[78] Magali Léo, « Patient connecté et données de santé : les vrais risques », *I2D – Information, données & documents*, 2016/3 (Volume 53), pp. 65-66.

[79] Bernard Benhamou, « L'Internet des objets. Défis technologiques, économiques et politiques », *Esprit*, 2009/3 (Mars/avril), pp. 137-150. URL : https://www.cairn.info/revue-esprit-2009-3-page-137.htm consulté le 24 novembre 2017.

[80] Odile Naudin, « Internet : former les parents autant que leurs enfants », *Après-demain*, 2009/1 (N ° 9, NF), pp. 39-44.

[81] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*.

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

[83] 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).*

Sous-section 1. La protection nécessaire de l'individu dans la société numérique

En France, le grand public a pris conscience de l'informatisation de la société à partir des années 1980 avec les expériences du vidéotex de Vélizy, puis du minitel[84] mis à disposition du public gratuitement par la Direction générale des Télécommunications[85] ou DGT. La première application numérique orientée grand public est l'annuaire électronique[86]. À partir d'un petit terminal, le minitel, tout abonné au téléphone peut rechercher le numéro de téléphone de n'importe quel autre abonné dans la France entière, hors abonnés en liste rouge. La technique numérique permet de s'affranchir de la limite des départements qui était la règle avec l'annuaire papier[87]. De plus, les critères de recherche sont étendus et ces recherches sont donc plus faciles : recherche d'un abonné avec extension orthographique du nom, extension d'une recherche aux communes limitrophes ou à l'ensemble du département, recherche des abonnés d'une rue ou d'un immeuble, etc. Ainsi, dès 1985, l'annuaire électronique modifie les habitudes des abonnés au téléphone. Des individus recherchent des cousins perdus de vue. Certaines sociétés créent des fichiers de prospection commerciale en collectant les adresses privées ou professionnelles disponibles gratuitement. À l'époque, la DGT renonce à une recherche d'un abonné sur l'ensemble du territoire français et ne met pas en service public la recherche inversée[88]. La seule protection disponible pour l'usager est de demander à être mis en liste rouge, c'est-à-dire à ne pas figurer dans la liste des résultats d'une requête. Ce service est alors facturé par la DGT et peut être assimilé à un droit à être non référencé.

En parallèle au développement du minitel, L'informatique se développe depuis les années 1970. Les techniques informatiques sont alors encore balbutiantes, les bases de données sont de gros fichiers hiérarchiquement organisés et les réseaux commencent à relier les sites d'un même

[84] Jean Harivel, « Le minitel, une exception française », Irène Bouhadana et William Gilles (sous la direction), *Revue de l'Institut du Monde et du Développement, RIMD* n° 4 – 2013 – Hiver/Winter, pp. 93-106.

[85] La Direction générale des télécommunications est renommée France Télécom le 1er janvier 1988, transformée en établissement de droit public par la loi n° 90-568 du 2 juillet 1990 *relative à l'organisation du service public de la poste et à France Télécom*, puis en société anonyme par la loi no 96-660 du 26 juillet 1996 *relative à l'entreprise nationale France Télécom*. Après l'ouverture au public de son capital en 1997 et le rachat d'ORANGE en 2000 puis 2003, le changement de nom du Groupe France Télécom en ORANGE est voté lors de l'assemblée générale du 28 mai 2013 et sera effectif au 1er juillet 2013. Op. cit.

[86] Inauguré en Ile et Vilaine le 5 mai 1983 avec une base de données régionale limitée aux abonnés du téléphone des départements bretons, et inauguré à Paris le 5 mai 1985, avec la base nationale des 23 millions d'abonnés au téléphone.

[87] Seul l'annuaire papier du département de l'abonné au téléphone est distribué gratuitement.

[88] Recherche de l'identité d'un abonné dont seul le numéro de téléphone est connu.

constructeur entre eux. Le réseau Transpac[89] permet à des sites non homogènes de s'échanger des données, il sera livré à la Direction générale des Télécommunications au début des années 1980. IBM[90] ne commercialisera sa première base de données relationnelle qu'aux environs des années 1980[91].

Cependant, devant le risque de fichage généralisé des individus et l'utilisation d'un identifiant unique, le numéro de sécurité sociale, pour relier les différents fichiers administratifs, les députés français, sous la pression de l'opinion publique et des médias[92], vont voter dès le 6 janvier 1978, la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés[93]. Son article 1er précise : « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Pour la première fois, la société prend conscience d'un risque pour les libertés, lié à l'utilisation des techniques nouvelles qui sont en cours de développement. Ainsi, alors que l'informatique est encore « adolescente », la nécessité d'une coopération internationale est affirmée et les risques principaux liés à l'informatisation prévisible de la société sont l'atteinte aux droits de l'homme, à la vie privée et aux libertés individuelles ou publiques. Cette loi n° 78-17 est la première loi spéciale relative à l'informatique, technique récente dont le potentiel d'intrusion dans la société et la vie privée est ainsi mis sous contrôle. Les traitements relatifs aux données collectées et enregistrées par les sociétés et l'administration doivent être déclarés à la CNIL qui peut en refuser ou restreindre la mise en place. Cette loi crée de nouveaux droits[94] pour les personnes physiques quant au contrôle des traitements de leurs données, mais ces droits ne sont pas toujours connus par les personnes physiques concernées[95].

---

[89] Réseau de télécommunications qui véhicule les données par paquets (protocole X25). Inventé en 1976, commercialisé à partir de 1979, le réseau sera abandonné en 2011 par France Télécom (sources personnelles de l'auteur).

[90] IBM, ou *International Business Machines*, est dans les années 70-80 le premier fournisseur mondial d'ordinateurs. À l'époque, le matériel, ou hardware, est loué avec le système d'exploitation, créant une dépendance entre le client et le constructeur.

[91] Le système R, système de gestion de base de données relationnelles, a débuté comme projet de recherche dans les années 1970. Le premier client de *system R* a été Pratt & Whitney en 1977. (*IBM Research Laboratory,* "A History and Evaluation of System R", *Communications of the ACM,* October 1981, Volume 24, Number 10, pp. 632-646, URL: https://people.eecs.berkeley.edu/~brewer/cs262/SystemR.pdf consulté le 19 mars 2018).

[92] Philippe Boucher, « SAFARI ou la chasse aux Français », *Le Monde*, 21 mars 1974.

[93] Loi nº 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés*, publiée au JORF du 7 janvier 1978 p. 227.

[94] Droit d'information, droit d'opposition, droits d'accès et de rectification.

[95] L'auteur peut aussi témoigner que cette loi n'est pas non plus connue des équipes informatiques qui développent les applications pour les entreprises.

Cette loi française concourt à l'élaboration de textes européens protégeant les données à caractère personnel. Le 23 septembre 1980, l'OCDE adopte les « *lignes directrices régissant la vie privée et le flux transfrontalières des données à caractère personnel* » qui énoncent divers principes de limitation en matière de collecte des données à caractère personnel obtenues par des moyens licites et après consentement de la personne concernée[96]. Ces lignes directrices sont établies pour harmoniser les législations, mais aussi ne pas entraver la libre circulation de ces données nécessaire à « d'importants secteurs de l'économie », banque et assurances.

Le 28 janvier 1981, le Conseil de l'Europe adopte la Convention internationale n° 108 consacrant les principes « informatique et libertés » inspirés de la loi française n° 78-17[97]. Dans son article 1er, le but de cette convention est « *de garantir […] à toute personne physique […] le respect de ses droits et de ses libertés fondamentales […] à l'égard du traitement automatisé des données à caractère personnel la concernant* ». La protection des données à caractère personnel se généralise ainsi en Europe, soit pour des raisons économiques et la libre circulation des données, soit pour défendre les droits des personnes physiques. Cette dualité d'objectifs reste présente dans les textes protecteurs qui, cependant, édictent les mêmes droits pour les personnes physiques.

Au niveau de la Communauté européenne, afin d'harmoniser les législations dans les États membres, une directive est publiée en 1995[98], dans son titre, la dualité protection des données et libre circulation de ces données est rappelé. Les droits des personnes physiques et la protection des données à caractère personnel sont dérivés de la loi n°78-17, des lignes directrices de l'OCDE et de la Convention n° 108. Les États membres se dotent ainsi d'une protection des données à caractère personnel contraignante et harmonisée.

---

[96] « *Compte tenu de l'essor pris par le traitement automatique de l'information, qui permet de transmettre de vastes quantités de données en quelques secondes à travers les frontières nationales et même à travers les continents, il a fallu étudier la question de la protection de la vie privée sous l'angle des données de caractère personnel. Des législations relatives à la protection de la vie privée ont été adoptées ou le seront prochainement dans près de la moitié des pays de l'OCDE (l'Allemagne, l'Autriche, le Canada, le Danemark, les États-Unis, la France, le Luxembourg, la Norvège et la Suède ont promulgué une législation. La Belgique, l'Espagne, les Pays-Bas et la Suisse ont établi des projets de loi) en vue de prévenir des actes considérés comme constituant des violations des droits fondamentaux de l'homme, tels que le stockage illicite de données de caractère personnel qui sont inexactes, l'utilisation abusive ou la divulgation non autorisée de ces données.* » (1er paragraphe de la préface, OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 1980*).

[97] Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »*, série des traités européens – n° 108, Strasbourg, 28 janvier 1981.

[98] 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.*

Depuis 1995, Internet s'est généralisé et les réseaux sociaux sont apparus. La généralisation du smartphone dans toutes les couches de la population et ses conséquences sur la vie privée imposent une refonte de la protection apportée par la Directive. En 2016, un nouveau règlement[99] est adopté après plusieurs années de discussions[100], il est approuvé par le Parlement européen début 2016 et doit être applicable le 25 mai 2018. Ce Règlement général sur la protection des données soumet la collecte des données à caractère personnel au consentement libre et éclairé de la personne physique concernée qui peut retirer son consentement à tout moment[101]. Il crée un nouveau droit à l'effacement des données[102] et encadre la sécurité des sites de stockage et de traitement desdites données[103]. Le règlement précise les règles de circulation des données entre responsables de traitement et sous-traitants[104] à l'intérieur du territoire de l'Union européenne, mais il laisse une marge de manœuvre aux États membres, rendant possible une renationalisation partielle de la protection des données personnelles, qui peut constituer un obstacle à la réalisation du marché unique numérique[105] source de valeurs ajoutées. La dualité protection de la vie personnelle et des données à caractère personnel et libre circulation de ces données reste donc présente.

La France, avec la loi pour une République numérique[106] a modifié la loi informatique et libertés, en introduisant le droit à l'oubli pour les données collectées auprès d'un enfant mineur, et a ajouté à l'article 1er de cette loi le droit pour toute personne de décider et contrôler les usages qui seront faits de ses données à caractère personnel, droit proche de la notion

[99] 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).*

[100] La Commission européenne a proposé de réformer la protection des données le 25 janvier 2012. Le 12 mars 2014, le Parlement européen manifeste son soutien au règlement général en séance plénière avec 621 votes pour, 10 votes contre et 22 abstentions. Le Parlement européen, le Conseil et la Commission parviennent à un accord sur le règlement général le 15 décembre 2015. Le règlement est publié au journal officiel de l'Union européenne le 24 mai 2016. (Source Le contrôleur européen de la protection des données, « Évolution historique du règlement général sur la protection des données », URL : https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_fr consulté le 19 mars 2018).

[101] Règlement (UE) 2016/679, article 7.

[102] Règlement (UE) 2016/679, article 17.

[103] Règlement (UE) 2016/679, article 32.

[104] Règlement (UE) 2016/679, articles 27-29.

[105] Catherine Barreau, « Le marché unique numérique et la régulation des données personnelles », *Annales des Mines - Réalités industrielles*, 2016/3 (Août 2016), pp. 37-41.

[106] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF n°0235 du 8 octobre 2016.

d'autodétermination informationnelle[107], introduisant dans le droit français ces notions prévues dans le règlement avant son application par les États membres.

La personne physique et les données à caractère personnel font l'objet de textes protecteurs[108], ces informations peuvent être utilisées pour réaliser une surveillance quasi permanente des individus. Avec les évolutions des techniques numériques, il devient possible de collationner et de recouper des informations concernant un individu. Aujourd'hui, il est aisé de localiser géographiquement un individu à partir de certains de ces actes (paiement par carte bancaire, utilisation des transports en commun avec utilisation de cartes RFID, utilisation de téléphone portable, caméra de vidéosurveillance…), mais également de capter sa correspondance privée, de connaître ses relations, et de collecter d'autres informations qui restaient, jusqu'à maintenant, propres à la sphère privée[109].

De fait, avec des techniques différentes de celles imaginées et décrites[110] par George Orwell[111], Big Brother[112] et sa surveillance omniprésente s'immisce dans notre monde moderne et numérique. Dans les centres commerciaux et les centres-villes, dans les transports en commun, dans les rues et les places des villes et villages, la surveillance des caméras de vidéoprotection[113], l'enregistrement des achats, la connaissance par les banques des revenus et des dépenses, le dévoilement des modes de vie et des centres d'intérêt par les paiements effectués avec une carte bancaire, tels sont les moyens de surveiller les personnes physiques[114]. En cas de disparition d'un individu, la localisation de son téléphone portable, les paiements et retraits effectués avec sa carte bancaire, permettent à l'enquête de rechercher sa trace éventuelle.

---

[107] CNIL, « La loi pour une République numérique et la protection des données personnelles », 2 décembre 2016, URL : http://www.cil.cnrs.fr/CIL/spip.php?article2902, consulté le 25 novembre 2017.

[108] Yves Poullet, « La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ? », *LEGICOM* 2009/1 (N° 42), pp. 47-69.

[109] Comme l'a révélé Edward Snowden en divulguant le programme PRISM des États-Unis d'Amérique en juin 2013. Lire sur le sujet Jean-Paul Deléage, « Avec Edward Snowden, l'homme sorti de l'ombre qui voulait éclairer le monde ! », *Ecologie & politique*, 2014/1 (N°48), pp. 5-12.

[110] Le télécran, plaque de métal oblongue, pouvait transmettre les sons et les images sans qu'il soit possible de savoir si on était surveillé, des hélicoptères pouvaient surveiller à l'intérieur des appartements (George Orwell, *1984*, premières pages).

[111] George Orwell, *1984, Editions* Secker and Warburg, 1949.

[112] "*Big Brother is watching you"* (en français : Big Brother vous regarde) tel est l'avertissement affiché sur les murs. (George Orwell, *1984*, premières pages).

[113] *Vidéosurveillance de la voie publique et des lieux ouverts au public*, Service-Public.fr, vérifié le 16 janvier 2017, URL : https://www.service-public.fr/particuliers/vosdroits/F2517, consulté le 25 novembre 2017.

[114] Gérald Berthoud, « L'horizon d'une surveillance omniprésente ? », *Revue européenne des sciences sociales*, 2002/2 (XL), p. 11.

Avec les techniques numériques, l'Allemagne Hitlérienne aurait pu contrôler les mouvements des individus et voir sa puissance de nuisance décuplée. L'étoile jaune, bien que visible, n'a pas la capacité de localisation d'une puce RFID, utilisée aujourd'hui pour suivre et assurer la traçabilité des bovins, ovins et autres porcins, voire des objets avec la venue de l'Internet des objets.

Mais, nos régimes démocratiques peuvent également connaître des dérives en utilisant ces moyens puissants et furtifs[115] mis à disposition grâce à la technologie numérique. Dans son livre[116], Alex Türk fait état d'un projet européen de géolocalisation des passagers dans les aéroports, le projet « *Op Tag* » dévoilé au public en 2006. Ce projet a été testé dans l'aéroport de Copenhague[117], mais il semble qu'il n'est pas mis en œuvre opérationnellement[118]. Couplée au réseau de vidéosurveillance, une puce RFID présente sur la carte d'embarquement doit permettre de repérer les voyageurs flâneurs dans l'aéroport, et qui retardent d'autant la procédure d'embarquement. Cet outil peut être facilement détourné de son usage primaire et devenir un outil policier très contraignant si aucun texte n'encadre son utilisation. Souvent, une invention humaine peut être utile pour la société, mais aussi utilisée contre la société. Ainsi, la fusion nucléaire est utilisée pour la production d'énergie électrique, mais peut aussi détruire l'humanité d'où la nécessité de non-prolifération de ces armes. La technologie est neutre[119], seules son utilisation et la politique peuvent en faire un outil de progrès ou de contrainte pour l'individu.

Les moyens modernes de surveillance peuvent aussi être utilisés à l'insu d'un individu par les forces de police et de gendarmerie dans le cadre des lois pour la sécurité et contre le terrorisme[120].

La personne physique ne doit pas être surveillée en permanence, cette surveillance permanente entrave sa liberté. Dans un État de droit, la sûreté présuppose que l'arbitraire ne réduise pas la

---

[115] Furtif, furtive (*adjectif, latin furtivus, dérobé, de fur, furis, voleur*) définition : qui se fait rapidement, à la dérobée, de manière à échapper à l'attention ; Littéraire. Qui passe rapidement, presque inaperçu : Des apparitions furtives ; Se dit d'un avion construit de manière à ne pouvoir être détecté que très difficilement par les radars. (Cf. Larousse, http://www.larousse.fr/dictionnaires/francais/furtif_furtive/35637 consulté le 5 mai 2012).

[116] Alex Tûrk, *La vie privée en péril, des citoyens sous contrôle,* Paris O. Jacob, 2011.

[117] Cécile Blanchard, *Localisation des passagers par RFID ou bluetooth testée à l'aéroport de Copenhague* 4 juin 2008, in ReseauxTelecom.net à http://www.reseaux-telecoms.net/actualites/lire-localisation-des-passagers-par-rfid-ou-bluetooth-testee-a-l-aeroport-de-copenhague-18282.html consulté le 5 mai 2012.

[118] Lire sur le sujet Janson Hui, « *RFID in Airports – Baggage and Passenger Tracking* », 8 juin 2008. URL : http://www.winmec.ucla.edu/rfid/course/2008s/RFID%20in%20Airports.pdf, consulte le 1er décembre 2017.

[119] Simone Manon, « La technologie est-elle une activité neutre ? », *Philolog Cours de philosophie,* 13 mars 2008, en ligne à http://www.philolog.fr/la-technique-est-elle-une-activite-neutre/, consulté le 25 novembre 2017.

[120] Paye Jean-Claude, « Lutte antiterroriste et contrôle de la vie privée », *Multitudes*, 2003/1 (no 11), pp. 91-105.

liberté d'aller et venir d'un individu. Mais pour jouir de sa liberté, le citoyen va demander à l'État de lui garantir une sécurité, sécurité contre les agressions extérieures, assurée traditionnellement par les forces armées, et sécurité contre les agressions aux personnes ou aux biens, assurée par les forces de police et de gendarmerie. Ce besoin de sécurité ne doit pas être échangé contre une restriction des libertés, comme le proclamait dès 1775 Benjamin Franklin[121].

Depuis le 11 septembre 2001, la lutte contre le terrorisme est devenue une préoccupation des États occidentaux et cette protection contre le terrorisme s'est trouvée assortie de nombreuses limites aux libertés des individus (liberté de circulation vers certains pays assortie d'une déclaration préalable, documents d'identité biométriques, restrictions aux libertés fondamentales avec les interceptions possibles des communications privées, etc.), voire de reniement de l'État de droit[122]. La sûreté des individus[123] n'est plus légalement garantie puisque si les indices convergent, un individu peut être arrêté, emprisonné ou assigné à résidence avant d'avoir commis une infraction liée au terrorisme s'il existe une forte suspicion de la préparation de cet acte[124].

Les techniques numériques, qui permettent des surveillances discrètes indécelables, ou difficilement décelables, permettent des atteintes aux libertés et à la vie privée des individus[125]. Le droit et la jurisprudence[126] doivent permettre de limiter et d'encadrer ces débordements facilités par les techniques numériques et la dématérialisation des échanges.

La société numérique présente des opportunités pour le développement de certaines libertés, liberté d'expression et liberté de la presse, liberté d'entreprise et d'établissement, mais elle fournit les moyens de surveillance des personnes physiques et, sous couvert de besoins sécuritaires, elle peut attenter aux libertés individuelles. Mais, sous la pression des techniques numériques permettant une meilleure information des citoyens, les gouvernements s'ouvrent à

---

[121] "*They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety*". Benjamin Franklin, Contributions to the Conference on February 17, 1775

[122] Colombe Camus, « La lutte contre le terrorisme dans les démocraties occidentales : État de droit et exceptionnalisme », *Revue internationale et stratégique*, 2007/2 (n° 66), pp. 9-24.

[123] La sûreté est définie comme un droit naturel et imprescriptible par l'article 2 de la déclaration des droits de l'homme et du citoyen de 1789.

[124] Code de la sécurité intérieure, art. L.228-1 à L.228-7.

[125] Comme révélé par Edward Snowden.

[126] Le Conseil constitutionnel et la Cour européenne des droits de l'homme analysent les restrictions apportées aux libertés en regard de l'intérêt général sur la base d'une juste proportionnalité entre restriction et objectif (Valérie Goesel-Le Bihan, « Le contrôle de proportionnalité dans la jurisprudence du Conseil constitutionnel : figures récentes », *Revue française de droit constitutionnel*, 2007/2 (n° 70), pp. 269-295. URL : https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2007-2-page-269.htm consulté le 19 mars 2018).

une participation citoyenne tant territoriale que nationale. Les individus adoptent également de nouvelles manières de communication. Le développement des techniques numériques entraîne une révolution et une mutation de la société[127].

Sous-section 2. Les adaptations de l'État dans la société numérique

La législation s'est adaptée ou est en cours d'adaptation à l'avènement du numérique. Cette adaptation a dû être effectuée en moins d'un demi-siècle, sous la pression d'une technique évoluant très rapidement. L'individu a vu son mode de vie profondément modifié en une vingtaine d'année. Sa vie privée n'est plus secrète, et il est possible de connaître ses actes, ses préférences, sa santé. Toutes ces mutations imposent de nouvelles normes de protection des individus, mais aussi une réaction rapide et adaptée à chaque nouvelle technique mise en œuvre. L'inertie réglementaire ou législative peut entraîner une dépossession des gouvernements de leur liberté de décision face aux pressions de sociétés commerciales qui disposent d'une meilleure réactivité, de plus d'autonomie et de moyens et peuvent interférer via un lobbying dans certaines décisions étatiques ou européennes[128].

La société elle-même connaît des mutations face à la révolution numérique. Gilles Babinet recense cinq domaines dont l'évolution en cours est liée au numérique[129] : la connaissance, l'éducation, la santé, la production et l'État. La mutation de l'État face à la « société de l'information » a commencé avec le gouvernement de Lionel Jospin[130]. Sous la présidence de François Hollande, la France a adhéré au partenariat pour un gouvernement ouvert le 24 avril 2014[131]. Lors de la préparation de la loi pour une République numérique, une consultation sur

[127] Rémy Rieffel, *Révolution numérique, révolution culturelle ?* Gallimard, 2014.
[128] Eleonore Pellé, « Heike Klüver, *Lobbying in the European Union: Interest Groups, Lobbying Coalitions, and Policy change*, Oxford, Oxford University Press, 2013, 278 pages. », *Politique européenne*, 2016/3 (n° 53), pp. 132-135.
[129] Gilles Babinet, *L'ère numérique, un nouvel âge de l'humanité – Cinq mutations qui vont bouleverser notre vie,* Le Passeur, 2014.
[130] Lionel Jospin, Discours à Hourtin, le 25 août 1995.
[131] En ouverture de la Conférence de Paris sur l'open data et le gouvernement ouvert, la ministre de la Décentralisation, de la Réforme de l'État et de la Fonction Publique a annoncé officiellement l'intention de la France d'adhérer au Partenariat pour un gouvernement ouvert (« La France rejoint le partenariat pour un gouvernement ouvert », *Le Portail de la modernisation de l'action publique*, 24 avril 2014, URL : http://www.modernisation.gouv.fr/laction-publique-se-transforme/en-ouvrant-les-donnees-publiques/france-rejoint-open-governement-partnership-ogp consulté le 20 mars 2018).

Internet a été organisée[132] pour recueillir des remarques et amendements sur le projet de loi avant son dépôt à l'Assemblée nationale. Ainsi après l'ouverture des données administratives, ou *Open Data* en anglais, une expérience de participation citoyenne[133] à l'élaboration des lois a été réalisée. Mais face à l'évolution rapide des techniques, l'élaboration des textes réglementant et encadrant les aspects numériques de la société doivent encore évoluer pour obtenir une adaptation permanente et rapide. Sans cette adaptation, la vie privée des individus risque de connaître des violations liées à des vols d'information sensible. La divulgation de certaines informations ou images a entraîné le suicide d'adolescents face à une perte d'image d'eux-mêmes ou un cyberharcèlement[134].

L'essor des technologies et des supports numériques est si fulgurant dans ces dernières années que ces technologies envahissent notre vie quotidienne, nos pratiques d'achat, notre santé. Elles envahissent aussi la vie professionnelle, les loisirs. Elles touchent aussi notre intimité et notre identité personnelle. Ces transformations affectent aussi l'État, l'administration, l'économie. Ces techniques peuvent être positives : Internet donne accès à une documentation incommensurable et permet l'accès à une information instantanée. Elles peuvent aussi avoir des conséquences négatives : la vie privée est exposée, tous les accès à Internet sont enregistrés mettant l'individu sous une surveillance permanente[135].

L'abolition des frontières amoindrit les protections légales existantes tant au niveau individuel qu'au niveau sociétal. Dans ce contexte, les libertés publiques et les libertés individuelles connaissent des mutations. La société doit continuer à faire vivre et évoluer ces libertés et les

---

[132] Consultation du 26 septembre 2015 au 18 octobre 2015, sur la plateforme www.republique-numerique.fr.

[133] Ank Michels, « Les innovations dans la gouvernance démocratique – En quoi la participation citoyenne contribue-t-elle à l'amélioration de la démocratie ? », *Revue Internationale des Sciences Administratives*, 2011/2 (Vol. 77), pp. 275-296.
Loïc Blondiaux, « Démocratie locale et participation citoyenne : la promesse et le piège », *Mouvements*, 2001/5 (nº18), pp. 44-51. URL : https://www.cairn.info/revue-mouvements-2001-5-page-44.htm consulté le 20 mars 2018.
Jean-Benoît Albertini, « Démocratie représentative et participation(s) citoyenne(s) : réflexions et applications pratiques », *Revue française d'administration publique*, 2014/2 (N° 150), pp. 529-541. URL : https://www.cairn.info/revue-francaise-d-administration-publique-2014-2-page-529.htm consulté le 20 mars 2018.

[134] « Canada : le suicide d'une ado harcelée bouleverse le pays », *Le Parisien*, 16 octobre 2012, en ligne à http://www.leparisien.fr/societe/canada-le-suicide-d-une-ado-harcelee-bouleverse-le-pays-14-10-2012-2231737.php, consulté le 1er décembre 2017.

[135] Yann Boutaric, « Surveillance d'Internet : votre vie privée en danger », *Contrepoints,* 15 janvier 2016, URL : https://www.contrepoints.org/2016/01/15/235489-surveillance-dinternet-votre-vie-privee-en-danger consulté le 18 mars 2018.
Xavier Niel, Dominique Roux, « La révolution internet », dans *Les 100 mots de l'internet.* Paris, Presses Universitaires de France, « Que sais-je ? », 2010, pp. 3-10. URL : https://www.cairn.info/les-100-mots-de-l-internet--9782130578956-page-3.htm consulté le 18 mars 2018.

protéger. Cette protection peut connaître des atténuations liées à l'intérêt général, ces altérations doivent être prévues par la loi et rester en adéquation avec le but poursuivi[136].

Dans une première partie, la protection des libertés, mais aussi les restrictions légales relatives à ces libertés sont étudiées dans l'environnement numérique : protection et encadrement par la loi ; loi générale ou loi spéciale. Les atteintes potentielles aux libertés liées à la surveillance des individus, surveillance mercantile ou surveillance étatique pour des besoins sécuritaires, sont analysées en regard des moyens de protection existant. Dans une seconde partie, l'atteinte aux libertés et les avancées démocratiques en termes de coopération citoyenne sont étudiées en regard de la mutation rapide de la société numérique. Enfin, le besoin d'un changement de paradigme législatif ou réglementaire nécessaire à une réaction rapide face à l'évolution des techniques est analysé.

Bien que l'objectif de ce document ne soit pas de faire une analyse détaillée du cadre juridique national, européen et international, compte tenu du caractère mondial de la société numérique et de l'Internet, certaines spécificités européennes ou américaines seront utilisées pour expliciter certains aspects légaux et leurs conséquences.

[136] *« Cette ingérence poursuivait des buts légitimes, à savoir la protection de la sécurité nationale, de la sûreté publique et des droits des victimes, ainsi que la prévention des infractions pénales. Elle était également proportionnée »* (Cour européenne des droits de l'homme, Arrêt du 2 septembre 2010, Affaire 35623/05 *Uzun c/ Allemagne)*.

Partie 1. Les libertés dans la société numérique

La Révolution française a été précédée tout au long du « siècle des Lumières », en réaction à un pouvoir royal absolu, d'un bouillonnement d'idées qui a remis en cause l'ordre établi, et a vu la notion de liberté défendue dans les écrits des philosophes[137], jusqu'à sa conceptualisation formulée dans la « Déclaration des droits de l'homme et du citoyen » adoptée le 26 août 1789 par l'Assemblée constituante[138]. Les libertés publiques ont été progressivement consolidées depuis le XVIII^{e} siècle au travers des Constitutions successives en France[139], la législation a encadré leurs contours par des lois contraignantes ou au contraire libérales. En France, les principes du droit public français s'affirment sous la III^{e} République[140]. Alors que les lois constitutionnelles de 1875[141] ne contiennent aucune référence aux droits et libertés, le Parlement a adopté plusieurs lois concernant les libertés publiques : loi du 30 juin 1881 sur la liberté de réunion[142], loi du 29 juillet 1881 sur la liberté de la presse[143], loi Waldeck-Rousseau du 1er juillet 1901 sur la liberté d'association[144]. Toutes ces lois, encore en vigueur actuellement, ont connu de nombreux amendements, afin de s'adapter progressivement aux évolutions de la société et aux événements historiques : Seconde guerre mondiale et instauration de l'État français de Vichy, IV^{e} République et guerres de décolonisation, V^{e} République, guerre d'Algérie, guerre froide et attentats terroristes à la fin du XX^{e} siècle et début du XXI^{e} siècle.

Les libertés sont également encadrées dans d'autres pays par la Constitution ou des amendements à la Constitution, comme pour les États-Unis d'Amérique[145] où des lois tentant de restreindre certaines pratiques liées à Internet sont invalidées par la Cour suprême du fait de

[137] John Locke, *Lettre sur la tolérance* (1689) ; Montesquieu, *De l'esprit des lois* (1748) ; Jean-Jacques Rousseau, *Du contrat social* (1762) ; Voltaire, *Dictionnaire philosophique portatif* (1764) ; Emmanuel Kant, *Critique de la raison pure* (1781), *Fondements de la métaphysique des mœurs* (1785).

[138] Articles votés entre le 20 et le 26 août 1789, la déclaration est promulguée par le roi Louis XVI dans des lettres patentes le 3 novembre 1789.

[139] Titre premier de la Constitution de 1791 des 3 et 4 septembre 1791 ; Déclaration des droits de l'homme et du citoyen de la Constitution de l'An I (24 juin 1793) ; Articles 1 et 2 des Droits de la Constitution du 5 fructidor An III ; Article 4 de la Charte constitutionnelle du 4 juin 1814 ; Titre VI – Droits des citoyens (Articles 59 et suivants) de l'Acte additionnel aux Constitutions de l'Empire du 22 avril 1815 ; Droit public des Français, Articles 1 à 11, de la Charte constitutionnelle du 14 août 1830 ; Préambule de la Constitution de 1848, II^{e} République du 4 novembre 1848 ; Article 1 de la Constitution de 14 janvier 1852 (Second Empire) ; Préambule de la Constitution du 27 octobre 1946 (IV^{e} République) ; Préambules de la Constitution du 4 octobre 1958 (V^{e} République).

[140] Patrick Wachsmann, *Libertés publiques*, 6^{e} édition, Dalloz, pages 23 et suivantes.

[141] Lois constitutionnelles des 24, 25 février et 16 juillet 1875.

[142] Loi du 30 juin 1881 *sur la liberté de réunion*, Recueil Duvergier, pp. 379-390, bulletin des lois 12e S., B. 644, n^{o} 10927.

[143] Loi du 29 juillet 1881 *sur la liberté de la presse*, publiée au journal officiel de la République française du 30 juillet 1881 p. 4201.

[144] Loi du 1er juillet 1901 *relative au contrat d'association*, parue au journal officiel de la république française du 2 juillet 1 901 p. 4025.

[145] La Déclaration des droits (*United States Bill of Rights*) est l'ensemble constitué des dix premiers amendements à la constitution américaine. Elle limite les pouvoirs du gouvernement fédéral et garantit les libertés de presse, de parole, de religion, de réunion, le droit de porter des armes, et le droit de propriété.

ces amendements. La Grande-Bretagne n'a pas de Constitution écrite, mais les libertés publiques y sont protégées, depuis la *Magna Carta*[146] ou la déclaration des droits de 1689[147], des agissements de l'autorité centrale. Ces textes assurent une limitation effective du pouvoir politique en consacrant une tradition, hors d'atteinte du pouvoir[148].

Après la Seconde guerre mondiale, la société a connu des bouleversements liés aux traumatismes résultant de ce conflit ainsi que des atteintes importantes à l'intégrité de la personne humaine dans la société occidentale. Ces traumatismes ont eu pour conséquences l'adoption au niveau européen et mondial des proclamations et chartes relatives aux libertés et aux droits de l'homme[149].

Mais avec l'apparition de nouvelles technologies liées à l'informatique, la société doit faire face à de nouveaux risques concernant les libertés individuelles et à des modifications du comportement des individus. La société n'avait que peu évolué du XIX^e^ siècle au milieu du XX^e^ siècle, malgré deux guerres mondiales qui, compte tenu de la ponction des hommes pour le front, avaient vu le rôle de la femme évoluer et s'affirmer, sans obtenir son émancipation, et la société rurale et patriarcale commencer à régresser face à une urbanisation constante. La société va connaître à partir des années 1970 une révolution technologique, sans égale dans l'histoire de l'humanité, liée à l'informatisation de la société tertiaire et surtout à la numérisation de la société qui en découlera.

L'émergence rapide de cette société numérique va entraîner une adaptation des législations nationales et internationales de protection des libertés, adaptation toujours en cours. Cette protection malgré certains textes de portée internationale et surtout européenne reste hétérogène (titre 1), la protection des droits individuels demeure confrontée aux mesures sécuritaires mises en place dans plusieurs États pour lutter contre l'insécurité et les risques terroristes (titre 2).

[146] La *Magna Carta Libertatum* (Grande Charte) est une charte de soixante-trois articles arrachée par le baronnage anglais au roi Jean sans Terre le 15 juin 1215.

[147] La Déclaration des droits (ou *Bill of Rights* en anglais) est un texte imposé en 1689 aux souverains d'Angleterre (Guillaume III et Marie II) à la suite de la Glorieuse Révolution. Il définit les principes de la monarchie parlementaire en Angleterre.

[148] Patrick Wachsmann, *Libertés publiques*, 6^e^ édition, 2009, Dalloz, pp. 20-21.

[149] La Déclaration universelle des droits de l'homme a été adoptée le 10 décembre 1948 par l'Assemblée générale de l'ONU, et la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, communément appelée Convention européenne des droits de l'homme, est un traité international signé par les États membres du Conseil de l'Europe le 4 novembre 1950.

Titre 1. La société numérique, un cadre hétérogène de protection des libertés

Les modifications technologiques, apportées par la numérisation croissante et rapide des sociétés, vont avoir des conséquences importantes sur le comportement des citoyens, modifications qui affectent le régime des libertés publiques.

Pour Patrick Wachsmann[150], « si les libertés sont qualifiées de publiques, ce n'est pas par opposition à des libertés privées », cette qualification introduit une précision quant à l'origine de la contrainte sociale qui les régit, elle dénote l'intervention du pouvoir. Les libertés sont envisagées en tant qu'objets de la réglementation juridique. Pour Jean Rivero[151], ce droit des libertés publiques emprunte à des disciplines juridiques multiples, le droit constitutionnel, le droit administratif, mais aussi le droit pénal et le droit civil, et il ne tire son unité que de son objet. Les libertés publiques n'existent que lorsque l'État en a consacré le principe et la protection.

Si de nombreuses libertés publiques continuent à être protégées par les textes adoptés avant la révolution numérique, amendés pour tenir compte de cette révolution, le législateur a ressenti la nécessité d'adopter de nouveaux textes garantissant l'individu contre une intrusion dans sa vie privée, intrusion facilitée par les nouvelles technologies qui collectent des données et qui en collationnant ces données dévoilent des pans de cette vie privée. Le numérique a entraîné des modifications du régime juridique de plusieurs libertés fondamentales[152], et suscité la reconnaissance de nouveaux droits. Mais, dans le même temps, un sentiment d'insécurité grandissant, entretenu par des mouvements terroristes et des attentats spectaculaires, va pousser les gouvernements à proposer des lois restreignant les libertés acquises progressivement durant plusieurs décennies, et étendant les possibilités de surveillance des individus par les forces de police, lesdits gouvernements utilisant, alors, les possibilités offertes par les nouvelles technologies pour surveiller les individus discrètement[153] ou échanger des informations concernant les citoyens suspects ou non de faits délictueux[154], donc améliorer les techniques d'investigation des forces de police.

Les libertés connaissent un régime de protection soit hérité des années antérieures à l'avènement du numérique, par adaptation et interprétation des textes consacrant et gérant ces

[150] Patrick Wachsmann, *Libertés publiques*, Dalloz, 6e édition, 2009, p. 2.
[151] Jean Rivero, Hugues Moutouh, *Libertés publiques, tome 1*, 9e édition, 2003, Presses universitaires de France, pp. 1-2.
[152] Conseil d'État, *Le numérique et les droits fondamentaux*, Les rapports du Conseil d'État, 2014, pp. 12-15.
[153] Cf. la loi no 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure* dite LOPPSI 2.
[154] Échange des données des dossiers passagers (en anglais *Passenger Name Record* ou PNR) entre l'Union européenne et les États-Unis d'Amérique.

libertés, en France (chapitre 1) ; soit par adoption de lois nouvelles liées aux nouvelles technologies de l'information et des communications, et aux risques encourus par la société, risques liés à la cybercriminalité et à l'émergence d'un terrorisme international (chapitre 2).

Chapitre 1. Une adaptation de la législation protégeant les libertés

Le réseau Internet, les technologies du WEB 2.0[155] et l'accès mobile à Internet et aux réseaux sociaux modifient les agissements individuels dans la société numérique. D'une attitude passive limitée à la consultation des sites, l'internaute devient acteur et peut interagir en direct avec l'information qu'il reçoit, voire il peut créer l'information ou la relayer. Les actions des utilisateurs du WEB 2.0 ajoutent de la valeur[156]. Sa liberté d'expression, mais aussi sa liberté de choix, se trouve démultipliée par l'univers numérique mis à sa disposition. De nouveaux besoins apparaissent dans une société mercantile cherchant à vendre et commercialiser de nouveaux concepts et modes de vie. Le téléphone mobile, apparu dans les années 1990, ne sert plus à téléphoner, mais à communiquer et à rester en relation avec un réseau de relations virtuelles. De téléphone, il est devenu *smartphone* en intégrant un appareil photographique, une caméra, un enregistreur de sons, un GPS. Il permet l'accès à Internet, la diffusion et la réception de messages courts en temps réels, la connexion permanente à son réseau social. Il est également utilisé pour écouter de la musique, voire pour regarder un film ou une émission de télévision. Dans certains pays, avec la technologie NFC[157], le smartphone remplace la carte de crédit. Bientôt, il sera utilisé pour enregistrer et capter des données vitales : rythme cardiaque, pouls, etc. Comme l'écrit Isabelle Compiègne[158], le téléphone portable, devenu smartphone, est devenu un véritable instrument d'innovation sociétale.

---

[155] Le WEB 2.0 est une évolution technique du WEB initial, la sophistication des techniques doit permettre à tout utilisateur d'un terminal (PC, smartphone, tablette, etc.) de communiquer et d'échanger des informations avec tout utilisateur. Sans connaissances techniques, l'utilisateur échange des informations, partage des photos ou des petits films, via les Blogs, ou via les réseaux sociaux, Facebook, Twitter, Alors qu'avec la technique initiale du WEB, l'utilisateur recevait de l'information, avec les techniques mises en œuvre par le WEB 2.0, il produit de l'information et devient acteur du WEB.
De plus, avec les techniques du PUSH liées aux abonnements, l'information est disponible, pour l'utilisateur, sur son terminal sans aucune sollicitation nouvelle.

[156] Tim O'Reilly, "The Future of Data Industry", *Where 2.0 Conference,* San José, 13-14 June 2006.

[157] *Near Field Communication* ou communication dans un champ proche.

[158] Isabelle Compiègne, *La société numérique en question(s)*, Éditions Sciences Humaines, 2011, p. 14.

L'épanouissement de l'individu peut se manifester par des opportunités de modes d'expression nouveaux, des facilités de choix ou des possibilités nouvelles, mais cet épanouissement peut être contrecarré par des abus de cette liberté nouvelle, abus du fait de la personne concernée, mais aussi abus de tiers. Internet peut annihiler toute retenue et favoriser une certaine délinquance en l'absence de sanction et devenir un vecteur du crime organisé[159].

Internet est également devenu un vecteur de diffusion de l'information. Aux États-Unis d'Amérique, Al Gore[160] a propagé l'idée des autoroutes de l'information durant la campagne présidentielle de 1992. Il prévoyait une architecture et une infrastructure capables de véhiculer toutes sortes d'informations, son, images, à très grande vitesse, avec des accès étendus et une infrastructure unifiée. Cette autoroute existe aujourd'hui et a largement dépassé les frontières des seuls États-Unis. Avec l'apparition de la toile[161], les internautes ont découvert un espace de communication puissant et international, se jouant des frontières[162], mais cet espace ouvert, inventé par des universitaires ou des étudiants libertaires sur les campus universitaires ou dans les laboratoires de recherche, n'a pas été réalisé comme un espace sécurisé, et, à ce titre, son utilisation peut réduire, voire anéantir, certaines libertés. Il peut, à l'opposé, être utilisé pour contrer un État policier et organiser des réunions voire des manifestations prérévolutionnaires, comme ce fut le cas en Tunisie et en Égypte au printemps 2011[163]. De plus, la généralisation de la dématérialisation de nombreux documents et la vulgarisation de certaines techniques, initialement militaires, comme le GPS, ou la vidéosurveillance peuvent venir aussi réduire cet espace de libertés.

---

[159] David S. Wall, "The Internet as a Conduit for Criminal Activity", March 2010, in April F. Pattavina, (ed) *Information Technology and the Criminal Justice System*, Thousand Oaks, CA, pp. 77-98, URL: https://www.researchgate.net/profile/David_Wall8/publication/228199078_The_Internet_as_a_Conduit_for_Criminal_Activity/links/54d0b4cb0cf298d656681e31/The-Internet-as-a-Conduit-for-Criminal-Activity.pdf consulté le 20 mars 2018.

[160] Vice-Président Al Gore, *Information Superhighways Speech*, discours du 31 mars 1994, en ligne à http://vlib.iue.it/history/Internet/algorespeech.html .

[161] *World Wide WEB* (WWW) ou littéralement en français la toile (d'araignée) mondiale.

[162] John Perry Barlow, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation,* February 8, 1996, Op. cit.

[163] Jean-Jacques Lavenue, « Printemps arabes, révolutions virtuelles ? », *Actes du colloque international « E-Révoution et révolutions »,* Lille, 220-21 décembre 2012.
Yves Gonzalez-Quijano, « Internet, le "Printemps arabe" et la dévaluation du cyberactivisme arabe », *Égypte/Monde arabe*, 2015/1 (n° 12), pp. 67-84. URL : https://www.cairn.info/revue-egypte-monde-arabe-2015-1-page-67.htm, consulté le 21 novembre 2017.

Mais le cyberespace, l'espace numérique dématérialisé, n'est pas un espace de non-droit[164], comme le préconisaient les premiers utilisateurs et concepteurs du réseau Internet[165]. Le droit commun s'applique à cet espace mouvant et international, même si certaines particularités y ont incité le législateur à introduire des règles spéciales tenant compte de cette spécificité. Si Internet n'est pas un espace libertaire[166], il demeure un espace de connaissance, d'échanges et de liberté.

« *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui* »[167], aussi, toute liberté trouve-t-elle ses limites dans le respect de la jouissance par autrui de ses propres libertés. Ces limites ou restrictions proportionnées au but à atteindre, peuvent provenir de la loi[168], mais elles peuvent aussi être induites par d'autres facteurs : la morale, des règles d'éthique, une réglementation, voire des clauses contractuelles[169]. Avec l'apparition du cyberespace, la question du droit applicable à cet espace nouveau, international et protéiforme s'est posée. Le législateur devait-il laisser cet espace s'autoréguler ou au contraire, cet espace devait-il être régi par une législation, ordinaire ou spéciale ? Dès 1998, le Conseil d'État a précisé que « l'ensemble de la législation existante s'applique aux acteurs d'Internet » et qu'il n'était pas « besoin d'un droit spécifique de l'Internet et des réseaux »[170].

Les droits fondamentaux (Section 1) ou les droits économiques (Section 2) connaissent des répercussions liées à l'omniprésence des techniques numériques dans la société actuelle. Les législations nationales, adoptées État par État, n'ont pas été élaborées pour faire face à un réseau mondial et à des interprétations légales divergentes. Des adaptations d'interprétation sont parfois nécessaires dans les États, en fonction de l'histoire et des coutumes, mais alors se pose la question du droit applicable. Au sein de l'Union européenne, une harmonisation partielle est réalisée par les directives, transposées dans le droit des États membres, et les règlements d'application directe. Toutefois, des divergences perdurent et sont utilisées par les acteurs

[164] Jean-François Théry, Isabelle Falque Pierrotin, *Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998,* Conseil d'État. Section du rapport et des études, Publié à la documentation française, décembre 1998.

[165] Le réseau ARPANET, puis Internet, était utilisé par la communauté de recherche universitaire pour échanger et partager des idées entre chercheurs, respectant et encourageant la tradition universitaire de la publication ouverte des idées et des résultats. Cette tradition s'est perpétuée avec les logiciels libres.

[166] Libertaire : « *partisan de la liberté absolue, anarchiste* » (définition du dictionnaire Larousse, URL : http://www.larousse.fr/dictionnaires/francais/libertaire/46993 consultée le 23 mars 2018).

[167] *Déclaration des droits de l'Homme et du citoyen* du 26 août 1789, Article 4.

[168] Déclaration des droits de l'homme et du citoyen de 1789, article 4. « *Ces bornes ne peuvent être déterminées que par la Loi* ».

[169] Murray N. Rothbard, *The Ethics of Liberty,* Humanities Press, 1982.

[170] Jean-François Théry, Isabelle Falque Pierrotin, *Internet et les réseaux numériques*. Op. cit.

internationaux pour un « dumping » législatif[171], les sites s'établissant dans les États membres où les contraintes sont moindres[172].

[171] Stéphane Astier, « Vers une régulation éthique de l'Internet : les défis d'une gouvernance mondiale », *Revue Internationale des Sciences Administratives*, 2005/1 (Vol. 71), pp. 143-161. URL : https://www.cairn.info/revue-internationale-des-sciences-administratives-2005-1-page-143.htm consulté le 7 décembre 2017.

[172] Lire l'avis de la commission nationale de l'informatique et des libertés (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)).

« *Article 8 (Champ d'application territorial)*

« L'article 8 du projet de loi vient préciser le champ d'application de la loi nationale. Il prévoit qu'en cas de divergence de législations entre États membres liée aux marges de manœuvre laissées par le Règlement, la loi nationale s'applique dès lors que la personne réside en France et ce, même si le responsable de traitement n'est pas établi en France. La logique est en revanche inversée dans le cadre du respect du droit à la liberté d'expression et d'information, par exemple dans le domaine de la presse, où le droit applicable est celui de l'État dans lequel est établi le responsable.

« La Commission prend acte de ces dispositions, tout en soulignant les difficultés opérationnelles qui pourraient naître avec les pays ayant retenu des critères différents et incompatibles avec ceux retenus par le projet de loi ».

De fait ces dispositions concernent les traitements mentionnés au 2 de l'article 85 du règlement général sur la protection de données : « *2.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* ».

Section 1. Les droits fondamentaux dans la société numérique

Comme précisé par le Conseil d'État, « l'ensemble de la législation existante s'applique aux acteurs d'Internet »[173] dans la société numérique. Les libertés fondamentales restent protégées par des textes adoptés avant l'avènement des techniques numériques. La loi protégeant et encadrant la liberté de la presse a été votée en 1881[174]. À l'époque, il n'était pas question de diffusion de ce média par des techniques électroniques et numériques, et pourtant cette loi reste la base de la protection de la communication sur Internet. Elle a, bien évidemment, été amendée par le législateur pour s'adapter à cette technologie, tout comme elle avait connu des amendements pour faire face aux défis de l'histoire[175]. Cette loi promulguée sous la III[e]

[173] Jean-François Théry, Isabelle Falque Pierrotin, *Internet et les réseaux numériques*. Op. cit.
[174] Loi du 29 juillet 1881 *sur la liberté de la presse*, publiée au Journal officiel de la République française du 30 juillet 1881 p. 4201.
[175] Loi du 12 décembre 1893 *portant modification des articles 24, paragraphe 1er, 25 et 49 de la loi du 29 juillet 1881*, JORF n°0338 du 13 décembre 1893 p. 6113,
Ordonnance du 6 mai 1944 *relative à la répression des délits de presse*,
Ordonnance du 26 août 1944 *sur l'organisation de la presse française*, JORF n°0072 du 30 août 1944 p. 779,
Loi n° 50-10 du 6 janvier 1950 *portant modification et codification des textes relatifs aux pouvoirs publics*, JORF n°0006 du 7 janvier 1950 p. 215,
Loi n° 52-336 du 25 mars 1952 *modifiant certaines dispositions de la loi du 29 juillet 1881 sur la liberté de la presse,* JORF n°0075 du 26 mars 1952 p. 3253.
Loi n° 52-1352 du 19 décembre 1952 *modifiant les articles 25, 30, 35 de la loi du 29 juillet 1881 sur la liberté de la presse*, JORF n°0302 du 20 décembre 1952 p. 11699.
Loi n° 53-184 du 12 mars 1953 *modifiant les articles 39 et 48 de la loi du 29 juillet 1881 sur la liberté de la presse*, JORF n°0062 du 13 mars 1953 p. 2371.
Loi n° 55-1552 du 28 novembre 1955 *complétant la loi du 29 juillet 1881 sur la liberté de la presse* JORF n°0282 du 1 décembre 1955 p. 11644,
Loi n° 58-92 du 4 février 1958 *complétant l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse* JORF n°0030 du 5 février 1958 p. 1348,
Loi n° 72-546 du 1 juillet 1972 *relative à la lutte contre le racisme* JORF n°0154 du 2 juillet 1972 p. 6803,
Loi n° 90-615 du 13 juillet 1990 *tendant à réprimer tout acte raciste, antisémite ou xénophobe* JORF n° 0162 du 14 juillet 1990 p. 8333,
Loi n° 98-468 du 17 juin 1998 *relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs* JORF n°0139 du 18 juin 1998 p. 9255,
Loi n° 2000-516 du 15 juin 2000 *renforçant la protection de la présomption d'innocence et les droits des victimes* JORF n° 0138 du 16 juin 2000 p. 9038,
Ordonnance n° 2000-916 du 19 septembre 2000 *portant adaptation de la valeur en euros de certains montants exprimés en francs dans les textes législatifs* JORF n° 0220 du 22 septembre 2000 page 14877.
Loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* JORF n°0143 du 22 juin 2004 p. 11168,
Loi n° 2004-1 343 du 9 décembre 2004 *de simplification du droit* JORF n° 0287 du 10 décembre 2004 p. 20857,
Ordonnance n° 2009-80 du 22 janvier 2009 *relative à l'appel public à l'épargne et portant diverses dispositions en matière financière* JORF n° 0019 du 23 janvier 2009 page 1431,
Loi n° 2010-1 du 4 janvier 2010 *relative à la protection du secret des sources des journalistes* JORF n°0003 du 5 janvier 2010 p. 272,
Loi n° 2012-954 du 6 août 2012 *relative au harcèlement sexuel* JORF n°0182 du 7 août 2012 p. 12921,
Loi n° 2012-1 432 du 21 décembre 2012 *relative à la sécurité et à la lutte contre le terrorisme* JORF n°0298 du 22 décembre 2012 p. 20281,

République a ainsi vu son contenu modifié par des lois, des ordonnances pour s'adapter aux évolutions de la société. Des décisions du Conseil constitutionnel en ont invalidé certaines dispositions pour non-conformité à la Constitution[176], en réponse à des questions prioritaires de constitutionnalité.

La société numérique fournit des moyens de communication aux personnes physiques qui sont en eux-mêmes une révolution par rapport à la communication papier ou analogique, qui était la règle jusque dans les années 1990. Les messageries électroniques permettent de communiquer instantanément, ou quasi instantanément vers n'importe quel point du globe. Dans un de ses ouvrages[177], Russell Weaver a souligné qu'au début du 20e siècle, un courrier mettait plusieurs semaines pour être acheminé de Washington à San Francisco, alors qu'il ne fallait plus que quelques secondes avec Internet, et que cette célérité avait des conséquences sur la démocratie des États. Dans son ouvrage, il analyse les conséquences des inventions technologiques, de l'imprimerie à Internet en passant par le télégraphe et le téléphone, sur l'apparition et le développement de la liberté d'expression et de la communication de masse : rapidité de propagation, diffusion des idées à un large public.

Loi nº 2013-711 du 5 août 2013 *portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne et des engagements internationaux de la France* JORF nº0181 du 6 août 2013 p. 13338,
Loi nº 2014-56 du 27 janvier 2014 *visant à harmoniser les délais de prescription des infractions prévues par la loi sur la liberté de la presse du 29 juillet 1881, commises en raison du sexe, de l'orientation ou de l'identité sexuelle ou du handicap* JORF nº0023 du 28 janvier 2014 p. 1561,
Loi n° 2014-1353 du 13 novembre 2014 *renforçant les dispositions relatives à la lutte contre le terrorisme* JORF n°0263 du 14 novembre 2014 page 19162,
Ordonnance nº 2016-131 du 10 février 2016 *portant réforme du droit des contrats, du régime général et de la preuve des obligations*, publiée au JORF nº 0035 du 11 février 2016,
Loi n° 2016-339 du 22 mars 2016 *relative à la prévention et à la lutte contre les incivilités, contre les atteintes à la sécurité publique et contre les actes terroristes dans les transports collectifs de voyageurs* JORF n°0070 du 23 mars 2016,
Loi n° 2016-1524 du 14 novembre 2016 *visant à renforcer la liberté, l'indépendance et le pluralisme des médias* JORF n°0265 du 15 novembre 2016
Loi n° 2017-86 du 27 janvier 2017 *relative à l'égalité et à la citoyenneté* JORF n°0024 du 28 janvier 2017.

[176] Décision nº 2011-131 QPC du 20 mai 2011 *Mme Térésa C. et autre [Exception de vérité des faits diffamatoires de plus de dix ans]*,
Décision nº 2013-319 QPC du 7 juin 2013 *M. Philippe B. [Exception de vérité des faits diffamatoires constituant une infraction amnistiée ou prescrite, ou ayant donné lieu à une condamnation effacée par la réhabilitation ou la révision]*,
Décision nº 2015-492 QPC du 16 octobre 2015 *Association Communauté rwandaise de France [Associations pouvant exercer les droits reconnus à la partie civile en ce qui concerne l'apologie des crimes de guerre et des crimes contre l'humanité]*.

[177] Russell L. Weaver, *From Gutenberg to the Internet: Free speech, advancing technology, and the implications for democracy*, Carolina Academic Press, 2012.

Les pages personnelles puis les *blogs*[178] permettent à toute personne ayant un accès Internet de diffuser une information ou une opinion. L'information circule sur Internet sans contrôle véritable, créant un flux d'information instantané, concurrencé par les chaînes d'information permanente, radio ou télévision. La société numérique est devenue une société générant de l'information[179]. Tous types d'informations circulent dans cette société numérique, que ce soit des informations générales, culturelles, techniques ou des informations privées. Ce flux d'information, non contrôlé, peut avoir un effet inverse de celui recherché, des journaux relaient des informations non contrôlées pour ne pas paraître en retard ou absentes, quitte à publier un correctif quelques heures plus tard[180]. Des informations privées peuvent se retrouver disponibles sur la toile alors qu'elles n'auraient jamais dû y être divulguées. Ainsi, la société numérique est-elle partagée entre une information libre, informative et instructive, permettant un épanouissement personnel des individus, et une information privée qui doit être respectée et donc contrôlée pour ne pas nuire aux individus. La liberté d'information ou d'expression doit concilier le droit du public d'être informé avec le droit du citoyen du respect de son intimité[181]. La numérisation de la société favorise les libertés dites de l'esprit : liberté de pensée, d'expression, de culte ou de réunion, sans nécessiter d'autres lois que les lois applicables en dehors du cyberespace, n'entraînant que des adaptations nécessaires au changement de contexte. En fournissant de puissants moyens de communication, elle favorise également la création d'entreprises délocalisées, individuelles, et donc vient amplifier la liberté de se déplacer [182] et d'entreprendre[183], libertés fondamentales de l'Union européenne.

---

[178] Un blog, anglicisme pouvant être francisé en bloc-notes, est un type de site web utilisé pour la publication d'articles, généralement succincts. À la manière d'un journal intime, ces articles ou « billets » sont datés, signés et se succèdent du plus récent au plus ancien. Les lecteurs peuvent souvent y apporter des commentaires.

[179] Mokhtar Ben Henda, Henri Hudrisier, « Penser, classer, apprendre et communiquer. Normalisation et nouveaux modes de classification du savoir », *Hermès, La Revue*, 2013/2 (n° 66), pp. 160-166. URL : https://www.cairn.info/revue-hermes-la-revue-2013-2-page-160.htm consulté le 7 décembre 2017.

[180] Le 28 février 2015, à partir d'une confusion patronymique, la mort de Martin Bouygues, PDG du groupe éponyme, a été annoncée par plusieurs médias, pour être démentie quelques heures plus tard. Fait relaté dans l'article « Fausse mort de Martin Bouygues : Les médias sont-ils pour toujours condamnés à l'emballement ? » du 1er mars 2015, sur *le Blog du communicant* accessible à http://www.leblogducommunicant2-0.com/2015/03/01/fausse-mort-de-martin-bouygues-les-medias-sont-ils-pour-toujours-condamnes-a-lemballement/, consulté le 23 janvier 2017.

[181] François Saint-Pierre, « Respect de la vie privée versus droit à l'information : un point utile sur la jurisprudence de la Cour européenne des droits de l'homme », *Dalloz actualité*, 27 février 2015, URL : https://www.dalloz-actualite.fr/chronique/respect-de-vie-privee-versus-droit-l-information-un-point-utile-sur-jurisprudence-de-cour-, consulté le 23 mars 2018.

[182] Libre circulation des personnes consacrée par l'article 20 du traité sur l'Union européenne et garantie par l'article 45 de la Charte européenne des droits fondamentaux.

[183] Liberté d'établissement (art. 49 TFUE et suivants) et liberté de prestation de services (art. 56 TFUE et suivants).

Sous-section 1. Les libertés de pensée et d'opinion dans la société numérique

La liberté d'émettre, de diffuser et de recevoir des idées, des pensées ou des opinions se décline autour de différentes notions telles que « liberté d'expression », « liberté d'information », « liberté de communication » ou « libre circulation des idées », thèmes défendus par les philosophes des Lumières. Voltaire défendait la liberté d'imprimer et la tolérance[184]. Pour Kant, la liberté de penser s'oppose à la contrainte civile : « *enlever aux hommes la liberté de communiquer publiquement leurs pensées, leur ôte aussi la liberté de penser* »[185]. Au XX[e] siècle, pour Jean Rivero[186], les libertés de la pensée sont multiples et essentielles : liberté d'opinion, liberté de conscience, liberté des cultes, liberté de l'expression de la pensée et liberté de réunion, de manifestation et liberté d'association.

La liberté d'émettre, de diffuser et de recevoir des idées, des pensées ou des opinions occupe, sur le plan politique, une place particulière et privilégiée par rapport aux autres droits et libertés fondamentaux[187]. Elle entretient des liens indissolubles avec les régimes démocratiques. Dans un entretien sur France Inter, Robert Badinter affirme : « *Sans liberté de la presse, il n'y a pas de liberté tout court* »[188].

La liberté de communication et d'expression est consacrée par l'article 11 de la Déclaration des droits de l'homme et du citoyen[189]. Lors de la Révolution française, cette liberté était celle de l'imprimeur et du journaliste, seuls capables alors de diffuser des idées dans les gazettes ou les libelles. Elle est devenue au fil du temps et de l'apparition de nouvelles techniques, celle du

---

[184] Voltaire, *Traité sur la tolérance, A l'occasion de la mort de Jean Calas*, s.n. Genève, 1763.

[185] Emmanuel Kant, *Mélanges de logique*, Qu'est-ce que s'orienter dans la pensée ? (VII), traduit par J. Tissot, Librairie Philosophique de Ladrange, 1862, p. 336,

[186] Jean Rivero, Hugues Moutouh *Libertés publiques Tome 1* 9[e] édition mise à jour, 2003, Thémis Droit Public, Presses Universitaires de France, pages 18 et suivantes.

[187] La manifestation à Paris du 11 janvier 2015, dite marche républicaine, faisant suite à l'assassinat de plusieurs journalistes a démontré l'attachement des Français à une liberté d'expression. Dans la prolongation de cette manifestation, le gouvernement, lors des débats de la loi Macron (Loi n[o] 2015-990 du 6 août 2015 *pour la croissance, l'activité et l'égalité des chances économiques*, dite « loi Macron ») à l'Assemblée nationale, a dû retirer un amendement proposé en commission et réduisant la liberté d'information et d'investigation des journalistes, mais protégeant le secret des affaires (Denis Cosnard, « Secret des affaires : le gouvernement retire son projet », *Le Monde.fr*, 30 janvier 2015, accessible à http://www.lemonde.fr/economie/article/2015/01/30/secret-des-affaires-le-gouvernement-retire-son-projet_4566657_3234.html, consulté le 23 janvier 2017)

[188] Robert Badinter, durant l'édition spéciale de l'émission « le 7/9 » du 8 janvier 2015 sur France Inter, en ligne à https://www.youtube.com/watch?v=Uqluz_d_T1g, écouté le 7 décembre 2017.

[189] Déclaration des droits de l'homme et du citoyen, Article 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* ».

lecteur de journaux, de l'auditeur de radio et du téléspectateur de la télévision[190]. « *La liberté d'expression constitue l'un des fondements essentiels de pareille société [démocratique], l'une des conditions primordiales de son progrès et l'épanouissement de chacun* », énonce la Cour européenne des droits de l'homme en 1976[191]. En 1999[192], la Cour européenne des droits de l'homme rappelle que la liberté d'expression constitue l'un des fondements d'une société démocratique et qu'il est de l'intérêt d'une société démocratique d'assurer et de maintenir la liberté de la presse, la restriction devant être toujours proportionnée au but légitime poursuivi. Dans sa décision des 10 et 11 octobre 1984, le Conseil constitutionnel considère[193] que la liberté de communication des pensées et des opinions constitue « *une liberté fondamentale, d'autant plus précieuse que son exercice est l'une des garanties essentielles du respect des autres droits et libertés et de la souveraineté nationale* ». Aujourd'hui, l'exercice de cette liberté implique la liberté d'accès à Internet[194]. En effet, dans la décision nº 2009-580 DC, après avoir rappelé « *le caractère fondamental du droit à la liberté d'expression et de communication* »[195], le Conseil constitutionnel considère « *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, ce droit implique la liberté d'accéder à ces services* »[196], c'est-à-dire à Internet. Cette décision crée un nouveau droit fondamental : le droit d'accès à Internet[197]. Comme l'écrit Thierry Revet[198], « *la défense de l'accès à Internet paraît bien être la défense d'une position contractuelle,* [le contrat d'abonnement,] *comme source et moyen de l'utilité "accès à internet", déclarée éminente au nom de la liberté de communication* ».

[190] Russell L. Weaver, « *From Gutenberg to the Internet: Free speech, advancing technology, and the implications for democracy* », Carolina Academic Press 2012.
[191] Cour européenne des droits de l'homme (plénière), Arrêt du 7 décembre 1976, Requête nº 5493/*72,* Affaire *Handyside c/ Royaume-Uni*.
[192] Cour européenne des droits de l'homme, Arrêt du 21 janvier 1999, Requête n° 29183/95, Affaire *Fressoz et Roire c/ France*
[193] Conseil constitutionnel, Décision nº 84-181 DC du 11 octobre 1984 *Loi visant à limiter la concentration et à assurer la transparence financière et le pluralisme des entreprises de presse*, considérant n° 37.
[194] Conseil constitutionnel, décision nº 2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur Internet*.
[195] Conseil constitutionnel, décision no 2009-580 DC du 10 juin 2009, Considérant n° 11.
[196] Conseil constitutionnel, décision no 2009-580 DC du 10 juin 2009, Considérant n° 12.
[197] Laure Marino, « Le droit d'accès à internet, nouveau droit fondamental », *Recueil Dalloz*, 2009, n° 30, pp. 2045-2046.
[198] Thierry Revet, « La consécration de la liberté d'accéder aux services de communication au public en ligne, protection comme res de la position contractuelle permettant l'accès au réseau internet ? », *Revue trimestrielle de droit civil*, octobre-décembre 2009, n° 4, pp. 756-757.

§ 1 - La renaissance et l'encadrement de la liberté d'expression dans la société numérique

La liberté d'expression est historiquement associée à la liberté de communication des idées et des informations donc à la liberté de la presse. Dans le Littré (1880), le mot « expression » est défini comme étant l'« *action de faire sortir, paraître au dehors, c'est-à-dire manière de rendre sa pensée par l'organe de la parole, ou par le ministère de la plume* » et la communication est l'action de communiquer, c'est-à-dire de « *rendre commun, faire part, transmettre* ». De ces définitions, il ressort que la communication est nécessaire à la transmission de la pensée exprimée par la parole ou par l'écrit. Historiquement, cette communication était réalisée par la presse et la diffusion des journaux, et nécessitait la liberté de la presse. Cette liberté de la presse s'est confrontée à la censure, censure plus ou moins pesante selon les époques et les circonstances. L'abolition de la censure n'a pas garanti la liberté d'expression[199] qui nécessite la tolérance, c'est-à-dire reconnaître l'égalité des autres même avec des idées différentes.

Avec l'apparition de la radio, puis de la télévision, la diffusion des informations et des idées s'accélère et touche une part plus importante de la population. Durant la Seconde Guerre mondiale, la radio permettra d'atteindre les groupes isolés de résistants sur les territoires occupés par l'armée allemande et de diffuser des messages « codés ».

Dans les années 1980, en France avec le Minitel, seuls les organes de presse pouvaient ouvrir des sites d'information. Le réseau Internet et le WEB, progressivement, permettent à d'autres acteurs de diffuser des opinions et des informations.

Comme le rappelle un rapport d'étude de l'Assemblée nationale[200], *« ce sont […] nos droits, au premier rang desquels la liberté d'expression et de communication ainsi que l'accès à la culture et au savoir ainsi que la démocratie qui disposent, avec Internet, d'un instrument incroyable de promotion* ». Avec la création des blogs et l'avènement du WEB 2.0[201], la liberté d'expression semble connaître une renaissance permettant à un plus grand nombre d'individus

[199] Gérard Leclerc, « De la censure à la liberté de penser », in Gérard Leclerc (dir.), *Histoire de l'autorité. L'assignation des énoncés culturels et la généalogie de la croyance*, Paris, Presses Universitaires de France, « Sociologie d'aujourd'hui », 1996, pp. 219-246. URL : https://www.cairn.info/histoire-de-l-autorite--9782130474371-page-219.htm consulté le 7 décembre 2017.

[200] Patrick Bloche, Patrice Verchère, *Rapport d'information sur les droits de l'individu dans la révolution numérique*, enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011, p. 20.

[201] Considéré comme une évolution naturelle du web initial, le WEB 2.0 est un concept d'utilisation d'Internet qui a pour but de valoriser l'utilisateur et ses relations avec les autres. Le WEB 2.0 regroupe des technologies nouvelles telles que les flux RSS, les messageries, les blogs (sortes de bloc-notes), les réseaux sociaux.

de s'exprimer[202]. Le WEB 2.0, avec les réseaux sociaux, a participé à une libération de la parole, chacun pouvant s'exprimer sans intermédiaire. Le concept de WEB 2.0 s'est répandu rapidement depuis quelques années. Entre 2005 et 2008, les grands portails Amazon, eBay, Yahoo!, Microsoft ou AOL ont été remplacés dans le classement des 10 premiers sites consultés par Facebook, YouTube, Wikipédia. Les sites marchands ont été supplantés par les sites interactifs[203]. Ce changement se caractérise par l'importance de la participation des utilisateurs, de consommateurs qu'ils étaient jusque-là, ils peuvent devenir acteurs et auteurs sur le NET en intervenant par des commentaires ou en publiant des écrits personnels. Tout utilisateur de traitement de texte peut mettre en œuvre un blog sans connaissance technique particulière. Il peut aussi accéder aux blogs des autres internautes, ou aux encyclopédies ouvertes qui permettent à chacun de réagir aux articles publiés, d'y apporter des commentaires, voire, sur les Wikis, de modifier directement les articles.

Il peut aussi diffuser son opinion en utilisant les réseaux sociaux qui par contagion permettent de toucher des milliers de lecteurs. Comme l'écrivaient Patrick Bloche et Patrice Verchère[204] : « *La possibilité d'une transmission complète et instantanée d'informations dématérialisées nous permet, chaque jour, de communiquer avec nos proches et nos collègues, de profiter de biens et services culturels d'une diversité quasi infinie, de gérer à distance certaines formalités administratives, de prévoir au mieux nos itinéraires et temps de transport, de faire nos courses dans des magasins virtuels, de réserver des voyages, de comparer les prix des produits de grande consommation, de prendre part à des jeux virtuels en réseaux... ».*

Twitter et Facebook sont des accélérateurs de cette propagation des idées et des informations. Twitter est ainsi utilisé par les médias de l'information pour suivre en direct ou en léger différé un procès, un journaliste présent dans la salle d'audience utilisant Twitter pour commenter en direct les faits importants d'un procès[205].

---

[202] La liberté d'expression était, de fait, contingentée aux journalistes ou aux politiques, le WEB 2.0 permet à un plus grand nombre de personnes de s'exprimer et de diffuser cette expression. En fin d'année 2017, cette libération de la parole a pu être constatée avec le mouvement #metoo ou #BalanceTonPorc (Ronan Tésorière, « "Balance ton porc" : sur Twitter, des milliers de femmes racontent leur harcèlement sexuel », *Le Parisien,* 15 octobre 2017, URL : http://www.leparisien.fr/laparisienne/actualites/societe/balance-ton-porc-le-hashtag-qui-denonce-le-harcelement-sexuel-14-10-2017-7331730.php consulté le 23 mars 2018.

[203] Dominique Cardon, « Réseaux sociaux de l'Internet », *Communications* 2011/1 (n° 88), pp. 141-148.

[204] Patrick Bloche, Patrice Verchère, *Rapport d'information sur les droits de l'individu dans la révolution numérique*, Op. cit., p. 20.

[205] Par exemple, lors de la comparution du directeur général du FMI suite à une plainte d'une femme de ménage à New York le 16 mai 2011, ou au procès en Afrique du Sud d'un athlète soupçonné de meurtre en mars 2014.

D'autres réseaux, comme YouTube, permettent à partir de la caméra d'un smartphone de transmettre le film d'un événement. Les journaux en ligne donnent ainsi la parole à leurs lecteurs qui deviennent alors correspondants desdits journaux, fournissant reportage oral ou enregistrement vidéo des événements effectués avant l'arrivée des journalistes officiels. La liberté d'expression prend une dimension nouvelle qui rend possible la création d'événements de masse, dimension que ne pouvaient lui donner les médias traditionnels[206].

Cette facilité est aussi utilisée pour donner un avis sur un prestataire, un objet, un voyage. Les sites de vente en ligne donnent ainsi la parole aux usagers pour vanter un produit ou le critiquer. Cette pratique est d'ailleurs dévoyée et utilisée par les prestataires eux-mêmes pour donner des notes excellentes à leurs prestations car insuffisamment contrôlée[207]. Un encadrement et des limitations légales à ces commentaires sont régis par l'article 49 de la loi pour une République numérique[208], avec l'introduction de la notion de loyauté des plateformes et d'information loyale des consommateurs dans le Code de la consommation : « *Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente* ». Ces commentaires peuvent aussi relever de l'injure et de la diffamation, délits punis et sanctionnés par des peines d'emprisonnement et des amendes[209]. Le WEB 2.0 a créé un espace de liberté, chaque individu peut s'y exprimer en toute liberté, mais cet espace reste soumis à des contraintes légales[210] ou à des règles propres aux différents sites. La liberté non contrôlée ou non régulée peut induire des informations erronées difficilement vérifiables, mais un contrôle trop strict équivaut à l'établissement d'une censure.

---

[206] Patrick Bloche, Patrice Verchère, *Rapport d'information sur les droits de l'individu dans la révolution numérique*, enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011, p. 21.

[207] « Il crée un faux restaurant à Londres et en 6 mois, devient numéro 1 sur TripAdvisor », *Food & Sens,* 9 décembre 2017, URL : http://foodandsens.com/deniche-sur-le-web/cree-faux-restaurant-a-londres-6-mois-devient-numero-1-tripadvisor/ consulté le 23 mars 2018.

[208] Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF nº 0235 du 8 octobre 2016.

[209] Article 29 alinéa 1 et alinéa 2 de la loi du 29 juillet 1881.

[210] Contraintes liées aux limites du droit à la liberté d'expression et d'information, mais aussi au droit au respect de la vie privée et de la dignité humaine, ainsi qu'aux conditions générales d'utilisation mises en place par les fournisseurs de ressources.

A) Les fondements juridiques et l'encadrement de la liberté d'expression : de la presse écrite à l'Internet

La liberté d'expression a, de tout temps, été associée à la liberté de la presse, l'une étant le vecteur de l'autre. La liberté de la presse est « *la base de toutes les autres libertés »,* sans elle, *« il n'est point de nation libre* » disait Voltaire[211]. Pour lui, chaque citoyen peut imprimer ce qu'il veut. La liberté d'expression garantit à toute personne la possibilité d'émettre librement une opinion, positive ou négative, sur un sujet, une personne physique ou morale, une institution.

Historiquement, c'est en Angleterre que la première affirmation de la liberté de la presse intervient légalement avec l'abolition de l'obligation de l'autorisation préalable des publications[212]. Le droit pour tout citoyen d'exprimer ses opinions se généralise et sera complété par le droit d'être informé[213]. À l'opposé des pays sous influence de la Réforme qui sont attachés à la responsabilité individuelle, les révolutionnaires français ont souligné la nécessité de limiter cette liberté[214]. Les libertés d'expression et d'information vont connaître des mutations dues à Internet à la fin du XX^{e} siècle et au début du XXI^{e} siècle.

Avec le WEB et les réseaux sociaux, les frontières entre les différents supports, médias entre la communication institutionnalisée et la communication informelle, sont devenues plus floues. Et il en va de même pour les frontières entre communication de masse et communication ciblée, c'est-à-dire entre les contenus destinés à un groupe d'individus précis, articles scientifiques, et les contenus destinés à tous, informations générales ou articles de vulgarisation. Un article scientifique peut être mal assimilé par un néophyte qui propagera ainsi une information erronée dans ses pages personnelles. Une formation à l'évaluation des informations trouvées sur Internet semble nécessaire[215].

À côté d'articles professionnels, journalistes, universitaires ou scientifiques, se trouvent également des informations fournies par des amateurs sous forme d'articles de lecteurs devenus

---

[211] Voltaire, *Collection des lettres sur les Miracles à Genève et à Neufchâtel*, s.n. Neufchâtel, 1767.

[212] En 1694, la *Regulation Printing* Act annule la *Licensing Act* de 1662.

[213] Ainsi que précisé par l'article 15 de la Déclaration des droits de l'homme et du citoyen de 1789, après les articles 10 proclamant la liberté de pensée et d'opinions et l'article 11 la liberté d'exprimer ces opinions.

[214] Lire sur le sujet Henri Pigeat, « Liberté de la presse – Nuances transatlantiques », *Commentaire* 2003/1 (Numéro 101), pp. 103-110.

[215] « Évaluer l'information sur Internet : des outils pour éduquer », *Enseigner avec le numérique,* éduscol Ministère de l'éducation nationale, en ligne à l'URL : http://eduscol.education.fr/numerique/dossier/competences/rechercher/methodologie/evaluation consulté le 25 mars 2018.

rédacteurs, d'images et de films pris par les smartphones et les appareils photo numériques omniprésents, et de sujets développés et réalisés par les internautes (la presse écrite ou audiovisuelle utilise également ces sources pour des événements survenus hors de la présence d'un journaliste professionnel). Le journalisme contemporain est devenu largement interactif et utilise des sources multiplateforme[216]. La presse écrite devient une presse en ligne, les stations de radio développe des sites interactifs mêlant information écrite, parlée ou des scènes filmées dans leurs studios. Les chaînes de télévision et d'information en continu utilisent des séquences produites par d'autres chaînes de télévision ou des stations de radio, ainsi que des films enregistrés par les témoins d'un fait divers ou d'une catastrophe, faute d'avoir un correspondant sur place. Tout individu disposant d'un smartphone peut se transformer en correspondant de presse.

En France, la liberté d'expression est consacrée à l'article 11 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789[217]. À la même époque, aux États-Unis d'Amérique le premier amendement à la Constitution[218] en est le garant quasi absolu. Depuis, la liberté d'expression est garantie par plusieurs sources internationales. La liberté d'expression bénéficie d'une protection au niveau européen à travers l'article 10 de la Convention européenne des droits de l'homme du 3 septembre 1953[219], mais aussi par l'article 19 de la Déclaration

[216] Marta Severo, « L'information quotidienne face au Web 2.0. La stratégie multiplateforme de six quotidiens nationaux français », *Études de communication*, 2013/2 (n° 41), pp. 89-102. URL : https://www.cairn.info/revue-etudes-de-communication-2013-2-page-89.htm consulté le 7 décembre 2017.

[217] *Déclaration des droits de l'Homme et du citoyen*, 26 août 1789, article 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 à l'abus de cette liberté dans les cas déterminés par la loi.* ».

[218] Le premier amendement fait partie des dix amendements ratifiés en 1791 et connus sous le nom de Déclaration des Droits ou *Bill of Rights* en anglais.

[219] Convention européenne des droits de l'homme, 3 septembre 1953, article 10 : « *Liberté d'expression*
1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.
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.. ».

universelle des droits de l'homme du 10 décembre 1948[220] et plus récemment par les articles 10 et 11 de la Charte des droits fondamentaux de l'Union européenne[221].

La liberté d'expression est multiple et protéiforme[222], elle inclut les libertés de pensée, de conscience et d'opinion, ainsi que la liberté de communication[223]. Cette liberté est de fait protégée par des textes de niveau constitutionnel. La Déclaration de 1789[224], comme la Convention européenne des droits de l'homme[225] ou la Charte des droits fondamentaux de l'Union européenne[226], énonce que les limites de l'exercice d'une liberté ne peuvent être déterminées que par la loi. Mais les restrictions, conditions et éventuelles sanctions assorties doivent être nécessaires et la nécessité établie de manière convaincante[227], c'est-à-dire impliquer un « besoin social impérieux », et respecter une juste proportion[228] entre atteinte aux libertés et intérêts publics[229].

---

[220] *Déclaration universelle des droits de l'homme,* 10 décembre 1948, article 19 : « *Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit* ».

[221] Charte des droits fondamentaux de l'Union européenne *(2000/C 364/01)*, du 18 décembre 2000
« *Article 10 Liberté de pensée, de conscience et de religion*
1. Toute personne a droit à la liberté de pensée, de conscience et de religion. Ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privé, par le culte, l'enseignement, les pratiques et l'accomplissement des rites.
2. Le droit à l'objection de conscience est reconnu selon les lois nationales qui en régissent l'exercice.
Article 11 Liberté d'expression et d'information
1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.
2. La liberté des médias et leur pluralisme sont respectés ».

[222] Thomas Andrieu, « L'étude du Conseil d'État : « Inventaire méthodique et codification du droit de la communication » », *LEGICOM*, 2007/4 (N° 40), pp. 9-18. URL : https://www.cairn.info/revue-legicom-2007-4-page-9.htm consulté le 3 avril 2018.

[223] « *Les libertés de pensée, de conscience et d'opinion peuvent être incluses sous la dénomination de liberté d'expression dès lors qu'il s'agit d'exprimer, d'extérioriser sa pensée, ses croyances ou ses opinions. Il est également possible de parler de liberté de communication afin de mettre l'accent, d'une part, sur le droit pour chacun d'exprimer sa pensée sur n'importe quel support d'information ou de communication, et d'autre part, sur le droit d'accéder à la pensée d'autrui, autrement dit le droit à l'information* » (Laurent Pech, « Fasc. 1250 : Liberté d'expression : aperçus de droit comparé », *JurisClasseur*, 10 juillet 2010, mise à jour 15 avril 2012).

[224] Déclaration des droits de l'homme et du citoyen, article 4. « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi* ».

[225] Convention européenne des droits de l'homme, article 10 §2 et article 18.

[226] Charte des droits fondamentaux de l'Union européenne, Article 52 §1.

[227] Cour européenne des droits de l'homme, *Observer et Guardian Newspapers Ltd c/ Royaume-Uni*, arrêt du 26 novembre 1991, série A n° 216.

[228] Charte des droits fondamentaux de l'Union européenne, Article 52 §1, Op. cit.
Convention européenne des droits de l'homme, Article 18, Op. cit.

[229] Conseil constitutionnel, Décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*.

1) En France, une limitation provenant de la loi sur la liberté de la presse de 1881

En France, cette liberté trouve ses restrictions dans la loi sur la presse de 1881[230], loi qui a été modifiée par la loi de 2004 pour la confiance dans l'économie numérique (LCEN)[231] afin de prendre en compte le nouvel environnement créé par Internet[232]. La liberté d'expression ne doit pas nuire à autrui, à la sécurité de l'État et à la prévention du crime[233]. Comme l'écrivent les sénateurs François Pillet et Thani Mohamed Soilihi[234] : « *Tout en affirmant cette liberté [la liberté de la communication publique], la loi du 29 juillet 1881 fixe également le cadre de la répression de ces abus, considérant que répression n'est pas restriction de la liberté d'expression* ». Le 24 août 1789, Mirabeau déclarait[235] : « *On vous laisse une écritoire pour écrire une lettre calomnieuse, une presse pour un libelle, il faut que vous soyez punis quand le délit est consommé. Or ceci est répression et non restriction. C'est le délit que l'on punit, et l'on ne doit pas gêner la liberté des hommes sous prétexte qu'ils veulent commettre des délits* ».

a) La répression de l'injure et de la diffamation

L'injure et la diffamation sont des délits incriminés par les articles 29 à 35 quater de la loi sur la presse de 1881. La diffamation consiste à alléguer ou imputer à une personne ou un corps, un fait qui porte atteinte à son honneur ou à sa considération. L'injure est toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait[236].

[230] Loi du 29 juillet 1881, *Loi sur la liberté de la presse* parue au JORF du 30 juillet 1 881 p. 4201.
[231] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* parue au JORF nº143 du 22 juin 2004 p. 11168.
[232] Basile Ader, « La loi de 1881, réceptacle naturel de toutes les infractions de "publication", depuis la presse et l'imprimerie jusqu'à Internet *», LEGICOM* 2016/2 (nº 57), pp. 19-21.
[233] Voir supra la Convention Européenne des Droits de l'Homme, article 10 § 2.
[234] François Pillet, Thani Mohamed Soilihi, Rapport d'information *relatif à l'équilibre de la loi du 29 juillet 1881 sur la liberté de la presse à l'épreuve d'Internet* enregistré à la Présidence du Sénat le 6 juillet 2016.
[235] Cité dans François Pillet, Thani Mohamed Soilihi, Rapport d'information *relatif à l'équilibre de la loi du 29 juillet 1881 sur la liberté de la presse à l'épreuve d'Internet,* Op.cit.
[236] Loi du 29 juillet 1881 sur la liberté de la presse, article 29.

La loi pour la confiance dans l'économie numérique rappelle dans son article 1er la liberté de communication au public[237], et elle modifie l'article 23 de la loi sur la presse de 1881, réprimant l'incitation à commettre un crime ou délit en y ajoutant tout moyen de communication au public par voie électronique.

En ajoutant aux moyens traditionnels de communication, la multiplication des possibilités de publier et faire circuler l'information sur Internet, la loi du 29 juillet 1881 sur la liberté de la presse n'aura jamais eu autant d'importance. Elle constitue, en effet, la base des procès en matière d'injure ou de diffamation quel que soit le support utilisé[238]. La Cour de cassation affirme même que c'est la seule possibilité ouverte en justice pour se plaindre d'un abus de la liberté d'expression. En effet, par un arrêt en date du 11 février 2010[239], la première chambre civile de la Cour de cassation a clairement rappelé le principe de l'exclusion de toute action en réparation fondée sur l'article 1382 du Code civil[240]. De plus, avant la promulgation de la loi du 27 janvier 2017[241], le juge ne pouvait pas requalifier une infraction en cas de poursuite mal qualifiée, ce qui entraînait de facto l'abandon de ces poursuites.

Une des principales limitations de la liberté d'expression par tout moyen de communication électronique ou par la presse reste l'injure et la diffamation[242] prévues par les articles 23, 29 et 32[243] de la loi sur la presse du 29 juillet 1881, modifiée par la LCEN du 21 juin 2004. Mais

---

[237] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique , article 1er : « *La communication au public par voie électronique est libre.*
« L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle ».

[238] Nicolas Verly, « Le point sur la diffamation et l'injure pour les blogueurs, la responsabilité des éditeurs de sites en cas de contributions extérieures (commentaires, forums de discussion...) », *LEGICOM*, 2016/2 (N° 57), p. 35-43. URL : https://www.cairn.info/revue-legicom-2016-2-page-35.htm consulté le 23 mars 2018.

[239] Cour de cassation, 1ère chambre civile, 11 février 2010, no 08-22.111 : « *les abus de la liberté d'expression prévus et réprimés par la loi du 29 juillet 1881, tels que, en l'espèce, l'injure, ne peuvent être réparés sur le fondement de l'article 1382 du code civil* ».

[240] Code civil, article 1382 : « *tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer* », abrogé et repris par l'article 1240 à compter du 1er octobre 2016 (Ord. n° 2016-131, 10 février 2016).

[241] Loi no 2017-86 du 27 janvier 2017 *relative à l'égalité et à la citoyenneté* publiée au JORF no 24 du 28 janvier 2017, Chapitre IV : Dispositions améliorant la lutte contre le racisme et les discriminations ; Section 1 : Dispositions modifiant la loi du 29 juillet 1881 sur la liberté de la presse et le code pénal.

[242] Xavier Agostinelli, « Diffamation, injure et provocation à la discrimination raciale », *LEGICOM*, 2002/3 (N° 28), pp. 47-60. URL : https://www.cairn.info/revue-legicom-2002-3-page-47.htm consulté le 8 décembre 2017.

[243] Modifiée en son article 23 par la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), la loi sur la liberté de la presse du 29 juillet 1881 incrimine les infractions de diffamation et d'injure.
« *Article 23. — Seront punis comme complices d'une action qualifiée crime ou délit ceux qui, soit par des discours, cris ou menaces proférés dans des lieux ou réunions publics, soit par des écrits, imprimés, dessins,*

alors que le délai de prescription, de trois mois, institué par la loi de 1881 part du jour de la publication, le projet de loi pour la confiance dans l'économie numérique prévoyait de faire partir ce délai de prescription du dernier jour de la parution sur Internet du texte incriminé. Cette modification a fait l'objet d'une décision du Conseil constitutionnel[244] justifiée par : « *la différence de régime instaurée, en matière de droit de réponse et de prescription, par les dispositions critiquées dépasse manifestement ce qui serait nécessaire pour prendre en compte la situation particulière des messages exclusivement disponibles sur un support informatique* ». Le Conseil constitutionnel, qui semble accepter dans ses considérants que le support numérique puisse faire l'objet de différentiation de régime par rapport au support papier, rejette la différenciation proposée rappelant ainsi la nécessité d'égalité et de proportionnalité des moyens au but recherché[245]. Cette décision peut cependant sembler défavoriser les victimes. En effet, un écrit sur papier est vite oublié et peu accessible en cas de recherche alors qu'une publication sur Internet est mémorisée et peut être accédée facilement par un moteur de recherche. La date de constat de la publication avait été retenue par certains juges[246], d'autres avaient considéré la

gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués, mis en vente ou exposés dans des lieux ou réunions publics, soit par des placards ou des affiches exposés au regard du public, soit par tout moyen de communication au public par voie électronique, auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet.

« Cette disposition sera également applicable lorsque la provocation n'aura été suivie que d'une tentative de crime prévue par l'article 2 du code pénal ».

« Article 29. — Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés.

« Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure ».

« Article 32. — La diffamation commise envers les particuliers par l'un des moyens énoncés en l'article 23 sera punie d'une amende de 12 000 euros.

« La diffamation commise par les mêmes moyens envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée sera punie d'un an d'emprisonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement.

« Sera punie des peines prévues à l'alinéa précédent la diffamation commise par les mêmes moyens envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.

« En cas de condamnation pour l'un des faits prévus par les deux alinéas précédents, le tribunal pourra en outre ordonner l'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 du code pénal ».

[244] Conseil constitutionnel, Décision n° 2004-496 DC du 10 juin 2004 - *Loi pour la confiance dans l'économie numérique*. Journal officiel du 22 juin 2004, p. 11182.

[245] Philippe Blanchetier, « Point de départ du délai de prescription des délits de presse sur internet : l'occasion manquée », *La Semaine juridique. Édition générale*, 14 juillet 2004, n° 29, p. 10117.

[246] TGI Paris, 13 novembre 1998 : *Expertises* janvier 1999, p. 443.

publication sur Internet comme un acte continu[247]. Mais après quelques hésitations, la date de publication initiale avait déjà été retenue par la Cour de cassation dans deux de ses arrêts[248].

Le délai de prescription a été porté à un an dans le cas où la diffamation publique a été proférée en raison d'une discrimination spécialement interdite[249], par exemple une diffamation publique portant sur l'origine, le sexe, l'ethnie, la race, la religion, le handicap, un crime contre l'humanité. Une harmonisation du délai de prescription à un an pour les délits de presse racistes et discriminatoires, publics ou non, a été retenue dans la loi relative à l'égalité et à la citoyenneté[250] modifiant certains articles de la loi du 29 juillet 1881, mais il débute toujours au premier jour de la publication. Ainsi malgré une mise à jour renouvelée jusqu'au 20 juin 2015 de propos déposés initialement sur un site le 30 mai 2014, le Tribunal de Grande Instance de Paris[251] a rappelé que la prescription courait à partir de la première publication et que les faits litigieux devaient être décrits de façon précise. La publication de propos injurieux ou diffamatoires renouvelée sur Internet n'est donc pas considérée comme un délit répétitif, puisque lorsqu'un délit se renouvelle dans le temps, la prescription ne court qu'à compter du dernier de ces actes[252], confirmant ainsi que le délit de presse reste un délit instantané. La rediffusion ne constitue pas une réédition[253].

Le 14 septembre 2016, en commission spéciale, le Sénat a proposé un amendement, non voté, faisant démarrer le délai de prescription pour injure et diffamation sur Internet à la cessation de la publication des propos litigieux[254], sauf en cas de publication simultanée sur papier.

---

[247] Cour d'Appel Paris, 11e chambre. A, 15 déc. 1999, *Licra et a. c/ J.-L. Costes*.
Virginie Facchina, Philippe A. Schmidt, « La nécessaire adaptation du droit positif à Internet : un tournant jurisprudentiel en matière d'application des règles de prescription prévues par la loi sur la presse du 29 juillet 1881 », *La Semaine Juridique Edition Générale* n° 13, 29 Mars 2000, p. 10281.
TGI Paris, 17e ch., 6 déc. 2000, Carl Lang c/ Réseau Voltaire.
Agathe Lepage, « Détermination du point de départ de la prescription de l'article 65 de la loi du 29 juillet 1881 », *La Semaine Juridique Edition Générale* n° 17, 25 Avril 2001, p. 10515.

[248] Cour de cassation, chambre criminelle, 30 janv. 2001.
Cour de cassation, chambre criminelle, 16 oct. 2001, arrêt n° 6374.
Philippe Blanchetier, « Point de départ du délai de prescription des délits de presse sur internet : l'occasion manquée », *La Semaine juridique. Édition générale*, n° 7,13 février 2002, p. 10028.

[249] Article 48-5 de la loi du 29 juillet 1881 modifié par l'article 34 de la Loi nº 2007-297 du 5 mars 2007 *relative à la prévention de la délinquance*.

[250] Loi nº 2017-86 du 27 janvier 2017 *relative à l'égalité et à la citoyenneté*, publiée au JORF nº 0024 du 28 janvier 2017.

[251] Tribunal de Grande Instance de Paris, 17e ch. correctionnelle, jugement du 4 novembre 2016, *Messieurs X. et Y., le Procureur de la République / Monsieur Z., Ligne WEB Services et Adista.*

[252] Cour de cassation, Crim. 7 mai 1998, n° 97-81.102.

[253] Christine Courtin, « Prescription de l'action publique », *Répertoire de droit pénal et de procédure pénale* octobre 2015 (actualisée février 2017).

[254] Relaté par Marc Rees, « *Injure, diffamation : au Sénat, les délais de prescription sur Internet explosent* » le 15 septembre 2016 sur https://www.nextinpact.com/news/101368-injure-diffamation-au-senat-delais-prescription-sur-Internet-explosent.htm, consulté le 2 février 2017.

b) La répression de la haine raciale et de l'incitation au crime ou délit

La loi du 29 juillet 1881, outre les délits de diffamation et injures, a prévu une limitation liée aux propos racistes, homophobes, contraires aux bonnes mœurs et pouvant porter atteinte à l'ordre public, et a créé un certain nombre d'autres délits passibles de sanctions pénales[255], ces délits sont : les provocations aux crimes et délits ; les délits contre la chose publique ; les délits contre les personnes ; les délits contre les chefs d'État et agents diplomatiques étrangers ; les publications interdites. La loi Gayssot[256] y a ajouté la contestation de crime contre l'humanité[257]. Certains auteurs[258], compte tenu de l'existence dans le Code pénal d'un sous-titre consacré aux crimes contre l'humanité[259], s'interrogent sur le bien-fondé d'incriminer le négationnisme au titre de la loi sur la presse de 1881 et non de le faire par le Code pénal, ce qui augmenterait, en conséquence, le pouvoir d'investigation du juge d'instruction pour ces incriminations.

Dans son ordonnance du 9 janvier 2014, le Conseil d'État[260] rappelle que *« l'exercice de la liberté d'expression est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés »*, mais qu'il « *appartient aux autorités chargées de la police administrative de prendre les mesures nécessaires à l'exercice de la liberté de réunion ; que les atteintes portées, pour des exigences d'ordre public, à l'exercice de ces libertés fondamentales doivent être nécessaires, adaptées et proportionnées* ». Comme Jean-Yves Monfort[261] l'écrit dans le titre d'un article : « *Le racisme, le sexisme et l'homophobie ne sont*

[255] Loi du 29 juillet 1881, *Loi sur la liberté de la presse*, Chapitre IV : Des crimes et délits commis par la voie de la presse ou par tout autre moyen de publication.
[256] Loi nº 90-615 du 13 juillet 1990 *tendant à réprimer tout acte raciste, antisémite ou xénophobe* publiée au JORF nº 162 du 14 juillet 1990 p. 8333.
[257] Jean-Baptiste Perrier, « Le délit de négationnisme enfin examiné par le Conseil constitutionnel : tout ça pour ça ? », *Revue française de droit constitutionnel,* septembre 2016, n° 107, pp. 700-703.
Régine Dhoquois, « Les thèses négationnistes et la liberté d'expression en France », *Ethnologie française*, 2006/1 (Vol. 36), pp. 27-33. URL : https://www.cairn.info/revue-ethnologie-francaise-2006-1-page-27.htm consulté le 4 avril 2018.
[258] Bernard Jouanneau, « Répression du négationnisme : la voix dissonante », *LEGICOM* 2015/1 (nº 54), pp. 59-67.
[259] Code pénal, Livre II : Des crimes et délits contre les personnes, Titre Ier : Des crimes contre l'humanité et contre l'espèce humaine, Titre Ier : Des crimes contre l'humanité et contre l'espèce humaine, Chapitre Ier : Du génocide, articles 211-1 et 211-2.
[260] Conseil d'État, Ordonnance Nº 374508 du 9 janvier 2014, *Ministre de l'intérieur c/Société Les Productions de la Plume et M. Dieudonné M'Bala M'Bala.*
[261] Jean-Yves Monfort, « Le racisme, le sexisme et l'homophobie ne sont pas des "opinions" », *LEGICOM* 2015/1 (nº 54), pp. 77-81.

pas des "opinions" » et constituent un abus illicite de la liberté d'expression. Cet abus ne relève pas du code pénal, mais bien de la loi de 1881.

Mais l'incrimination de cet abus n'est pas simple, comme le montrent deux décisions de la Cour de cassation concernant Jean-Marie Le Pen qui a été jugé plusieurs fois pour incitation à la haine raciale. Ainsi, en 1993, il est poursuivi pour avoir prononcé dans l'émission télévisée « l'heure de vérité » des propos contre un danger mortel de colonisation de notre pays par le monde islamo-arabe. La Chambre criminelle de la Cour de cassation[262] a cassé la condamnation de la Cour d'appel attendu que ces propos ne visant pas une personne ni un groupe de personnes déterminées « *n'étaient pas de nature à inciter le public ni à la haine, ni à la violence, ni à la discrimination raciale* », et restaient dans les limites de la liberté d'expression. Mais quelques années plus tard, cette même chambre criminelle approuve une condamnation[263] pour provocation à la haine contre le même personnage politique en raison de propos tenus lors d'une interview, propos également dirigés vers l'immigration clandestine arabe. La Cour de cassation a refusé en 2010[264] et 2012[265] les demandes de Jean-Marie Le Pen de transmettre une demande de conformité de la loi Gayssot au Conseil constitutionnel[266].

Les hommes politiques utilisent la diffamation ou l'injure pour ester en justice contre des journalistes ou leurs homologues, mais ils disposent d'une certaine immunité. En effet, les parlementaires[267] sont protégés par l'article 41 de la loi du 29 juillet 1881[268] au sein de leur assemblée, leurs propos et discours ainsi que la relation de ces propos et discours par tout moyen de communication ne peuvent être poursuivis en justice, seule une sanction disciplinaire peut être prononcée. Cette irresponsabilité ne concerne que les parlementaires, les ministres ne bénéficient pas de cette mansuétude[269]. Elle ne protège pas non plus les parlementaires en

[262] Cour de cassation, Chambre criminelle, Affaire nº 89-83 298, arrêt du 8 juin 1993.
[263] Cour de cassation, Chambre criminelle, Affaire nº 93-82.552, arrêt du 27 juin 1995.
[264] Cour de cassation, 7 mai 2010, Affaire n° 09-80.774.
[265] Cour de cassation, 10 octobre 2012, Affaire n° 12-81.505.
[266] Lire les commentaires de Anne-Marie Le Pourhiet, « Politiquement correct, mais juridiquement incorrect », *Constitutions* 2010 p.583, 15 septembre 2010 ; Jean Barthélémy, Louis Boré, « La chose jugée sur la QPC devant les juridictions de filtrage », Constitutions 2012 p.583
[267] Didier Baumont, *Liberté d'expression et irresponsabilité des députés*, accessible à https://www.unicaen.fr/puc/images/crdf0202baumont.pdf, consulté le 4 février 2017.
[268] Loi du 29 juillet *1881sur la liberté de la presse*, article 41 : « *Ne donneront ouverture à aucune action les discours tenus dans le sein de l'Assemblée nationale ou du Sénat ainsi que les rapports ou toute autre pièce imprimée par ordre de l'une de ces deux assemblées. […]* ».
[269] Madame Ségolène Royal, alors ministre déléguée à l'enfance et à la famille, est comparue en mai 2000, devant la Cour de justice de la République pour « complicité de diffamation envers des fonctionnaires publics » (Armelle Thoraval, « Ségolène Royal relaxée avec les félicitations de la Cour. La ministre était jugée pour diffamation envers deux enseignants », *Libération,* 17 mai 2000).

dehors de l'enceinte de leur Assemblée. Cette irresponsabilité dont bénéficient les parlementaires vise à ce que leurs travaux ne soient pas entravés ni par les citoyens, ni par les juges, ni par le gouvernement[270]. Cette immunité est largement admise dans les Parlements européens et acceptée par la Cour européenne des droits de l'homme[271].

Cet article 41 étend cette immunité à la relation des débats parlementaires ainsi qu'à la relation des débats judiciaires en cas de compte rendu « fidèle fait de bonne foi ». Mais comme le montre un arrêt du Tribunal correctionnel de Paris[272], le commentaire d'une décision de justice doit rester « basé factuellement sur la motivation même de cette décision » pour ne pas être incriminé de diffamation. La liberté académique du chercheur doit être précisée pour éviter les « poursuites-baillons »[273], poursuites qui n'ont pour seul but que d'éviter des publications gênantes par une autocensure de l'auteur face au coût d'un procès prévisible[274].

La liberté d'expression trouve ainsi des limites dans la protection de l'individu et dans la protection de l'État et de la société à partir de ces incriminations, mais ces limitations doivent être nécessaires, proportionnées et adaptées. Ces trois critères sont également utilisés par le Conseil constitutionnel lors de l'examen de la constitutionnalité des textes législatifs qui lui sont soumis pour atteintes aux libertés[275]. La poursuite pour diffamation ou injure est donc possible devant les tribunaux, son auteur est pénalement responsable s'il est connu. Mais le directeur de la publication peut aussi être poursuivi[276].

---

[270] Michel Ameller, *L'Assemblée nationale*, Paris, PUF (Que sais-je ?), 1994 : « *Toute atteinte au dogme de l'irresponsabilité parlementaire porte en elle le germe d'une régression du droit républicain, et partant, des libertés essentielles* ».

[271] Cour européenne des droits de l'homme, *Affaire A. c/ Royaume-Uni*, Requête no 35373/97, Arrêt du 17 décembre 2002 ; Cour européenne des droits de l'homme, *Affaire Cordova c/ Italie (nº 1)*, Requête no 40877/98, Arrêt du 30 janvier 2003.

[272] Tribunal correctionnel de Paris, 17e chambre correctionnelle, *Affaire CHIMIREC c/ Laurent NEYRET*, jugement du 13 janvier 2017, confirmé par la Cour d'Appel de Paris le 28 septembre 2017, n° 17/00854.

[273] Lire Charles Fortier, « Vers un régime juridique de la diffamation propre aux universitaires », 6 novembre 2017, *AJDA* 2017, p.2097.

[274] « Des journalistes et des ONG dénoncent des "poursuites bâillons" de la part du groupe Bolloré », *Le Monde*, 24 janvier 2018, URL : http://www.lemonde.fr/idees/article/2018/01/24/des-journalistes-et-des-ong-denoncent-des-poursuites-baillons-de-la-part-du-groupe-bollore_5246496_3232.html consulté le 23 mars 2018.

[275] Cf. Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 1. § 2 -A)1)c) La jurisprudence du Conseil constitutionnel dans la lutte contre le terrorisme.

[276] Les dérogations prévues à la disposition des États membres par le 2 de l'article 85 du règlement général sur la protection des données peuvent entraîner des difficultés opérationnelles comme l'indique la CNIL dans son avis (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* Op. cit.).

c) La responsabilité pénale issue de la loi pour la confiance dans l'économie numérique

La quasi-totalité du régime de responsabilité éditoriale des services de communication au public en ligne réside dans le long article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[277]. Celui-ci renvoie expressément, pour certaines règles communes, aux régimes de responsabilité éditoriale de la presse et de l'audiovisuel, en transposant les responsabilités des acteurs de la presse traditionnelle aux acteurs de la publication en ligne.

La loi du 29 juillet 1881 prévoit l'établissement d'un régime de responsabilité pénale spécifique instituant une présomption de responsabilité du directeur de la publication, puis à défaut des auteurs, puis à défaut des imprimeurs, puis à défaut des vendeurs[278], et la mise en place d'un régime procédural particulier, dérogeant au droit commun, avec des règles contraignantes limitant les poursuites, notamment une prescription des infractions réduite à trois mois, sauf exceptions, à compter de la publication des propos incriminés, afin de protéger la liberté de la presse. Le directeur de la publication, présumé responsable, est censé avoir eu connaissance des écrits et en avoir approuvé la publication. La poursuite des autres participants à l'infraction de presse est exercée selon le droit commun de la complicité[279].

La loi pour la confiance dans l'économie numérique (LCEN) distingue trois principaux acteurs responsables sur le réseau : le fournisseur d'accès Internet (FAI)[280] ; l'hébergeur, non responsable des contenus qu'il héberge, sauf s'il acquiert la connaissance du caractère illicite de ceux-ci et qu'il n'agit pas promptement pour les retirer ou en interdire l'accès[281] ; l'éditeur de service[282], classiquement responsable des contenus qu'il choisit de mettre en ligne, qui est l'équivalent du directeur de la publication de la presse écrite, il est pénalement responsable des éventuels propos litigieux diffusés sur un site[283]. La responsabilité pénale des auteurs de propos illicites est reconnue par la loi, et les fournisseurs d'accès ou les hébergeurs doivent pouvoir sur réquisition de l'autorité judiciaire, fournir les informations permettant d'identifier les

[277] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* publiée au JORF nº143 du 22 juin 2004 p. 11168.
[278] Christophe Bigot, « Exposé introductif : les spécificités de la loi de 1881 concernant tant le régime de responsabilité en cascade que celui des règles dérogatoires de procédure et de prescription », *LEGICOM*, 2006/1, n° 35, pp. 21-23. URL : https://www.cairn.info/revue-legicom-2006-1-page-21.htm consulté le 11 décembre 2017.
[279] Code pénal, article 121-7.
[280] LCEN, article 6-I-1.
[281] LCEN, article 6-I-2.
[282] LCEN article 6 - III.
[283] Code pénal, articles 93-2 et 93-3 et Loi nº82-652 du 29 juillet 1982 *sur la communication audiovisuelle.*

auteurs de ces propos illicites. De plus, la loi pour la confiance dans l'économie numérique (LCEN) a prévu dans son article 6, que les fournisseurs d'accès Internet et les hébergeurs doivent faire diligence pour empêcher l'accès à tout propos illicite dès qu'ils sont informés de l'illicéité de ces propos, cette diligence les exonère alors de toute responsabilité pénale[284].

Si ces fournisseurs d'accès ou hébergeurs ne sont pas tenus de surveiller les propos échangés sur leur site ou leur réseau, la même loi les oblige à mettre en place un dispositif de signalisation de certains propos contraires à l'ordre public[285] : apologie des crimes contre l'humanité ; incitation à la haine raciale ; pornographie enfantine. Tout signalement abusif ou toute demande abusive de retrait de propos illicites est sanctionné pénalement[286], ce qui permet d'éviter des abus ou des censures de certains propos non légalement illicites. Ainsi, à travers la limitation de responsabilité de cet article 6 de la LCEN, ce sont les hébergeurs ou, à défaut, les fournisseurs d'accès, qui doivent mettre promptement en œuvre les moyens de faire cesser les publications pénalement incriminables. Mais par la possibilité pour les usagers de signaler tout propos condamnable, la loi pour la confiance dans l'économie numérique institue légalement un régime de dénonciation. Le régime de responsabilité allégé pour l'éditeur et le producteur[287] n'a pas été modifié par la loi pour une République numérique, malgré l'arrêt du 16 juin 2015

[284] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique,* article 6 alinéa 3 *: « 3. Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.*
« L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa. »

[285]Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique,* article 6 alinéa 7 : « *7. Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.*
« Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.
« Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et à l'article 227-23 du code pénal.
« À ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.
« Tout manquement aux obligations définies à l'alinéa précédent est puni des peines prévues au 1 du VI. »

[286] Un an d'emprisonnement et 15 000 EUR d'amende

[287] Nicolas Verly, « Le point sur la diffamation et l'injure pour les blogueurs, la responsabilité des éditeurs de sites en cas de contributions extérieures (commentaires, forums de discussion...) », *LEGICOM* 2016/2 (nº 57), pp. 35-43.

de la Cour européenne des droits de l'homme[288] qui semble valider une obligation générale de surveillance pour les portails d'actualité en ligne commerciaux[289].

2) En Europe, un encadrement généralisé

La liberté d'expression est indissociable de la liberté de la presse. Mais si l'article 10, alinéa 1er de la Convention européenne des droits de l'homme consacre la liberté d'expression, son alinéa 2[290] précise que l'exercice des libertés comporte des devoirs et obligations et donc que cet exercice peut être conditionné au respect de certaines règles et conditions.

La Cour européenne des droits de l'homme a eu à se prononcer sur la liberté d'expression et la violation de l'article 10 de la convention européenne des droits de l'homme. En particulier dans l'affaire dite « du canard enchaîné », elle énonce : « *La liberté d'expression vaut non seulement pour les "informations" ou "idées" accueillies avec faveur et considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de "société démocratique" »*[291]. Elle rappelle ainsi que la démocratie ne peut pas exister sans respect de la liberté d'expression.

Dans les pays sortant du fascisme en 1945, les constitutions promulguées après la fin de la guerre protègent la liberté d'expression. Elles prévoient un encadrement de cette liberté par la loi (a).

En Angleterre, pays de tradition libérale, il n'existe pas de texte unique consacrant la liberté d'expression, mais les fondements de cette liberté sont anciens, répartis entre textes et jurisprudence qui protègent l'individu contre l'arbitraire du pouvoir royal et lui garantissent la liberté de culte. La conception britannique de la liberté d'expression est différente de la conception française, mais il y existe plusieurs restrictions. En 1936, un juge du *Privy Council*

---

[288] Cour européenne des droits de l'homme, Grande chambre, Affaire *Delfi c/ Estonie*, Requête no 64569/09, Arrêt du 16 juin 2015.

[289] Katarzyna Blay-Grabarczyk, « Conventionnalité de la condamnation d'un exploitant de portail d'actualités sur Internet en raison de commentaires injurieux », *La Semaine Juridique Edition Générale* no 27, 6 Juillet 2015, 798.

[290] Convention européenne des droits de l'homme, article 1, alinéa 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* ».

[291] Cour européenne des droits de l'homme, 21 janvier 1999, no 29183/95, *Fressoz et Roire c/ France, plus communément appelé l'affaire du canard enchainé.*

a ainsi résumé ce qu'est la liberté d'expression[292] : *« free speech does not mean free speech […] it means freedom governed by law »*[293]. Au Royaume-Uni, pays de la liberté d'expression, cette liberté est encadrée par le législateur (par promulgation de loi ou Act), mais aussi par les juges (common law ou case law) afin de protéger les personnes et l'État, voire l'Église (b).

a) Une protection constitutionnelle en réaction au fascisme

En République fédérale d'Allemagne, la liberté d'expression est consacrée par l'article 5 al.1er de la Loi fondamentale[294] : « *Chacun a le droit d'exprimer et de diffuser librement son opinion, par l'écrit et par l'image, et de s'informer sans entraves aux sources qui sont accessibles à tous. […] La censure n'existe pas »*[295]. Le texte allemand relie ainsi la liberté d'expression à la liberté d'information, chacun est libre de puiser son information dans les sources existantes et d'exprimer son opinion librement. Ces libertés constitutionnellement garanties et protégées sont la réaction aux exactions du régime nazi[296], régime autoritaire qui a suspendu les dispositions de la Constitution allemande qui protégeaient les libertés individuelles, qui brûlait les livres non autorisés et qui muselait toute opposition par l'assassinat ou l'internement[297].
Cet article 5 précise : « *Ces droits trouvent leurs limites dans les prescriptions des lois générales, dans les dispositions légales sur la protection de la jeunesse et dans le droit au respect de l'honneur personnel »*[298]. Mais pour la Cour constitutionnelle fédérale, étant donné l'importance essentielle du droit fondamental, il ne serait pas logique d'accepter que la portée matérielle de ce droit fondamental puisse être relativisée par une simple loi[299].

---

[292] Related by Rosalind Croucher, "ALRC Inquiry into Freedoms", in *Free Speech 2014 Symposium Papers,* 7 August 2014, p. 10, in line at URL: https://www.humanrights.gov.au/sites/default/files/document/publication/free-speech-report2014.pdf consulted on 3 April 2018.
[293] La liberté d'expression ne signifie pas liberté d'expression … cela signifie liberté régie par la loi.
[294] Grundgesetz für die Bundesrepublik Deutschland, GG, 23 Mai 1949.
[295] Art 5 (1) „*Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt*".
[296] Johann Chapoutot, *Fascisme, nazisme et régimes autoritaires en Europe (1918-1945)*, août 2013, Presses Universitaires de France.
[297] Lire entre autres sur le sujet « Le début de la terreur nazie » dans *Encyclopédie multimédia de la Shoah »* en ligne à https://www.ushmm.org/wlc/fr/article.php?ModuleId=290# consulté le 8 décembre 2017.
[298] Art 5 (2) „*Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre*".
[299] Cour constitutionnelle fédérale d'Allemagne, *Affaire Lüth/Harlan (Rayonnement des droits fondamentaux en droit civil)* Arrêt de la Première Chambre du 15 janvier 1958 (Recueil des décisions de la Cour constitutionnelle fédérale, BVerfGE, t. 7, pp. 198-230).

Sous le régime fasciste de Mussolini[300], l'Italie a fait aussi l'expérience d'une suppression substantielle de la liberté de presse, en dépit de l'énoncé du Statut de 1848 formellement en vigueur pendant cent ans, et aux termes duquel « *La presse sera libre, mais une loi en réprimera les abus* »[301].

Depuis la promulgation de la Constitution[302] de 1948, la liberté d'expression a été constitutionnalisée comme l'expose Valério Onida, ancien président de la Cour constitutionnelle italienne[303]. L'Assemblée constituante a établi des règles et des garanties précises, censées défendre cette liberté fondamentale. Avec l'article 21 de la Constitution, les constituants ne se sont pas accommodés de proclamations telles que « *Chacun a le droit de manifester librement sa pensée à l'oral, à l'écrit et à travers tout autre moyen de diffusion* »[304], en posant par là un principe susceptible d'intéresser tout moyen et toute forme d'expression et de divulgation de la pensée et des informations. Ils ont également précisé que « *la presse ne peut être assujettie à des autorisations ou censures* »[305], et que « *l'on ne peut procéder à une saisie qu'en présence d'un acte émis par l'autorité judiciaire en cas de délits pour lesquels l'autorisation expresse de la saisie est sanctionnée par la loi sur la presse, ou en cas de violation des dispositions visées par cette même loi, relatives à la désignation des responsables* »[306].

L'œuvre constitutionnelle et législative[307] de l'Assemblée constituante est le témoignage de l'extrême sensibilité des constituants à la question de la liberté d'expression, qui est ainsi « matière constitutionnelle ». Au cours des premières années succédant à l'entrée en vigueur de la Constitution, avant la mise en place de la Cour constitutionnelle, la jurisprudence de la Cour de cassation classait l'article 21 de la Constitution au nombre des normes dites « *programmatiques* », donc, non susceptibles de produire, en tant que telles, des effets immédiats, et ne pouvant être mises en œuvre que par l'intervention du législateur. La Cour constitutionnelle, dans son premier arrêt[308], déclarait une loi « illégitime », car contraire à

[300] Johann Chapoutot, *Fascisme, nazisme et régimes autoritaires en Europe (1918-1945)*, août 2013, Presses Universitaires de France, Op. cit.
[301] Constitution du royaume de Sardaigne, puis du royaume d'Italie, Statut Albertin - 1 848, Article 28.
[302] Costituzione della Repubblica Italiana, promulguée le 27 décembre 1947, entrée en vigueur le 1 janvier 1948.
[303] Valério Onida, Professeur à l'Université de Milan, ancien membre et président de la Cour constitutionnelle italienne. « La liberté d'expression en Italie : un regard d'ensemble », in *CRDF*, n°8, 2010 pp. 27-32.
[304] Constitution de la République italienne, art. 21, 1er alinéa, « *Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione* ».
[305] Constitution de la République italienne, art. 21, 2e alinéa.
[306] Constitution de la République italienne, art. 21, 3e alinéa.
[307] Loi n° 47 du 8 février 1948.
[308] Italie, Cour constitutionnelle, Arrêt n°1 du 5 juin 1956.

l'article 21 de la Constitution. Mais, l'abondante législation, datant de l'époque fasciste, au sujet des délits « d'opinion » et de bien d'autres aspects intéressant les limites de la liberté d'expression, restera en vigueur pendant de nombreuses années avant d'être progressivement frappée d'inconstitutionnalité partielle par quelque deux cents décisions en soixante ans[309].
Le juge constitutionnel a de plus précisé que la liberté d'expression ne se heurte pas seulement aux limitations de l'article 21 de la Constitution, mais aussi à l'obligation de protéger l'ordre public[310], à l'interdiction de l'apologie de crimes[311]. Il admet les sanctions pénales pour outrage aux institutions ou à la religion[312].
Dans ces pays, comme en Espagne ou au Portugal, après une période où les libertés ont connu de fortes restrictions, la liberté d'expression est protégée directement par la Constitution ou son équivalent, mais aussi sanctionnée en cas d'abus. Ces limitations législatives sont acceptées dans toute l'Europe continentale comme une protection contre les abus et un reniement de l'histoire. Au Royaume-Uni, comme précisé ci-dessous, les limites de cette liberté d'expression proviennent de la jurisprudence et accessoirement de la loi, la tradition en est ancienne et la responsabilité de la personne est primordiale.

b) Des limites anciennes en Common Law au Royaume-Uni

Aucune Constitution écrite n'existant, la *Common Law* et le principe de la primauté du droit, de façon non écrite, assurent aux citoyens leurs libertés. Le juge a un pouvoir important dans l'estimation de la violation de cette liberté. Trois textes, même s'ils ne consacrent pas expressément la liberté d'expression, peuvent être cités comme fondateurs des libertés, dans la mesure où ils constituent les premiers textes constitutionnels de l'Angleterre et montrent que l'homme est naturellement libre et propriétaire de biens avant d'être sujet du Roi. Tout d'abord, la Grande Charte[313], imposée en 1215 au Roi par les barons du royaume, tient lieu de document constitutionnel, et garantit contre l'absolutisme royal les droits et privilèges des seigneurs féodaux. Puis, l'*Habeas Corpus Act* de 1679, loi votée par le Parlement, précise les bases de la liberté individuelle contre l'arbitraire royal. Enfin, le schisme de l'Église d'Angleterre, consacré par l'Acte de Suprématie, voté en 1534, ouvre la voie à davantage de tolérance religieuse, de

[309] Valério Onida, « La liberté d'expression en Italie : un regard d'ensemble » Op. cit.
[310] Italie, Cour constitutionnelle, Arrêt n°19 de 1 962 et arrêt n°199 de 1 972.
[311] Italie, Cour constitutionnelle, Arrêts n°1 de 1 957, n°87 de 1966, n°65 de 1970 et n°16 de 1973.
[312] Italie, Cour constitutionnelle, Arrêt n°20 de 1 974 et arrêt n°188 de 1975.
[313] *Magna Carta Libertatum*, 15 juin 1215.

garantie des libertés individuelles. En 1694, la *Regulation Printing Act* annule la *Licensing Act*[314] *de 1662*, c'est-à-dire le système d'autorisation préalable à toute impression[315], affirmant ainsi la liberté de la presse[316]. Elle ouvre la voie à la parution en 1702 du premier journal quotidien anglais, le *Daily Courant*.

Parmi les conquêtes arrachées au XVIII[e] siècle, figurent les jugements rendus dans les deux affaires, Leach c/ Monety[317] et Entick c/ Carrington[318]. Ces arrêts mettent fin au privilège qu'avait l'exécutif de délivrer des mandats d'arrêt contre toute personne suspectée de publication diffamatoire, d'effectuer des perquisitions à son domicile, ou de prononcer la saisie de sa publication. Tout au long du XVIII[e] siècle, les journalistes anglais sont confrontés à de nombreuses difficultés et notamment les poursuites judiciaires pour diffamation. Les délits de presse sont à cette époque jugés par des juges professionnels liés au pouvoir royal, et non par des jurys, issus du peuple et plus tolérants. Mais en 1792, le Parlement vote le *Libel Act*[319], qui transfère au jury la vocation de juger les délits de presse. Désormais, à partir du XIX[e] siècle, la liberté d'expression et de la presse va se consolider et s'institutionnaliser en s'éloignant du pouvoir royal[320].

De nouveaux textes vont, au XX[e] siècle, protéger la personne et les mœurs[321]. Concernant la protection de la personne[322], la Commission d'examen des plaintes en matière de déontologie (*the Press Complaints Commission*), organisme indépendant créé en 1991, veille à ce que les journaux et magazines britanniques respectent le code de déontologie adopté le 16 novembre

[314] La loi d'autorisation de la presse (*Licensing Act* 1662) est une loi du Parlement anglais (13 & 14 Car. II. ch. 33), dont le titre est "*An Act for preventing the frequent Abuses in printing seditious treasonable and unlicensed Bookes and Pamphlets and for regulating of Printing and Printing Presses."* soit « une loi pour prévenir les abus fréquents dans l'impression de livres et de pamphlets séditieux, traites et non autorisés et pour réguler l'imprimerie et la presse écrite ».

[315] Lyman Ray Patterson, "Copyright And `The Exclusive Right' Of Authors"*, Journal of Intellectual Property*, Vol. 1, No.1 Fall 1993. URL: http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1342&context=fac_artchop, consulté le 2 février 2015.

[316] Henri Pigeat, « Liberté de la presse. Nuances transatlantiques », *Commentaire*, 2003/1 (Numéro 101), pp. 103-110. URL : https://www.cairn.info/revue-commentaire-2003-1-page-103.htm consulté le 3 avril 2018.

[317] *Leach v. Money* (1763), 19 State Trials 981.

[318] *Entick v Carrington* (1765), 19 State Trials 1029.

[319] *Libel Act* 1792 Chapter 60 32 Geo 3, *An Act to remove Doubts respecting the Functions of Juries in Cases of Libel.*

[320] Céline Boyer, « La liberté d'expression au Royaume-Uni », 17 février 2005, *e-juristes,* URL : http://www.e-juristes.org/la-liberte-d-expression-au-royaume/ consulté le 23 mars 2018.

[321] Au Royaume-Uni (Angleterre et Pays de Galles), l'homosexualité a été considérée comme un crime jusqu'en 1967 (*Sexual Offences Act* 1967).

[322] Éric Barendt, « La protection de la vie privée en Angleterre », *LEGICOM*, 1999/4 (N° 20), pp. 115-120. URL : https://www.cairn.info/revue-legicom-1999-4-page-115.htm consulté le 3 avril 2018.

1997[323] qui repose sur le principe de l'autoréglementation. Même si les questions d'ordre juridique ne sont pas de son ressort, elle assure un juste équilibre entre la protection du droit à l'information et la protection des droits des particuliers. Sa compétence s'étend à des questions telles que l'exactitude des faits rapportés[324], le bien-être des enfants[325], le respect de la vie privée[326], l'obligation de ne pas divulguer l'identité des victimes d'agressions sexuelles, et la protection du caractère confidentiel des sources. Cette protection relève ainsi d'un autocontrôle et du droit mou ou *Soft Law* en anglais. La commission a été remplacée le 8 septembre 2014 par *l'Independant Press Standards Organization* ou IPSO[327]. Comme indiqué sur son site[328], l'IPSO est le régulateur indépendant de la plupart des journaux et magazines du Royaume-Uni. Il protège les droits des personnes, maintient un haut niveau des standards journalistiques et aide à défendre la liberté d'expression. Alors que la PCC pouvait négocier des remèdes aux plaintes, l'IPSO peut infliger des amendes[329].

L'incitation à la haine raciale qui pouvait donner lieu à plainte auprès de la PCC, est également définie comme infraction par *The Public Order Act* de 1986[330]. La section 17 définit la haine raciale comme étant la haine à l'égard d'un groupe de personnes, défini par référence à sa couleur, sa race, sa nationalité, ou son origine nationale ou ethnique[331].

Concernant la protection des mœurs, la loi de 1959 et 1964, *the Obscene Publications Act* (OPA)[332], prohibe tout document qui, pris dans son ensemble, tend à « dépraver et corrompre » ceux qui le voient ou l'entendent. D'après *the Protection of Children Act* de 1978[333], le fait de prendre, distribuer, afficher ou faire la publicité d'une photo, d'une vidéo ou d'un film indécent d'un enfant de moins de 16 ans est une infraction. De la même manière, *the Criminal Justice Act* de 1988[334] a introduit une nouvelle infraction, celle de posséder une photo indécente d'un

[323] *Editors' Code of Practice*, initialement adopté le 16 novembre 1997, la dernière version a pris effet le 1er janvier 2016 (disponible à https://www.ipso.co.uk/media/1058/a4-editors-code-2016.pdf) .
[324] Press Complaints Commission, Complaints *Carrie Twomey*, 21/01/2015, *Mr Henry Kirkland*, 21/01/2015, *Dr Stephen Ferguson,* 12/09/2014.
[325] Press Complaints Commission, Complaints *Dr Sarah Wollaston MP*, 20/10/2015, *Ms Pip Quinn*, 06/10/2014, *A woman*, 05/06/2014.
[326] Press Complaints Commission, Complaints *Ms Lindsey Talbott*, 18/12/2014*, A woman*, 25/11/2014.
[327] Comme indiqué sur la page d'accueil du site http://www.pcc.org.uk/ .
[328] https://www.ipso.co.uk/ .
[329] Comme précisé sur sa page d'accueil à l'URL ci-dessus.
[330] *Public Order Act* 1986 Ch. 64.
[331] *Public Order Act* 1986 "*17. In this Part "racial hatred" means hatred against a group of persons in Great Britain defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins".*
[332] *Obscene Publications Act* 1959 7&8 Eliz.2 Ch. 66; *Obscene Publications Act* 1964 Eliz. 2 Ch. 74.
[333] *Protection of Children Act* 1978 Ch.37.
[334] *Criminal Justice Act* 1988 Ch. 33.

enfant de moins de16 ans. Enfin, le dernier texte est le *Sex Offence Act* de 2003[335], qui modifie certains des textes précédemment cités. La pédopornographie sur Internet est un crime.

D'autres infractions liées à la liberté d'expression existent. Elles concernent la protection du sacré et de l'État. Il existait ainsi une infraction de *Common Law*, appelée *blasphemy* ou *blasphemous libel*[336], c'est-à-dire le fait d'exprimer un manque de respect à l'égard de Dieu ou quelque chose de sacré, cette infraction n'a été abolie qu'en 2008, par le *Criminal Justice and immigration Act* de 2008[337]. Il est à noter qu'en France, le blasphème a été supprimé du droit par la loi du 29 juillet 1881 sur la presse et la loi du 9 décembre 1905 concernant la séparation des Églises et de l'État, mais qu'il a perduré en Alsace-Lorraine jusqu'en janvier 2017[338]. Après les attentats de Charlie hebdo de janvier 2015, certaines associations ont demandé le rétablissement de la pénalisation du blasphème au titre du respect des religions[339].

Enfin, une dernière catégorie de restriction à la liberté d'expression tient à la protection non plus de la personne, mais de l'État. En effet, tout d'abord il existait une infraction de sédition, révolte organisée contre l'autorité de l'État, soulèvement, insurrection contre l'ordre établi, qui était une infraction de *common law.* La sédition est définie comme une intention de développer la haine, le mépris ou le mécontentement contre le Monarque, le gouvernement ou la Constitution du Royaume-Uni, l'administration de la Justice[340]. Cette infraction a été abolie par la section 73 du *Coroners and Justice Act* de 2009[341] avec effet au 12 janvier 2010. Mais une deuxième restriction à la liberté d'expression dans le but de protéger l'État tient à la notion de secrets officiels. La loi de 1989 sur les secrets officiels (*Official Secrets Act* 1989) définit quatre catégories d'informations strictement protégées : les informations que le gouvernement considère comme préjudiciables à la défense nationale ; celles transmises à titre confidentiel à d'autres États ou à des organisations internationales ; celles se rapportant aux activités des services de sécurité et de renseignements ; celles relatives aux relations internationales.

---

[335] *Sexual Offences Act* 2003 Ch. 42.
[336] *Criminal Libel Act* 1819 and *Libel Amendment Act* 1888.
[337] *Criminal Justice and Immigration Act* 2008 Ch. 4. *Part 5 Blasphemy "79 Abolition of common law offences of blasphemy and blasphemous libel".*
[338] À la fin de l'annexion de l'Alsace-Lorraine par l'Allemagne en 1918, le blasphème a été réintroduit en droit français par l'incorporation de l'article 166 du code pénal allemand. Il est abrogé par la loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté, art. 172.
[339] Jacques de Saint-Victor, « Du blasphème dans la République », *Le Débat*, 2015/3 (n° 185), pp. 11-20. URL : https://www.cairn.info/revue-le-debat-2015-3-page-11.htm consulté le 14 mars 2018.
[340] Le dernier procès pour sédition s'est tenu en 1972.
[341] Coroners and Justice Act 2009, Part 2, Chapter 3, section 73 : "*Abolition of common law libel offences etc The following offences under the common law of England and Wales and the common law of Northern Ireland are abolished - (a) the offences of sedition and seditious libel; (b) the offence of defamatory libel; (c) the offence of obscene libel*".

Les lois du Royaume-Uni limitant la liberté d'expression prennent en compte Internet. Ainsi, la loi de 1996, *the Defamation Act 1996*, qui régule la diffamation, s'applique à Internet, et aux fournisseurs d'accès. Il dispose qu'une personne peut être mise hors de cause si elle prouve : qu'elle n'est ni l'auteur, ni le rédacteur, ni l'éditeur des informations faisant l'objet de la plainte ; qu'elle a suffisamment fait attention lors de la publication[342] ; et qu'elle n'avait aucune intention de diffamer ou n'avait aucune connaissance du caractère diffamatoire des informations litigieuses.

Les internautes sont également mis à contribution. En matière de contenu sur Internet, il existe en Angleterre une *hotline.* L'*Internet Watch Foundation* a été créée en 1996, suite à un accord entre le gouvernement, la police et les fournisseurs d'accès à Internet. Le principe est que ce sont les internautes qui vont reporter à cet organisme l'existence de contenus racistes ou pédophiles. L'*Internet Watch Foundation* va alors avertir les fournisseurs d'accès, qui ne pourront pas prétendre ne pas être au courant, et devront ainsi faire disparaître ces contenus, en cas de refus, la police se chargera de leur demander, et le fournisseur d'accès ne pourra plus se placer sous la protection du *Defamation Act* de 1996[343].

L'encadrement de la liberté d'expression au Royaume-Uni tend à rejoindre les limites imposées par la loi en Europe continentale, même si la loi est souvent remplacée par la jurisprudence et l'analogie des cas jugés (*case law*). Liée à l'énoncé de principes sur le continent, la limitation de la liberté est pragmatique au Royaume-Uni[344]. Dans les cas litigieux, le juge, au cas par cas, va rechercher la résolution du problème[345]. Le régime britannique se trouve aux antipodes du système français, codifié, héritier du droit romain. Mais, la presse y est dynamique et demeure une des plus lues du monde[346].

Des limitations à la liberté d'expression existent dans les États membres l'Union européenne et la Cour européenne des droits de l'homme accepte ces limitations prévues par l'article 10 de la Convention des droits de l'homme si elles ne sont pas excessives.

---

[342] « *reasonnable care in relation to its publication* ».

[343] *Godfrey v Demon Internet Ltd*, QBD, [1999] 4 All ER 342, [2000] 3 WLR 1020; [2001] QB 201 (full decision provided).

[344] « *The life of the law has not been logic: it has been experience* » (Olivier Wendell Holmes, *The Common Law*, New York, Dover Publications, Lecture I : « Early Forms of Liability », p. 1).

[345] David Fennelly, « *Penser par cas* : A common law perspective », *Revue interdisciplinaire d'études juridiques*, 2014/2 (Volume 73), pp. 155-171. URL : https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2014-2-page-155.htm consulté le 2 mars 2018.

[346] En mars 2015, malgré une baisse moyenne sur un an de 7,6%, l'ensemble des quotidiens britanniques tirait à 7,6 millions d'exemplaires par jour (source *The Guardian*), à rapprocher d'une diffusion quotidienne française de 3,4 millions pour les quotidiens français en 2016 (source ACPM/OJD).

c) Une liberté encadrée sur Internet au niveau européen

Le 6 juillet 2006, le Parlement européen adopte une résolution concernant la liberté d'expression sur Internet[347]. Le Parlement considère que « *la lutte pour la liberté d'expression est aujourd'hui en grande partie menée en ligne, étant donné qu'Internet est devenu le moyen d'expression privilégié des dissidents politiques, des militants en faveur de la démocratie, des défenseurs des Droits de l'homme et des journalistes indépendants dans le monde entier,* » et donc, que *« limiter cet accès* [à Internet] *est incompatible avec le droit à la liberté d'expression* » et que les seules restrictions ne devraient exister que dans le « *cas de l'utilisation d'Internet pour des activités illégales telles que l'incitation à la haine, à la violence et au racisme, la propagande totalitaire ainsi que l'accès des enfants à la pornographie ou leur exploitation sexuelle,* » et en conséquence, le Parlement demande « *au Conseil et aux États membres de l'Union de se mettre d'accord sur une déclaration commune confirmant leur engagement vis-à-vis de la protection des droits des internautes et de la promotion de la liberté d'expression sur Internet dans le monde entier* ».

La Convention européenne des droits de l'homme définit et protège la liberté d'expression dans son article 10. Pour la Cour européenne des droits de l'homme, cet article 10 s'applique à la communication et au moyen d'Internet[348]. Des restrictions sont prévues à l'alinéa 2 de cet article 10, elles sont pour la Cour d'interprétation stricte, elles doivent être « nécessaires dans une société démocratique », c'est-à-dire correspondre à un « besoin social impérieux », et être proportionnés au but légitime poursuivi[349]. Ainsi un discours de haine ne bénéficie pas de la protection de l'article 10[350]. En vertu de l'article 17 de la Convention[351], un « *discours incompatible avec les valeurs proclamées et garanties par la Convention n'est pas protégé par*

[347] *Résolution de Parlement européen sur la liberté d'expression sur Internet*, P6_TA/2006/0324 du 6 juillet 2006, parue au Journal officiel de l'Union européenne du 13.12.2006.
[348] Cour européenne des droits de l'homme, Grande chambre, Affaire *Delfi c/ Estonie*, Requête nº 64569/09, Arrêt du 16 juin 2015.
[349] Lyn François, « Les droits nationaux de la liberté d'expression et le principe européen de proportionnalité », *LEGICOM,* 2014/1 (N° 52), pp. 101-107. URL : https://www.cairn.info/revue-legicom-2014-1-page-101.htm consulté le 3 avril 2018.
[350] Cour européenne des droits de l'homme, Affaire *Gündüz c/ Turquie*, Requête nº 35071/97, Arrêt du 4 décembre 2003.
[351] Convention européenne des droits de l'homme, article 17 : « *Aucune des dispositions de la présente Convention ne peut être interprétée comme impliquant pour un Etat, un groupement ou un individu, un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits et libertés reconnus dans la présente Convention ou à des limitations plus amples de ces droits et libertés que celles prévues à ladite Convention* ».

l'article 10 »[352]. Des exemples de pareil discours comprennent des propos niant l'Holocauste[353], justifiant une politique pronazie[354], associant tous les musulmans à des actes graves de terrorisme[355] ou qualifiant les juifs de « source du mal »[356]. Mais la Cour veille à la protection de la presse qui communique sur des questions légitimes d'intérêt public[357] ou d'intérêt général[358]. Pour la Cour, les informations confidentielles et celles d'ordre privé que tout individu espère ne pas voir publier sans son consentement, sont à préserver[359]. La protection de la vie privée et de la réputation d'une personne doit prendre le pas sur la liberté d'expression[360].

Si l'Union européenne, et plus généralement l'Europe[361], admet d'encadrer la liberté d'expression pour des raisons de protection de l'individu ou de l'intérêt général, cette restriction n'est pas admise dans les États-Unis d'Amérique.

[352] Conseil de l'Europe, *Internet : la jurisprudence de la Cour européenne des droits de l'homme,* mise à jour juin 2015, Op. cit. p.58.
[353] Cour européenne des droits de l'homme (Grande Chambre), Arrêt du 23 septembre 1998, *Affaire Lehideux et Isorni c/ France,* Requête n° 24662/94.
[354] Cour européenne des droits de l'homme, Décision du 24 juin 2003 sur la recevabilité de la requête n° 65831/01, *Affaire Garaudy c/ France.*
[355] Cour européenne des droits de l'homme (Deuxième Section), Décision du 16 novembre 2004 de recevabilité de la requête n° 23131/03, *Affaire Norwood c/ Royaume-Uni*.
[356] Cour européenne des droits de l'homme, Décision du 20 février 2007 sur la recevabilité de la requête n° 35222/04, *Affaire Pavel Ivanov c/ Russie*.
[357] Cour européenne des droits de l'homme (séance plénière), *Affaire Observer et Guardian c/ Royaume-Uni*, Requête no13585/88, Arrêt du 26 novembre 1991.
[358] Cour européenne des droits de l'homme, Affaire *Bladet Tromsø et Stensaas c/ Norvège*, Requête nº 21980/93, Arrêt du 20 mai 1999.
[359] Cour européenne des droits de l'homme, Division de la recherche, *Internet : la jurisprudence de la Cour européenne des droits de l'homme*, mise à jour juin 2015, disponible à http://www.echr.coe.int/documents/research_report_Internet_fra.pdf, consulté le 6 février 2017.
[360] Cour européenne des droits de l'homme, Affaire *Alexey Ovchinnikov c. Russie*, Requête nº 24061/04, Arrêt du 16 décembre 2010.
[361] Les 47 pays membres du Conseil de l'Europe.

3) Aux États-Unis d'Amérique, la conséquence du premier amendement

Aux États-Unis d'Amérique, la liberté d'expression n'est pas protégée par le texte original de la Constitution, mais par le premier amendement[362] qui fait partie des dix amendements[363] qui prennent effet dès 1791[364], et les interprétations successives de la Cour suprême. Le premier amendement est la justification d'une liberté d'expression quasi totale[365], sans contrainte Il interdit au Congrès des États-Unis d'adopter des lois limitant la liberté de religion et d'expression, la liberté de la presse ou le droit à s'« *assembler pacifiquement* ». La liberté ne peut être assurée que par la non intervention de l'État. La Cour suprême utilise le critère du « *danger clair et actuel* » pour limiter la liberté d'expression, ce critère reste le critère d'équilibre permettant d'opter entre les intérêts du gouvernement et la liberté d'expression[366]. Le principe retenu par les États-Unis est que l'échange libre d'idées encourage la compréhension, fait avancer la recherche de la vérité et permet de débusquer le mensonge[367]. Au milieu du XIX[e] siècle, John Stuart Mill défendait la notion d'une place de marché des idées : « *Primo, si une opinion est astreinte au silence, cette opinion autant que nous sachions peut certainement être vraie. Le nier est prétendre être infaillible. Secundo, bien que cette opinion réduite au silence soit erronée, elle peut contenir, et généralement elle contient, une part de vérité et comme l'opinion dominante sur tout sujet est rarement ou jamais complétement la vérité vraie, c'est seulement par la confrontation d'idées que le reste de la vérité a une chance d'être révélée* »[368].

---

[362] Constitution américaine du 17 septembre 1787 - Premier amendement de 1 791: "*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*", version disponible en ligne à http://www.usconstitution.net/const.html#Am1.
Traduction française proposée par la Documentation française : « *Le Congrès ne fera aucune loi accordant une préférence à une religion ou en interdisant le libre exercice, restreignant la liberté d'expression, la liberté de la presse ou le droit des citoyens de se réunir pacifiquement et d'adresser à l'État des pétitions pour obtenir réparation de torts subis* », disponible à http://www.ladocumentationfrancaise.fr/dossiers/election-presidentielle-americaine-2008/constitution-americaine.shtml#eztoc21806_2_8:.

[363] Connus sous le nom de « *Bill of Rights* » (Déclaration des droits).

[364] Adoptée par la Chambre des représentants le 21 août 1789 et le Congrès le 26 septembre 1789, la Déclaration des droits est progressivement approuvée par les États fédérés. Ces amendements prennent effet le 15 décembre 1791 après la ratification par la Virginie.

[365] Russell L. Weaver, *Understanding the first amendment*, LexisNexis, 5th edition, 2014, pp. 10-13.

[366] United States Supreme Court, *Schenck v. United States,* Nos. 437, 438, Decided March 3, 1919, 249 U.S. 47.

[367] Ambassade des États-Unis d'Amérique, « La liberté d'expression aux États-Unis », publié en 2003, http://photos.state.gov/libraries/amgov/133183/french/1304_Freedom_of_Expression_UnitedStates_French_Digital.pdf , consulté le 6 février 2017.

[368] Cité par Russel L. Weaver, *Understanding the first amendment*, LexisNexis, 5th edition, p. 10. "First, if any opinion is compelled to silence, that opinion for aught we can certainly know, be true. to deny this is to assume

Alors que la protection du premier amendement n'était effective qu'au niveau fédéral, la Cour suprême l'a étendue, en 1931, au niveau des États fédérés[369] et interdit aussi la plupart des formes de restriction de la liberté de la presse. Mais en 1971, La Cour suprême autorise *The New York Times* à publier des articles relatifs à la guerre au Vietnam[370] alors que le gouvernement soutenait que cette publication compromettrait la sécurité nationale. La décision de la Cour est basée sur le fait que le gouvernement n'a pas prouvé que la publication porterait une « *atteinte directe, immédiate et irréparable à l'intérêt national* », critère utilisé depuis 1919 avec l'arrêt Schenck[371].

Selon l'interprétation actuelle, le Premier amendement interdit au gouvernement, au Parlement et au juge de limiter la liberté de presse ou d'expression au niveau fédéral et, en pratique, au niveau des États et des villes[372]. Cette limitation stricte du rôle du législateur empêche la mise en place de protections sur Internet[373]. L'annulation de la *Communications Decency Act* de 1996 (DCA) aux États-Unis représente un échec pour ceux qui souhaitaient établir une régulation du contenu sur le réseau[374]. Une partie de cette loi voulait criminaliser des pratiques illicites liées à l'obscénité et la violence lorsque l'éditeur avait connaissance du fait que ce contenu était susceptible d'être vu par des mineurs. L'administration Clinton et le Congrès souhaitaient étendre la protection des mineurs à Internet en aménageant des espaces non accessibles aux mineurs[375]. Cependant, sur le réseau, il est impossible de vérifier l'âge de

---

our own infallibility. Secondly, though this silenced opinion be in error, it may and very commonly does, contain a portion of the truth, and since the generally prevailing opinion of any subject is rarely or never the whole truth, it is only by the collision of adverse opinion that the remainder of the truth had any chance being supplied".

[369] United States Supreme Court, *Near v. Minnesota,* No. 91, Decided June 1, 1931, 283 U.S. 697.

[370] United States Supreme Court, *New York Times Co. v. United States*, No. 1873, Decided: June 30, 1971, 403 U.S. 713,1.

[371] United States Supreme Court, *Schenck v. United States,* Nos. 437, 438, Decided March 3, 1919, 249 U.S. 47.

[372] United States Supreme Court, *Near v. Minnesota,* No. 91, Decided June 1, 1931, 283 U.S. 697.

[373] Viviane Serfaty, « Le refus d'interdire : éléments pour une analyse de la liberté d'expression sur Internet aux États-Unis », *Raisons politiques*, 2012/3 (n° 47), pp. 189-202. URL : https://www.cairn.info/revue-raisons-politiques-2012-3-page-189.htm consulté le 11 décembre 2017.

[374] Nicolas Curien, « IV Neutralité et droits du citoyen », dans *La neutralité d'Internet*. Paris, La Découverte, « Repères », 2011, pp. 65-82. URL : https://www.cairn.info/la-neutralite-d-internet--9782707167156-page-65.htm conté le 11 décembre 2017.

[375] Onze ans plus tard, ce problème de l'accès à la pornographie par les adolescents reste d'actualité. Le Président Macron a écrit sur Twitter le 25 novembre 2017 : « *La pornographie a franchi la porte des établissements scolaires. Nous ne pouvons ignorer ce genre, qui a fait de la femme un objet d'humiliation* ». Le même jour, dans un discours prononcé à l'Élysée, il a précisé : « *nous ne régulons pas aujourd'hui l'accès aux jeux vidéo, aux contenus sur Internet, aux contenus pornographiques de plus en plus diffusés. […] Nous devrons donc repenser le cadre de notre régulation, en particulier des contenus audiovisuels, en prenant en compte l'évolution du numérique afin d'étendre les pouvoirs et la régulation du CSA* » (discours disponible à l'URL : http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-a-l-occasion-de-la-journee-internationale-pour-l-elimination-de-la-violence-a-l-egard-des-femmes-et-du-lancement-de-la-grande-cause-du-quinquennat/ consulté le 11 décembre 2017.

l'internaute. Ainsi, tout site qui pourrait être considéré comme dommageable pour un mineur devrait être complètement interdit. Ceci restreindrait la liberté d'expression des adultes.

Le 8 février 1996, le jour où la loi a été signée par le Président Clinton, l'*American Civil Liberties Union* (ACLU) et dix-neuf autres groupes ont porté plainte devant la Cour Suprême, pour violation du premier amendement de la Constitution américaine. La Cour Suprême a rendu sa décision le 26 juin 1997[376], et elle a censuré cette loi. La Cour a souligné la puissance d'Internet comme moyen de communication en comparant Internet à une tribune où tout individu peut s'exprimer librement, tenant ainsi un raisonnement proche de celui du Conseil constitutionnel français[377] ou de la Cour européenne des droits de l'homme[378]. Elle a considéré que l'intervention gouvernementale sur le réseau ne pouvait que nuire à la liberté d'expression, et en particulier celle des adultes. La Cour a identifié dans la loi contestée deux effets paralysants[379]. Premièrement, en limitant les contenus explicitement sexuels ou indécents, la loi pourrait viser par ricochet, outre la pornographie, les informations sur la contraception ou les maladies sexuellement transmissibles. Deuxièmement, les éditeurs ne souhaitant pas prendre de risques seraient amenés à cesser la mise à disposition de contenus pornographiques destinés aux adultes[380]. La Cour invite plutôt les autorités publiques à trouver d'autres modalités pour protéger les mineurs, par exemple l'information parentale et le filtrage.

Il semble également qu'aux États-Unis d'Amérique, une loi interdisant des propos d'incitation à la haine raciale ou religieuse serait contraire au Premier Amendement[381]. En effet, en 1992, la Cour Suprême[382] a invalidé un arrêté municipal interdisant le placement d'objets, de symboles ou de graffiti susceptibles de provoquer l'indignation ou la colère d'autrui en raison de leur race ou de leur religion.

---

[376] United States Supreme Court, *Reno c/ACLU,* n° 96-511, decided June 26,1997*,* 521 U.S. 844.

[377] Conseil constitutionnel, décision n° 2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur Internet*.

[378] Cour européenne des droits de l'homme, Affaire *Ahmet Yildirim c/ Turquie*, requête n° 3111/10, arrêt du 18 mars 2013.
Cour européenne des droits de l'homme, Affaire *Cengiz et autres c. Turquie*, requêtes n^{os} 48226/10 et 14027/11, arrêt du 1 décembre 2015.
Cour européenne des droits de l'homme, Affaire *Jankovskis c. Lituanie*, requête no 21575/08, arrêt du 17 janvier 2017.

[379] En anglais « *chilling effects* ».

[380] Winston J. Maxwell, « La jurisprudence américaine en matière de liberté d'expression sur Internet », *Étude 2014 du Conseil d'État, « Le numérique et les droits fondamentaux »,* septembre 2014, pp. 393-406.

[381] Ibid.

[382] United States Supreme Court, *R.A.V. v. City of St. Paul,* N° 90-7675, decided June 22, 1992*,* 505 U.S. 377 (1992).

Cette non-intervention du législateur sur Internet semble être remise en cause pour des raisons commerciales. En effet, la neutralité du réseau Internet votée en 2015[383] sous la présidence de Barack Obama semble être remise en cause. La *Federal Communications Commission* ou FCC remet en cause le principe d'égalité de traitement des flux de données par les opérateurs de télécommunications, en ne leur imposant qu'une simple règle : être « *transparents sur leurs pratiques, pour que les consommateurs puissent souscrire à l'offre qui leur convient le mieux* ». Ainsi, un opérateur de télécommunications pourra favoriser le débit du réseau pour certaines offres et le réduire pour d'autres, sur la base contractuelle de l'abonnement à ses services[384]. L'administration américaine privilégie la dérégulation au profit d'une auto-régulation ouvrant la voie à une restriction d'accès à certains services. L'UCLA ou d'autres associations en référeront-elles à la Cour suprême au titre du premier amendement ?

La liberté de pensée et d'expression est aussi l'objet de textes au niveau du continent américain. La Convention américaine relative aux droits de l'homme[385] protège avec ses articles 12 et 13 la liberté de conscience et de religion et la liberté de pensée et d'expression. Le 1er alinéa de l'article 13 est très ouvert : « *Toute personne a droit à la liberté de pensée et d'expression ; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, que ce soit oralement ou par écrit, sous une forme imprimée ou artistique, ou par tout autre moyen de son choix* ». Le second alinéa exclut toute censure préalable, mais précise que cette liberté comporte des responsabilités fixées par la loi. Cette convention institue une Commission interaméricaine des droits de l'homme qui reçoit et instruit les plaintes ou pétitions, et une Cour interaméricaine des droits de l'homme qui ne peut être saisie que par la Commission ou un des États.

Tous ces textes sont applicables et d'actualité dans la société numérique et la démultiplication des moyens d'expression. Mais si aux États-Unis d'Amérique, le premier amendement est ainsi la justification d'une liberté quasi totale, la liberté d'expression connaît en Europe des

[383] Le 26 février 2015, la FCC a considéré par 3 voix contre deux que l'Internet devait être considéré comme un « bien public » (Martin Untersinger, « Le régulateur des télécommunications a annoncé après des années de débats de nouvelles règles concernant le traitement des données sur le Web », 26 février 2015, *Le Monde.fr,* URL : http://www.lemonde.fr/pixels/article/2015/02/26/etape-decisive-pour-la-neutralite-du-net-aux-etats-unis_4583490_4408996.html consulté le 11 décembre 2017).

[384] Relaté par la presse : Amaelle Guiton, « Les États-Unis vers l'Internet à deux vitesses », 22 novembre 2017, *Libération,* URL : http://www.liberation.fr/planete/2017/11/22/les-etats-unis-vers-l-internet-a-deux-vitesses_1611829; Valentin Graff, « Neutralité du Net : l'égalité numérique mise à mal aux Etats Unis par l'administration Trump », 30 novembre 2017, *France 24,* URL : http://www.france24.com/fr/20171130-etats-unis-neutralite-net-egalite-numerique-trump-mozilla-internet-fcc, consultés le 11 décembre 2017.

[385] *Convention américaine relative aux droits de l'homme*, adoptée à San José, Costa Rica, le 22 novembre 1969, à la conférence spécialisée interaméricaine sur les droits de l'homme.

atténuations légales[386] acceptées par la Cour européenne des droits de l'homme si elles ne sont pas excessives et nécessaires à l'ordre public[387]. Aucune législation commune européenne ou internationale n'existe pour limiter de façon harmonieuse la liberté d'expression[388] et défendre d'autres droits attaqués par certaines pratiques liées à la liberté d'expression. Certains États encadrent cette liberté par la loi ou la jurisprudence[389], d'autres comme les États-Unis d'Amérique protègent de façon stricte cette liberté au détriment d'autres droits. Mais si le Premier Amendement protège le citoyen contre des mesures prises par l'État ou ses représentants, il ne semble pas protéger le citoyen des contrats privés qui limiteraient cette liberté d'expression par la mise en place d'une véritable censure.

B) Les atteintes à la liberté d'expression par le retour d'une censure sur Internet

La censure étatique a longtemps été un frein à l'expression libre de la presse écrite et de la radiodiffusion[390]. Internet peut aussi, à l'inverse, permettre à des ouvrages interdits par la justice d'être accessibles aux internautes. *Le grand secret* du docteur Gübler[391], médecin de François Mitterrand, dont le livre a été retiré de la vente pour violation du secret médical par décision de justice, était disponible quelques jours plus tard sur Internet pour un téléchargement en toute illégalité[392]. Cette affaire montre la difficulté de mettre en place une véritable censure sur le réseau Internet.

---

[386] Irène Bouhadana, William Gilles, Jean Harivel, "Freedom of expression and the values of the French Republic. Article dedicated to the memory of the victims of the terrorist attacks of 2015 in France", in Russell L. Weaver and Steven I. Friedland (Edited by), *Comparative Perspectives on Freedom of Expression, Global Papers Series, Vol. II,* Carolina Academic Press, 2017, pp. 141-158.

[387] Cour européenne des droits de l'homme, Requête n° 25239/13, *Dieudonné M'Bala M'Bala c/ France*, 20 octobre 2015.

[388] Des restrictions légales sont prévues par la Convention européenne des droits de l'homme pour protéger la santé ou la morale, la réputation ou les droits d'autrui, la sécurité nationale, l'intégrité territoriale, la sûreté publique, la défense de l'ordre, pour prévenir le crime, empêcher la divulgation d'informations confidentielles ou garantir l'autorité et l'impartialité du pouvoir judiciaire (Article 10, §2). Chaque État peut apporter les restrictions qu'il juge nécessaire, mais ces restrictions doivent être prévues par la loi. La Cour européenne des droits de l'homme vérifie l'adéquation et la proportionnalité des restrictions au but général recherché (Cf. « La liberté d'expression en Europe », *dossiers sur les droits de l'homme* nº 18, Éditions du Conseil de l'Europe, mise à jour du 31 décembre 2015).

[389] Cf. 2) En Europe, un encadrement généralisé.

[390] Jean-Yves Mollier, « La censure et l'histoire », *Ethnologie française*, 2006/1 (Vol. 36), pp. 125-128. URL : https://www.cairn.info/revue-ethnologie-francaise-2006-1-page-125.htm consulté le 11 décembre 2017.

[391] Claude Gübler, Michel Gonod, *Le Grand secret*, Plon, 1996.

[392] Relaté par Meryem Marzouki, « Nouvelles modalités de la censure : le cas d'Internet en France », *Le Temps des médias*, 2003/1 (n° 1), pp. 148-161. URL : https://www.cairn.info/revue-le-temps-des-medias-2003-1-page-148.htm consulté le 11 décembre 2017.

Elle existe cependant dans certains États autocratiques[393]. Avec la lutte contre le terrorisme ou la pédopornographie, une censure administrative a été rétablie sur Internet, dans des États démocratiques. Une censure « privée » s'est imposée sur Internet, sous couvert d'application de règles d'éthique ou de réglementation interne[394].

1) La censure gouvernementale

Dans plusieurs pays, Internet reste confronté à une censure gouvernementale qui limite la liberté d'expression. Cette censure peut aussi être utilisée comme arme économique.

a) La censure d'État des régimes autoritaires

En République populaire de Chine, il existe un ministère de la propagande qui gère les médias. La censure d'Internet y est organisée et régie par plusieurs lois et réglementations. Ces réglementations sont mises en œuvre par les fournisseurs d'accès à Internet qui sont par ailleurs contrôlées par les gouvernements provinciaux. En 1998, le gouvernement chinois lance le projet « Bouclier doré ». Les autorités chinoises non seulement bloquent le contenu de certains sites, mais elles surveillent l'accès à Internet par les individus[395].

Techniquement, le système de blocage des adresses IP est composé de firewalls et de serveurs proxy standards positionnés sur les passerelles Internet. Il permet un blocage des adresses avant qu'elles ne soient routées. L'accès à certaines adresses IP peut être interdit ou les serveurs de nom de domaines (DNS) renvoient des adresses erronées rendant le site inaccessible[396].

Depuis 2006, un véritable schisme du réseau Internet a été réalisé par la Chine : les DNS qui traduisent les noms de domaine en idéogrammes en adresse IP ne passent plus par l'ICANN. Le contrôle de la navigation sur Internet est directement contrôlé par le gouvernement chinois.

---

[393] Chine, Turquie, Inde entre autres (Cf. ci-dessous a) La censure d'État des régimes autoritaires).

[394] *« Lorsque nous pensons qu'un contenu représente un réel risque de préjudice physique ou une atteinte directe à la sécurité publique, nous supprimons ledit contenu, désactivons les comptes concernés et collaborons avec les autorités. »* (Extrait des « *Standards de la communauté* », Facebook, disponible à l'URL https://www.facebook.com/communitystandards, consulté le 12 mars 2018).

[395] Lire l'article de Frédéric Douzet, « Les frontières chinoises de l'Internet » in *125 – Chine, nouveaux enjeux géopolitiques,* second trimestre 2007, Hérodote revue de géographie et de géopolitique, URL : http://www.herodote.org/spip.php?article282, consulté le 15 décembre 2017.

[396] "How Censorship Works in China: A Brief Overview", *Human Rights Watch*, URL : https://www.hrw.org/reports/2006/china0806/3.htm consulté le 11 décembre 2017.

La technique du VPN permet de contourner certains blocages. Apple a cédé au gouvernement chinois et a confirmé le 30 juillet 2017 avoir retiré de son App Store en Chine les logiciels permettant de gérer des VPN[397].

Cette surveillance des réseaux associée aux restrictions d'accès aux sites occidentaux a des répercussions économiques. Les entreprises chinoises Baidu, Tencent et Alibaba[398] profitent du blocage des concurrents internationaux, principalement américains, et sont devenues des géants de l'Internet. Des moteurs de recherche et des réseaux sociaux chinois ont été développés. Outre le non référencement de sites par les moteurs de recherche, il est possible de surveiller les échanges effectués sur ces réseaux sociaux pourtant aussi utilisés pour diffuser des messages de propagande et dénoncer la corruption. Mais certains sujets restent interdits, comme relater les événements survenus sur la place Tienanmen[399].

La censure sur Internet peut se manifester par des décisions autres que le blocage des sites. Ainsi, en Russie, le Parlement russe a voté plusieurs lois en juillet 2017 pour supprimer l'anonymat de l'internaute et renforcer la censure[400]. Depuis 2012 et le retour au pouvoir de Vladimir Poutine, ces lois permettent de bloquer tout site ayant un contenu « non-autorisé pour la Russie ». L'usage de VPN qui permettent de passer outre à un blocage d'un site, est interdit. Elle oblige les messageries, *WhatsApp* ou *Telegram* par exemple, à établir l'identité des utilisateurs au moyen de leur numéro de téléphone. Les moteurs de recherche doivent déréférencer les sites faisant l'objet d'un blocage[401].

D'autres pays, bien que démocratiques, ont aussi institué une forme de censure. L'Inde surveille l'accès aux sites Internet étrangers. Un site peut être censuré par le Gouvernement indien[402], le

---

[397] Thierry Noisette, « La Chine durcit encore sa censure d'Internet, imitée par la Russie », 1 août 2017, *L'Obs avec Rue 89,* URL : https://tempsreel.nouvelobs.com/rue89/rue89-nos-vies-connectees/20170801.OBS2836/la-chine-durcit-encore-sa-censure-d-internet-imitee-par-la-russie.html consulté le 13 décembre 2017.

[398] Le chiffre d'affaires annuel d'Alibaba Group a progressé en un an de 61 % pour s'établir au 30 septembre 2017 à 8,285 Mds US$ (source Alibaba Group Quarter 2017 Results, URL : http://www.alibabagroup.com/en/news/press_pdf/p171102.pdf consultée le 13 décembre 2017).

[399] Josh Chin, "Tiananmen Effect : "Big Yellow Duck" a Banned Term", *The Wall Street Journal*, 4 juin 2013, URL: https://blogs.wsj.com/chinarealtime/2013/06/04/tiananmen-effect-big-yellow-duck-a-banned-term/ consulté le 11 décembre 2017.

[400] AFP, Miladen Antonov, « Russie: de nouvelles mesures pour mieux contrôler l'accès à Internet », 7 août 2017, *Les voix du Monde RFI,* URL : http://www.rfi.fr/europe/20170807-russie-internet-acces-controle-lois-vpn-messageries-anonymat-manifestation-russie-no consulté le 13 décembre 2017.

[401] Julie Perrin, « La Russie adopte une loi sur la censure sur Internet visant les blogueurs de l'opposition et des journalistes », *Le VPN,* 26 décembre 2016, URL : https://www.le-vpn.com/fr/loi-russie/ consulté le 13 décembre 2017.

[402] Information Technology Act (ITA), enacted on 9 June 2000 by the Indian Parliament (Act n° 21 of 2000, notified on 17 October 2000), amended in November 2008 to reinforce the government's power to block internet sites.

blocage est réalisé au niveau des serveurs DNS et tous les FAI indiens l'appliquent. Un internaute qui ne respecte pas la législation, encourt une amende de 4 500 US $ et une peine d'emprisonnement de 3 ans[403].

Le blocage des sites peut aussi être utilisé par des États démocratiques pour des raisons de sécurité et de lutte contre la pédopornographie et le terrorisme.

b) La censure justifiée par la sécurité et l'ordre public

En Europe, la liberté d'expression sur Internet est protégée et fait l'objet de nombreuses décisions de la Cour européenne des droits de l'homme[404], mais il y existe aussi un contrôle discret. En 2013, la Suède était jugée comme un pays de liberté d'expression totale sut Internet[405]. En 2016, des articles de presse faisaient état de censure concernant les délits commis par les immigrés[406].

En France, la loi LOPPSI 2[407] avait prévu le blocage des sites Internet pour pédopornographie. Dans les faits, cette interdiction administrative n'a été utilisée qu'après le vote de la loi sur le terrorisme de 2014[408] et ses décrets d'application[409] et a été définie pour les sites pédopornographiques et pour les sites incitant au terrorisme.

Toute tentative d'accès à de tels sites se traduit par le message suivant :

---

[403] VPN Actu, « Internet en Inde : les censures s'intensifient », *VPN Actu*, 1 septembre 2016, URL : http://vpnactu.fr/inde-les-censures-en-ligne-sintensifient/ consulté le 13 décembre 2017.

[404] Division de la recherche, « III. Internet et liberté d'expression », *Internet : La jurisprudence de la Cour européenne des droits de l'homme,* juin 2015, Conseil de l'Europe, pp. 17-36.

[405] Boris Manenti, « La Suède, pays de l'Internet libre », 9 mars 2013, *O,* URL : https://o.nouvelobs.com/high-tech/20130307.OBS1214/la-suede-pays-de-l-internet-libre.html consulté le 14 décembre 2017.

[406] Pierre-Alain Depauw, « Immigration – La censure d'Internet s'intensifie en Suède », 2 février 2016, *Immigration / Société Medias-presse.info,* URL : http://www.medias-presse.info/immigration-la-censure-dinternet-sintensifie-en-suede/48422/ consulté le 14 décembre 2017.

[407] Loi no 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure.*

[408] Loi n° 2014-1353 du 13 novembre 2014 *renforçant les dispositions relatives à la lutte contre le terrorisme.*

[409] Décret n° 2015-125 du 5 février 2015 *relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* publié au JORF n°0031 du 6 février 2015 page 1811.
Décret n° 2015-253 du 4 mars 2015 *relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique*, publié au JORF n°0054 du 5 mars 2015 page 4168.

Une personnalité qualifiée au sein de la Commission nationale de l'informatique et des libertés est chargée de contrôler la régularité des demandes de retrait, de blocage et de déréférencement des moteurs de recherche émises par les forces de police. Dans un rapport d'avril 2016[410], elle fait état de 1 439 demandes de retrait de contenus (1 286 pour terrorisme et 153 pour pédopornographie) dont 1 179 ont été effectives de mars 2015 à février 2016, et de 244 demandes de blocage pour pédopornographie et 68 pour terrorisme.

Les textes appliqués relèvent plus du droit administratif que du droit pénal[411]. La lutte contre le terrorisme et la lutte contre la pédopornographie sont traitées sur le même plan. La procédure se déroule en deux temps : l'autorité administrative[412] demande aux éditeurs d'un service de communication en ligne ou aux hébergeurs de retirer les contenus incriminés et en informe les fournisseurs d'accès, en cas d'absence de retrait des contenus dans les vingt-quatre heures, l'autorité administrative notifie aux fournisseurs d'accès la liste des adresses des services de communication pour en empêcher l'accès. Un contrôle est prévu, l'autorité administrative transmet à une personnalité qualifiée au sein de la CNIL[413] les demandes de retrait et les adresses contrevenantes.

[410] Alexandre Linden, *Rapport d'activité 2015 de la personnalité qualifiée prévue par l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 créé par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme,* mars 2015-février 2016, Commission de l'informatique et des libertés, disponible à l'URL : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_blocage_sites_internet_2016_0.pdf .

[411] Jean-Yves Monfort, « Le blocage administratif des sites prévu dans la loi du 13 novembre 2014 de lutte contre le terrorisme », *LEGICOM*, 2016/2 (N° 57), pp. 69-74. URL : https://www.cairn.info/revue-legicom-2016-2-page-69.htm consulté le 11 décembre 2017.

[412] Dans la loi n° 2014-1353 du 13 novembre 2014 (article 14), cette « autorité administrative » n'est pas qualifiée. Cette dénomination est utilisée en opposition à « autorité judiciaire » et permet de désigner tout ministre ou personne déléguée par un ministre.

[413] La personnalité qualifiée ne peut pas être un des parlementaires siégeant dans la commission (Article 6-1, loi n° 2004-575 du 21 juin 2004).

Comme l'écrit Jean-Yves Montfort[414], les parlementaires ont souhaité éviter de mettre en avant une mesure de blocage qui ressemblait par trop à une censure, en demandant d'abord un retrait du contenu litigieux. De plus, le Conseil constitutionnel n'a pas été appelé à se prononcer sur la constitutionnalité de la loi de novembre 2014, même si le dispositif de blocage similaire prévu par la loi LOPPSI 2 avait été accepté par le Conseil en 2011. Les décrets d'application ont quant-à-eux été entérinés indirectement par le Conseil d'État qui a rejeté deux recours exercés contre la procédure de blocage hors de toute décision d'un juge[415].

Avec la lutte contre le terrorisme et la pédopornographie, une forme de censure est administrativement rétablie sur Internet sans intervention à priori du juge judiciaire. Avant cette renaissance d'Anastasie, les réseaux sociaux ont établi au travers de règles d'éthique[416] la possibilité de retirer eux-mêmes certains contenus, voire fermer certains comptes.

2) La censure privée de certains réseaux sociaux

En février 2011, Twitter a fermé trois comptes d'utilisateurs, sous prétexte du non-respect de l'étiquette, à la demande de l'équipe de campagne d'un des candidats à l'élection présidentielle. « *Nous nous réservons le droit de suspendre les comptes qui ne respectent pas nos conditions d'utilisation* », justifie une porte-parole de Twitter dans un article[417]. L'équipe Internet du candidat Nicolas Sarkozy a reconnu avoir réclamé la fermeture des comptes qui « *pouvaient prêter à confusion* », ainsi le droit à la caricature qui est admis par la loi sur la presse, et confirmé par la jurisprudence, se trouve ainsi dénoncé par une équipe partisane.

Facebook a aussi censuré certains comptes. La reproduction du tableau de Courbet, « l'origine du monde »[418], est interdite de séjour sur Facebook pour des raisons internes de morale[419], le tableau étant considéré comme pornographique. D'autres cas de censure par Facebook existent.

---

[414] Dans l'article précité.

[415] Conseil d'État, requêtes n[os] 389140 et 389896, *Association french data network et autres*, arrêt du 1[er] février 2016.

[416] *« Lorsque nous pensons qu'un contenu représente un réel risque de préjudice physique ou une atteinte directe à la sécurité publique, nous supprimons ledit contenu, désactivons les comptes concernés et collaborons avec les autorités. »* (Extrait des « *Standards de la communauté* », Facebook,) Op. cit.

[417] Bois Monenti, « Nicolas Sarkozy, Twitter et la censure », 21 février 2012, *L'Obs,* URL : http://tempsreel.nouvelobs.com/high-tech/20120221.OBS1927/nicolas-sarkozy-twitter-et-la-censure.html, consulté le 5 mai 2012.

[418] Tableau présenté au Musée d'Orsay à Paris.

[419] Judith Duportail « Comprendre la censure sur Facebook », *L'Express,* 9 avril 2011, URL : http://www.lexpress.fr/actualite/high-tech/comprendre-la-censure-sur-facebook_980973.html, consulté le 5 mai 2012.

En Suède, une campagne concernant le cancer du sein qui décrivait la méthode d'autopalpation des seins a été censurée, et devant la polémique, Facebook a dû présenter des excuses[420].
Cette censure privée, liée à un certain puritanisme peut d'autant plus surprendre que certains sites, qui seraient légalement sanctionnés en France ou en Europe pour haine raciale ou apologie du crime, peuvent continuer leur diffusion à partir du territoire des États-Unis d'Amérique en bénéficiant de la protection du premier amendement[421]. Aux États-Unis d'Amérique, il n'existe pas de texte réprimant l'incitation à la haine raciale ou la diffamation. Tout le monde peut dire absolument ce qu'il veut, ceci afin de ne pas restreindre la liberté d'expression. Les États-Unis sont très attachés à cette liberté d'expression, inscrite dès le premier amendement de leur constitution. Ainsi, des sites dont le contenu négationniste, incitant à la haine raciale, pédopornographique ou appelant au terrorisme, serait contraire à la loi, en France ou dans plusieurs États membres de l'Union européenne, restent en ligne et sont protégés par le premier amendement. Mais, des publications artistiques ou médicales, non illicites, peuvent être interdites de diffusion pour des raisons morales sur les réseaux sociaux gérés par des sociétés respectant la législation nord-américaine, montrant ainsi la difficile harmonisation du droit au niveau mondial.

C) La difficile harmonisation internationale des réglementations en matière de liberté d'expression dans un monde numérique

Si l'Union européenne, avec la transposition des directives, permet d'atténuer les écarts entre les normes internes des États membres, la mondialisation du réseau accentue la difficulté d'application de normes de droit non homogènes entre États membres et États non membres. Les grands acteurs de l'Internet sont américains et se placent sous la protection des lois nord-américaines, plus permissives que les lois des pays de l'Union européenne en matière de protection de la liberté d'expression. Une condamnation prononcée par un tribunal d'un État membre connaît quelques difficultés pour être effective[422]. À l'inverse, les lois et règlements nord-américains s'imposent à l'ensemble des entreprises quelle que soit leur nationalité[423].

[420] Melinda Davan-Soula, « Facebook a encore dû présenter ses excuses après avoir censuré une vidéo diffusée dans le cadre de la campagne de prévention du cancer du sein », *LCI,* 21 octobre 2016, at http://www.lci.fr/high-tech/couvrez-ce-sein-que-je-ne-saurais-voir-facebook-le-censure-2008822.html, consulté le 16 février 2017.
[421] Voir l'affaire YAHOO! ci-après.
[422] Voir ci-après l'affaire Yahoo!
[423] Voir ci-après les condamnations de banques ou l'affaire World Sport Exchange.

1) Une portée extraterritoriale de la législation des Etats-Unis d'Amérique

Face aux litiges portés devant les juridictions nord-américaines, les décisions diffèrent selon que le défendeur soit ou non d'origine nord-américaine. Alors que les lois des Etats-Unis d'Amérique peuvent devoir être appliquées par des sociétés européennes ou autres hors du territoire des Etats-Unis[424], les juges protègent les sociétés nord-américaines qui contreviendraient à une législation européenne sur le territoire de l'Union européenne.

En 2000, le tribunal de Grande Instance de Paris a condamné Yahoo pour avoir donné accès à une vente aux enchères d'objets nazis, sur son site via Yahoo US. Le juge français a rejeté l'argumentation de Yahoo, selon laquelle instituer un blocage en fonction de l'origine géographique était impossible. L'ordonnance[425] rendue par le tribunal imposait à l'entreprise américaine de : « *prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de ventes aux enchères d'objets nazis et de tout autre site ou service qui constituent une apologie du nazisme ou une contestation des crimes nazis* ». Suite à cette décision soulevant la question de l'applicabilité de l'injonction d'un juge français sur le territoire des États-Unis, la Cour du District de San José (Californie), saisie par Yahoo! Inc., dans un jugement du 7 novembre 2001, considéra que « *bien que la France ait le droit souverain de contrôler le type d'expression autorisée sur son territoire, cette cour ne pourrait appliquer une ordonnance étrangère qui viole la Constitution des États-Unis en empêchant la pratique d'une expression protégée à l'intérieur de nos frontières* »[426]. Ce jugement fut cependant annulé par la cour d'appel du 9e District, dans un arrêt du 23 août 2004, pour des raisons de procédure.

La Cour d'appel fédérale de San Francisco a rendu le 12 janvier 2006 une décision au fond s'agissant de l'application de la décision française sur le territoire américain[427]. Son raisonnement suit plusieurs points. Tout d'abord, elle a relevé que : Yahoo! Inc. n'avait pas

---

[424] Par exemple, les règles d'embargo édictées par les Etats-Unis d'Amérique doivent être respectées dès que le dollar est utilisé comme monnaie de transaction.

[425] Tribunal de Grande Instance de Paris, Ordonnance de référé du 22 mai 2000, *UEJF et Licra c/Yahoo! Inc. et Yahoo France.*

[426] Judge Jeremy Fogel *"Although France has the sovereign right to regulate what speech is permissible in France, this court may not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders*," Federal District Court for the Northern District of California, in San Jose.

[427] *"*Court throws out Yahoo case over French WEB restrictions*",* Juanary 18, 2006, URL: https://www.rcfp.org/browse-media-law-resources/news/court-throws-out-yahoo-case-over-french-web-restrictions, consulté le 16 février 2017.

choisi d'effectuer un recours devant les juridictions françaises, mais directement devant les juridictions américaines. Puis, elle a rappelé que Yahoo! Inc. avait respecté les mesures ordonnées par le tribunal français en restreignant l'accès du site aux Français uniquement et que, dès lors, il n'y avait pas lieu de se prononcer sur l'entrave au premier amendement. En outre, elle a considéré que les restrictions ne s'appliquant qu'au public français et n'ayant aucune incidence sur le public américain, l'atteinte substantielle au premier amendement ne pouvait être invoquée : « *Comme indiqué précédemment, l'extension - en fait l'existence - d'un tel droit extraterritorial en vertu du premier amendement est incertaine* »[428].

La Cour a relevé le fait que l'accès à de tels contenus était interdit en France et qu'il ne fallait en aucun cas faciliter la violation par les Français de la législation française. Concernant l'argument, mis en avant par Yahoo! Inc., selon lequel la décision française, restreignant l'accès du site, était susceptible d'avoir des répercussions, de manière indirecte, sur le public américain, elle a estimé que les conséquences, en matière d'accès, sur les utilisateurs américains n'étaient pas démontrées en l'espèce. Elle a ajouté que même si cela avait été démontré, l'application du premier amendement ne pouvait être étendue à la France.

Ensuite, elle a envisagé la possibilité pour les juridictions françaises de condamner Yahoo! Inc. à de nouvelles restrictions. Pour la Cour, une interdiction générale d'accès au site, ayant des conséquences sur les utilisateurs américains, aurait constitué une atteinte à la liberté d'expression sur le sol américain.

Enfin, la cour d'appel américaine a émis de vives interrogations s'agissant de restrictions excessives pouvant être prononcées par les juridictions étrangères et susceptibles de porter atteinte aux droits des citoyens américains : « *Ce niveau de préjudice n'est pas suffisant pour éliminer l'incertitude factuelle portant sur la question juridique présentée et ainsi rendre cette poursuite acceptable* »[429]. Elle a cependant admis les difficultés liées à l'utilisation internationale de l'Internet. En effet, elle a considéré que les problèmes liés à la liberté d'expression sur l'utilisation internationale d'Internet sont « *nouveaux, importants et difficiles* » : *« Nous devons agir avec précaution, avec conscience des limites de notre compétence judiciaire dans ce domaine peu développé de la Loi. Précisément de la nouveauté, de l'importance et de la difficulté des implications du premier amendement dont YAHOO!*

[428] "*As we indicated above, the extent – indeed the very existence – of such an extraterritorial right under the First Amendment is uncertain*".

[429] "*This level of harm is not sufficient to overcome the factual uncertainty bearing on the legal question presented and thereby to render this suit ripe".*

cherche à débattre, nous devons observer scrupuleusement les limites prudentielles dans l'exercice de notre pouvoir »[430].

Les associations françaises ont formé un recours devant la Cour suprême afin d'obtenir confirmation de la décision rendue par la Cour d'appel fédérale de San Francisco. La Cour suprême, disposant d'un pouvoir discrétionnaire, a refusé le 30 mai 2006 l'examen de ce recours. Yahoo! Inc. peut donc saisir d'autres juridictions pour tenter d'obtenir des décisions en sens contraire de l'arrêt rendu par la Cour d'appel de San Francisco. Cette décision n'est pas définitive en droit américain, pays de Common Law. D'autres sociétés peuvent se prévaloir de cette affaire pour rester hors de portée des législations européennes et des décisions de justice les condamnant.

Cette affaire Yahoo! montre la difficulté de faire appliquer une décision d'un tribunal français sur un territoire étranger, la procédure d'exequatur se heurtant alors aux droits locaux. Si la Cour d'appel fédérale de San Francisco a reconnu au gouvernement français la possibilité d'agir pour faire respecter sa législation sur son territoire, ce jugement n'est pas définitif, car non confirmé par une Cour suprême. Comme le constate Jean-Jacques Lavenue[431], la situation inverse, une violation des lois américaines par un serveur situé hors du territoire des États-Unis a connu une réponse complètement inverse[432]. Ainsi, alors que les tribunaux américains poursuivent des entreprises non américaines pour non-respect de la législation américaine[433], les entreprises américaines condamnées par un tribunal non américain quand elles violent une loi non américaine, voient l'effectivité de la condamnation remise en cause si elles respectent une législation américaine moins contraignante. Si pour les États-Unis d'Amérique, la législation américaine a une portée extraterritoriale, les législations d'autres États ne peuvent que difficilement s'imposer aux entreprises américaines[434].

---

[430] "*We should proceed carefully, with awareness of the limitations of our judicial competence, in this undeveloped area of the law. Precisely of the novelty, importance and difficulty of the First Amendment issues Yahoo! seeks to litigate, we should scrupulously observe the prudential limitations on the exercise of our power*".

[431] Jean-Jacques Lavenue, « Internationalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberespace confronté à la notion d'ordre public », *Lex Electronica*, vol. 11 n°2 (Automne / Fall 2006). Disponible en ligne à l'URL : http://www.lex-electronica.org/articles/v11-2/lavenue.pdf consulté le 14 décembre 2017.

[432] Affaire *World Sport Exchange*, citée par Jean-Jacques Lavenue dans l'article précité.

[433] Juin 2014, BNP Paribas s'est vu infliger une amende de 8,9 milliards de dollars pour avoir utilisé le dollar dans des transactions avec des « ennemis des États-Unis » sous embargo américain.
Décembre 2014, Alstom est condamné à payer une amende de 772 millions de dollars pour violation des lois américaines sur la corruption pour avoir payé des pots de vin en Chine, Inde et Indonésie.

[434] Jean-Jacques Lavenue, « Internet : efficacité des poursuites et ordre public international » in Irène Bouhadana, William Gilles (sous la direction.), *Cybercriminalité cybermenaces et cyberfraudes*, pp. 84-91, Les éditions Imodev, mars 2012.

Un site américain peut continuer à favoriser l'apologie du nazisme ou de crimes contre l'humanité au titre du premier amendement, même si un tribunal américain reconnaît des problèmes liés à la liberté d'expression sur un réseau international. Mais la censure pratiquée par les sites Facebook ou YouTube n'est pas justifiée par la loi et contrevient donc aux protections internationales, en particulier à la Déclaration universelle des droits de l'homme de 1946, signée par les États-Unis d'Amérique. Plutôt que pratiquer une censure basée sur les mentalités américaines, une déclinaison de versions locales des sites Internet, respectant les législations nationales ou régionales, permettrait un respect de la liberté d'expression dans le cadre des lois ou traités internationaux.

2) Une compétence judiciaire mal reconnue

Une difficulté, résultant de la mondialisation de l'Internet, est de connaître la juridiction compétente pour connaître d'un litige international, les sites étant implantés sur un territoire et les utilisateurs sur un autre. La jurisprudence française a tendance à considérer que le juge français est compétent si le site est exclusivement dirigé vers le marché français, c'est-à-dire si le site est traduit en français et que l'URL est une adresse en « . fr ». Récemment, le tribunal de grande instance de Paris a toutefois considéré qu'il était compétent concernant un litige entre un ressortissant français et un site dont l'adresse était en « . it » considérant que le site était bien dirigé vers le marché français, car il avait été traduit en français[435]. Toutefois, il reste à ce jugement à être confirmé en cassation et éventuellement au niveau des juges de la Cour de justice de l'Union européenne. Le nouveau Règlement général sur la protection des données de l'Union européenne règle ce conflit de compétence concernant la protection des données dans l'Union européenne[436].

[435] Par un jugement du 14 janvier 2016, le TGI de Paris a considéré qu'un site italien qui offre une traduction en français de son contenu et qui donne les coordonnées d'un distributeur en France de ses produits vise un public français, avec lequel il présente un lien significatif et suffisant. Le tribunal s'est fondé sur l'article 5-3 du règlement communautaire n° 4/2001 qui prévoit qu'« Une personne domiciliée sur le territoire d'un État membre peut être attraite, dans un autre État membre : [...] 3) En matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire ». Le TGI de Paris est donc compétent pour connaître des demandes relatives à l'utilisation d'une marque d'une société française sur un site en .it. (Sylvie Rozenfeld, « Le TGI de Paris compétent pour un site italien visant un public français », 2 mars 2016, *Legalis L'actualité du droit des nouvelles technologies,* URL : https://www.legalis.net/actualite/le-tgi-de-paris-competent-pour-un-site-italien-visant-un-public-francais/ consulté le 12 mars 2018).

[436] Règlement général sur la protection des données, art. 55, 56.

Dans l'Union européenne, la compétence délictuelle et contractuelle peut être définie par application des accords Rome[437] ou Bruxelles 1[438]. Il n'en est pas de même des litiges entre les États-Unis d'Amérique et le reste du Monde, comme le montre le cas Yahoo, les tribunaux américains ayant tendance à appliquer les lois américaines avec une interprétation extraterritoriale manifeste, d'autant que les conditions générales d'utilisation précisent toujours que les tribunaux compétents en cas de litiges sont des tribunaux américains, souvent des tribunaux californiens et que la loi applicable est la loi américaine ou californienne dans ce cas. Toutefois, dans une décision du 5 mars 2015[439], le tribunal de grande instance de Paris a considéré que la clause d'attribution de compétences des conditions générales de Facebook était une clause abusive en droit français, donc frappée de nullité et réputée non écrite, en s'appuyant sur le fait que « *les difficultés pratiques et le coût d'accès aux juridictions californiennes sont de nature à dissuader le consommateur d'exercer toute action devant les juridictions concernant l'application du contrat et à le priver de tout recours à l'encontre de la société Facebook Inc.* » créant ainsi « *un déséquilibre significatif entre les droits et obligations des parties au contrat* ».

Facebook, Google et Amazon ont longtemps refusé d'admettre la légitimité des décisions européennes à leur encontre. Cette position est en train de se modifier depuis les récentes décisions prises au niveau de la Cour de justice de l'Union européenne[440] bien que Google ou Facebook en contestent la portée. Ainsi par application de la décision de la Cour de justice de l'Union européenne, la Commission nationale de l'informatique et des libertés a infligé une amende de 100 000 euros à Google pour déréférencement insuffisant. Google a contesté l'amende devant le Conseil d'État qui a préféré renvoyer la question à la Cour de justice de l'Union européenne[441].

[437] Convention de Rome de 1980 *sur la loi applicable aux obligations contractuelles* publiée au Journal officiel n° C 027 du 26/01/1998 pp. 34-46.
[438] Convention de Bruxelles de 1968 *concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale* publiée au Journal officiel n° L 299 du 31/12/1972 pp. 32-42.
[439] Tribunal de grande instance de Paris, 4e chambre - 2e section, ordonnance du juge de la mise en état du 5 mars 2015.
[440] Cour de justice de l'Union européenne (grande chambre), *Google Spain SL, Google Inc. c/Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Affaire C-131/12, décison du 13 mai 2014 ; Cour de justice de l'Union européenne (grande chambre), Maximillian Schrems c/ Data Protection Commissioner, Affaire nº C 362/14, décision du 6 octobre 2015.
[441] Conseil d'État, Affaire n° 399922, *Google inc.,* décision du 19 juillet 2017.

3) Une coopération internationale inexistante

Les États démocratiques et occidentaux essaient de défendre la liberté d'expression sur Internet même si une certaine limite peut être définie pour protéger l'ordre public et lutter contre la criminalité et le terrorisme. Néanmoins, ils soulignent pratiquement toujours l'impossibilité de tout contrôler et la nécessité de promouvoir l'autorégulation par les internautes[442]. Cette position n'est pas partagée par certains pays moins démocratiques, qui essaient de limiter l'accès, non seulement à certains sites, mais parfois à tout le réseau. La notion de « sécurité de l'État » prend une tout autre forme dans des pays comme la Chine, Singapour ou la Birmanie, qu'en Occident.

En janvier 2015, un tribunal turc ordonne le blocage des sites Internet ayant choisi de reproduire la une du numéro de Charlie Hebdo publié après l'attentat du 7 janvier 2015[443]. Plus généralement, la Turquie a bloqué les sites de Twitter et de YouTube en demandant aux fournisseurs d'accès d'interdire à leurs clients d'accéder à ces sites[444]. En 1996, la Chine a bloqué l'accès à des sites comme CNN, Wall Street Journal et des sites de dissidents à l'étranger[445]. À Singapour, la discussion sur Internet est acceptée seulement si elle ne va pas à l'encontre des valeurs morales, la stabilité politique ou l'harmonie religieuse dans le pays. En Birmanie, la possession d'un accès non autorisé au réseau ou l'envoi ou la réception d'information sur des thèmes comme la sécurité de l'État, l'économie ou la culture nationale était passible d'un emprisonnement de 7 à 15 ans avant la chute de la junte militaire en 2011. Dans de telles régions, la tradition de libertés civiles est faible. En 1996, les pays membres de l'ASEAN[446] se sont mis d'accord pour surveiller Internet et bloquer des sites qui iraient à

---

[442] Signalement des abus en France après la loi pour la confiance dans numérique ou au Royaume-Uni les règles d'autorégulation définies par l'*Independant Press Standards Organization.*

[443] Les Échos, « Ces pays où la "Une" de Charlie Hebdo ne passe pas », 15 janvier 2015, *LesEchos.fr*, URL : https://www.lesechos.fr/15/01/2015/lesechos.fr/0204083595209_ces-pays-ou-la----une---de-charlie-hebdo-ne-passe-pas.htm consulté le 15 décembre 2017.

[444] Le Monde.fr avec Reuters, « La Turquie bloque l'accès à Twitter, WhatsApp, Facebook et YouTube », 4 novembre 2016, Le Monde.fr, URL : http://www.lemonde.fr/pixels/article/2016/11/04/la-turquie-bloque-l-acces-a-twitter-whatsapp-facebook-et-youtube_5025217_4408996.html consultée le 15 décembre 2017.

[445] Frédéric Douzet, « Les frontières chinoises de l'Internet » in *125 – Chine, nouveaux enjeux géopolitiques,* second trimestre 2007, Hérodote revue de géographie et de géopolitique, URL : http://www.herodote.org/spip.php?article282, consulté le 15 décembre 2017.

[446] Association des nations de l'Asie du Sud-Est fondée en 1967 à Bangkok (Thaïlande) par cinq pays Indonésie, Malaisie, Philippines, Singapour et Thaïlande, auxquels se sont joints Brunei (1984), Viet Nam (1995), Laos (1997), Birmanie (1997) et Cambodge (1999).
Lire sur l'ASEAN : Boisseau du Rocher Sophie, « L'Asean et les nouvelles règles du jeu. Le régionalisme en Asie du Sud-est à l'épreuve de la mondialisation », *Revue internationale de politique comparée*, 2001/3 (Vol. 8), pp. 395-417. URL : https://www.cairn.info/revue-internationale-de-politique-comparee-2001-3-page-395.htm consulté le 15 décembre 2017.

l'encontre des « valeurs asiatiques »[447]. Cette expression est vague, mais tout de même inquiétante. Dans de tels pays autoritaires, le contrôle du contenu et de la communication sur Internet se fait par la pression, des menaces, la surveillance et la restriction de l'accès aux moyens de communication.

Internet peut aussi subir des pressions économiques dans les pays démocratiques. L'Union européenne[448] prône la neutralité du réseau et le libre accès aux informations par Internet[449]. En France, la loi pour une République numérique garantit la neutralité de l'internet[450] et l'ARCEP en contrôle l'effectivité[451]. Mais aux États-Unis d'Amérique, alors que l'administration OBAMA protégeait cette neutralité, l'administration TRUMP revient sur cette protection. La Commission fédérale de réglementation des communications, ou FCC, a entériné, le 14 décembre 2017, la fin du principe qui garantit un traitement égal des flux des données par les opérateurs[452]. Si cette décision n'a pas de conséquences immédiates dans l'Union européenne, la neutralité des plateformes de Google et Facebook, dont les sites servent d'interface à un nombre croissant de services, risque à terme de se poser. Il en sera de même avec l'Internet des objets ou les véhicules autonomes qui vont utiliser et nécessiter une bande passante adaptée. Déjà, Stéphane Richard, PDG d'Orange réclame une certaine autonomie : « *Certains usages futurs de l'Internet - je pense à l'Internet des objets ou à la voiture autonome - vont nécessiter des Internet particuliers en termes de latence et de vitesse. Il faudra que nous soyons capables de proposer des Internet avec des fonctionnalités, des puissances et des qualités de service*

[447] Relaté par Paul Mathias, « Liberté d'expression et Internet », *Internet, Enjeux de théorie politique,* Conférence à l'Institut d'Études Politiques de Paris, 31 mars 2000, URL : http://barthes.ens.fr/scpo/Presentations99-00/Bjorstad/ .

[448] 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) nº 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union.*

[449] Cour européenne des droits de l'homme, Arrêt du 22 mai 1990, Requête série A nº 178 Affaire *Autronic AG c/ Suisse* ; Arrêt du 28 novembre 2013, Requête nº 39534/07, Affaire *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung c/ Autriche ;* Arrêt du 18 décembre 2012, requête n° 3111/10, *Affaire Ahmet Yildirim c/ Turquie,*

[450] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, articles 40 à 46.

[451] Code des postes et communications électronique, art. L.32-1 *« II. – Dans le cadre de leurs attributions respectives, le ministre chargé des communications électroniques et l'Autorité de régulation des communications électroniques et des postes prennent, dans des conditions objectives et transparentes, des mesures raisonnables et proportionnées en vue d'atteindre les objectifs suivants : […] 5° bis La neutralité de l'Internet, définie au q du I de l'article L.33-1 ; […]* ».

[452] Federal Communications Commission, "*FCC ACTS TO RESTORE INTERNET FREEDOM - Reverses Title II Framework, Increases Transparency to Protect Consumers, Spur Investment, Innovation, and Competition*", December 14, 2017 at URL : http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db1214/DOC-348261A1.pdf consulté le 15 décembre 2017.

différentes. Il faut nous laisser faire »[453]. Il s'agit d'une demande d'autorégulation à l'américaine. L'égalité d'accès au réseau Internet va-t-elle être remise en cause après la décision américaine ? À terme, la disparition de cette égalité de traitement des flux ouvrirait la porte à une censure qui ne dirait pas son nom. Les internautes privilégieraient les sites ayant un temps de réponse rapide au détriment des sites à accès ralenti. Cette censure serait une censure des plateformes après la censure des services.

§ 2 - La liberté de pensée et de religion vecteur de propagation des sectes dans une société numérisée

La liberté de pensée est associée à la liberté d'expression, elle est aussi liée à la liberté de religion. La liberté de religion ou de conviction est inscrite à l'article 10 de la Déclaration des droits de l'homme et du citoyen de 1789 et au niveau international dans la Déclaration universelle des droits de l'homme[454] à l'article 18, et réaffirmée dans le Pacte international relatif aux droits civils et politiques[455] à l'article 18. Cette liberté comprend, outre la liberté de culte, la liberté de se réclamer d'une religion ou d'une conviction, de ne pas avoir de religion, d'en changer ou d'y renoncer. Au niveau international, la France défend la portée universelle de la liberté de religion et de conviction[456] et rappelle que les droits de l'homme visent à protéger les individus et non les systèmes de pensée comme les religions ou leurs symboles qui ne constituent pas des sujets de droit. La France s'oppose ainsi au concept de « respect des religions » qui légitimerait la répression du blasphème voire la restriction des libertés de pensée de certaines minorités[457]. En droit français, comme en droit international, le concept de

[453] Relaté par Martin Untersinger, « En Europe, la neutralité du Net est garantie par la loi, mais risque d'être écornée », 13 décembre 2017, *Pixels LeMonde.fr*, URL : http://www.lemonde.fr/pixels/article/2017/12/13/en-europe-la-neutralite-du-net-est-garantie-par-la-loi-mais-risque-d-etre-ecornee_5229055_4408996.html consulté le 15 décembre 2017.
[454] Adoptée et proclamée par l'Assemblée générale des Nations Unies, dans sa résolution 217 A (III) du 10 décembre 1948.
[455] Adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale des Nation Unies dans sa résolution 2 200 A (XXI) du 16 décembre 1966, entrée en vigueur le 23 mars 1976.
[456] « Liberté de religion ou de conviction. La France est la liberté de religion et de conviction » en ligne sur http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/droits-de-l-homme/liberte-de-religion-ou-de-conviction/, consulté le 18 février 2017.
[457] Ibid..

blasphème n'est pas reconnu et seuls les appels caractérisés à la haine, à la discrimination ou à la violence pour des raisons à base religieuse, raciale, ethnique ou nationale peuvent être condamnés[458]. En outre, la « loi Gayssot »[459] pose pour principe la « répression de tout acte raciste, antisémite ou xénophobe » et modifie la loi sur la liberté de la presse en conséquence[460]. Les mouvements sectaires qui portent atteinte à la dignité et à l'intégrité humaines peuvent être dissous après une condamnation de ces pratiques par le juge[461]. Par la répression pénale d'actes contraires à la dignité de l'homme ou à son intégrité, la France s'est également dotée d'armes juridiques pour lutter contre les mouvements et réseaux sectaires. Ainsi, la liberté de religion n'est pas directement limitée par la loi, seuls les effets collatéraux entrant en conflit avec d'autres droits fondamentaux sont réprimés légalement.

Internet est un vecteur de propagation de la liberté de pensée et de la liberté de religion. De nombreuses églises y possèdent un ou plusieurs sites d'information et d'expression. Comme pour la liberté d'expression et d'opinion, la réglementation internationale n'est pas homogène. Aux États-Unis d'Amérique, la liberté de religion est protégée par le premier amendement et tout prêcheur peut y créer son église, sans restriction apparente. En Europe, une législation contre les sectes voit le jour, mais les critères d'appréciation varient d'un pays à l'autre, une église reconnue au-delà des Pyrénées peut être considérée comme secte en deçà.

À proprement parler, Internet est neutre vis-à-vis de la liberté religieuse et ne favorise aucune religion. Derrière son clavier, l'internaute reste libre de choisir sa religion. Mais, l'outil de communication qu'est Internet est utilisé par les églises pour communiquer avec leurs fidèles, voire pour recruter de nouveaux adeptes. La liberté religieuse trouve un terreau pour s'épanouir avec l'Internet, elle permet aussi la recrudescence de mouvements sectaires, non directement détectés comme tels ou qui utilisent les divergences d'appréciation entre pays.

---

[458] Loi n° 72-546 du 1 juillet 1972 *relative à la lutte contre le racisme* parue au journal officiel de la République française n°0154 du 2 juillet 1 972 p. 6803.

[459] Loi n° 90-615 du 13 juillet 1990 *tendant à réprimer tout acte raciste, antisémite ou xénophobe* parue au journal officiel de la République française n° 0162 du 14 juillet 1 990 p. 8333.

[460] Jean-Yves Monfort, « Liberté d'expression, loi de 1881, et respect des croyances : une cohabitation impossible ? », *LEGICOM*, 2015/2 (N° 55), pp. 29-35. URL : https://www.cairn.info/revue-legicom-2015-2-page-29.htm consulté le 4 avril 2018.

[461] Voir ci-après La liberté de culte en France et les mouvements sectaires.

A) La présence des communautés religieuses sur Internet

Les grandes organisations religieuses n'ont pas mesuré le potentiel d'Internet dans les premières années de son déploiement. À partir d'initiatives individuelles, la plupart des religions ont compris l'importance et l'intérêt d'Internet en termes de communication, et donc l'intérêt d'y être présent et actif[462].

1) La facilité de communication des églises avec leurs adeptes

Le WEB a vu la création de sites spécialisés dans les religions chrétienne[463], catholique[464], musulmane[465] ou juive[466], mais aussi bouddhique[467] voir sectaires[468]. À travers tous ces sites communautaires, l'internaute peut retrouver des informations lui facilitant la pratique de son culte, même peu répandu en France. Une communauté peut exister et se créer, même si ses membres sont disséminés sur l'ensemble du territoire sans point de concentration notable. Des actualités religieuses, des événements tels les dates de début et de fin du ramadan, des cours de langues, hébreu ou arabe littéraire, des cours d'instruction religieuse tels l'étude de la Torah, mais aussi des mises en garde contre l'antisémitisme ou des informations communautaires seront ainsi proposés.

Toutes ces facilités, liées aux techniques du numérique, ne pourraient pas se développer avec les techniques traditionnelles. En France, avant Internet, seules des émissions spécifiques existaient sur une chaîne de télévision à un horaire particulier, le dimanche matin, quelle que soit la religion concernée. Ces émissions continuent aujourd'hui et, par exemple, l'émission « Le jour du Seigneur » sur la seconde chaîne nationale propose chaque dimanche, ou à Noël, la retransmission en direct d'une célébration de la messe. Cette retransmission est particulièrement suivie par les malades ou les personnes qui ne peuvent plus se déplacer ou qui ne disposent plus près de leur domicile de lieu de culte ouvert. Pour les autres religions, seuls des causeries ou des entretiens sont diffusés, avec cependant, parfois, des offices relatifs à des événements importants pour la communauté religieuse.

---

[462] Jean-François Mayer, « Internet et religion », *Religioscope*, 2008.
[463] http://topchretien.jesus.net/ consulté le 12 mai 2012.
[464] http://www.eglise.catholique.fr/accueil.html consulté le 12 mai 2012.
[465] http://uoif-online.com/ consulté le 4 février 2015.
[466] http://www.col.fr/ consulté le 12 mai 2012.
[467] http://www.bouddhiste.org/ consulté le 12 mai 2012.
[468] http://www.scientologie.fr/ consulté le 5 mai 2012.

D'autres religions, moins implantées sur le territoire français, utilisent ces moyens pour communiquer avec leurs fidèles. Le bouddhisme, peu développé en France, met sur son site des informations définissant les principaux termes utilisés : Nirvana, triple joyau, Karma. Il explicite les différentes formes du bouddhisme : le bouddhisme theravada, le bouddhisme mahayana ou « grand véhicule » et le bouddhisme hinayana ou « petit véhicule ». Il permet une première prise de connaissance du bouddhisme sans avoir, dans son entourage proche, un adepte ou un initié.

Les églises savent utiliser les nouvelles techniques pour rester en relation avec leurs adeptes ou permettre à d'autres de s'informer tant sur le dogme que sur les événements. Elles forment les clercs aux nouvelles techniques de communication[469]. Mais ces techniques sont aussi utilisées par les sectes ou les mouvements salafistes pour recruter de nouveaux adeptes[470].

2) Le prosélytisme des sectes et de la mouvance salafiste favorisé par les techniques numériques

Avant l'apparition des moyens numériques, les sectes se propageaient et recrutaient de nouveaux adeptes par le démarchage à domicile et les contacts personnels. Avec Internet, les sectes disposent de leurs propres sites, sites diffusant leurs informations à partir de pays étrangers pour contourner les limitations légales pouvant exister dans certains pays.

Dans son rapport 2013-2014[471], la mission interministérielle de vigilance et de lutte contre les dérives sectaires analyse l'apport d'Internet pour la mouvance sectaire. Internet favorise l'emprise mentale en retardant la prise de conscience de cette emprise par l'entourage. En effet dès que des proches perçoivent une radicalisation de la pensée, ils la désapprouvent et tentent de la combattre. En s'isolant sur Internet, l'individu qui se radicalise soit en adhérant aux idées d'un mouvement sectaire, soit à une mouvance terroriste, ne laissera pas percevoir cette radicalisation à son entourage, sachant par ailleurs, que le groupe sectaire ou terroriste lui demande de rompre ou d'affaiblir les liens avec son monde social. Internet facilite l'adhésion à

---

469 Conseil pontifical pour les communications sociales, *L'église et Internet,* en ligne à http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_church-Internet_fr.html, consulté le 22 février 2017.

470 Gérald Bronner, « II. Pourquoi Internet s'allie-t-il avec les idées douteuses ? », dans *La démocratie des crédules.* Paris, Presses Universitaires de France, « Hors collection », 2013, pp. 55-128. URL : https://www.cairn.info/la-democratie-des-credules--9782130607298-page-55.htm consulté le 15 décembre 2017.

471 Mission interministérielle de vigilance et de lutte contre les dérives sectaires, « Le risque sectaire et Internet », *Rapport au Premier ministre, 2013-2014*, La Documentation française.

un mouvement dès que l'individu est déjà en recherche. Généralement en cherchant sur Internet des réponses à un questionnement personnel, psychique ou médical, l'individu en recherche va progressivement entrer dans la mouvance sectaire[472]. La scientologie a créé de nombreux sites pseudo-médicaux qui redirigent vers d'autres sites plus radicaux. Il facilite également l'auto-endoctrinement et la radicalisation de l'individu en le rendant solitaire et isolé[473]. Les témoins de Jéhovah, la scientologie ou la mouvance salafiste utilisent les possibilités de l'Internet pour recruter ou convertir de nouveaux adeptes.

Le choix des religions, d'y adhérer ou d'y renoncer est garanti par la Constitution et la Déclaration des droits de l'homme et du citoyen, ainsi que par des textes internationaux[474]. La France n'a pas limité cette liberté, seules certaines pratiques sont interdites, par exemple, l'enterrement est obligatoirement réalisé avec un cercueil en France[475], le cadavre enseveli dans la terre directement avec son seul linceul est interdit pour des raisons d'hygiène publique.

La possibilité de création de sites sectaires est difficilement contrôlable et l'existence d'un site ne peut être remise en cause que dans les cas prévus par la législation : atteinte à la dignité humaine, incitation à la haine raciale, etc., ce qui contribue à la prolifération des sectes sur Internet. Le contrôle des sectes est d'autant plus délicat que certaines sectes sont considérées comme des églises dans d'autres pays. Les États-Unis d'Amérique protègent les sectes au nom de la liberté de culte et d'expression[476], et à partir du territoire nord-américain[477], ces « églises » peuvent recruter des adeptes dans les pays où elles sont considérées comme des sectes[478]. L'église de scientologie dispose d'un portail dédié à la France, mais le site l'abritant est géré

[472] Jean-Claude Maes, *Emprise et manipulation. Peut-on guérir des sectes ?*De Boeck Supérieur, « Carrefour des psychothérapies », 2010, 286 pages. URL : https://www.cairn.info/emprise-et-manipulation--9782804101503.htm consulté le 4 avril 2018.

[473] Jean-Claude Maes, « Le lien sectaire : des relations fondées sur la rupture. Critique de "l'expérience sectaire : rupture ou réparation" », *Thérapie Familiale*, 2006/2 (Vol. 27), pp. 133-159. URL : https://www.cairn.info/revue-therapie-familiale-2006-2-page-133.htm consulté le 4 avril 2018.

[474] Article 18 de la Déclaration universelle des droits de l'homme de 1948 ; article 9 de la Convention européenne des droits de l'homme de 1950 ; article 10 de la Charte des droits fondamentaux de l'Union européenne de 2000.

[475] Code général des collectivités territoriales, articles R. 2213-25 à 27.

[476] 1er amendement, (voir supra).

[477] Bruneau Fouchereau, « AU NOM DE LA LIBERTE RELIGIEUSE Les sectes, cheval de Troie des États-Unis en Europe », mai 2001, *Le Monde diplomatique,* disponible en ligne à http://www.prevensectes.com/lobbies5.htm consulté le 15 décembre 2017.

[478] Nathalie Luca, « Quelles politiques face aux sectes ? La singularité française », *Critique internationale*, 2002/4 (nº 17), pp. 105-125. URL : https://www.cairn.info/revue-critique-internationale-2002-4-page-105.htm consulté le 4 avril 2018.

depuis les États-Unis d'Amérique[479] et se trouve donc protégé par le premier amendement et la jurisprudence Yahoo![480].

Sur son site, il incite les internautes à contacter un scientologue et à rejoindre l'église de scientologie pour défendre les droits de l'homme et lutter contre certaines dérives de la société. Ce site est l'un des rares sites consultés qui est sonorisé dès son accession. Le prosélytisme y est présent et palpable. Son objectif est de recruter de nouveaux adeptes, à travers un discours complexe et pseudo-scientifique : « *L'accomplissement extraordinaire de la Dianétique et de la Scientologie a été de mettre au point des méthodes précises et exactes destinées à améliorer la conscience spirituelle de l'Homme et ses aptitudes* ».

Sur Internet, la Scientologie publie un site concernant la liberté de religion « Défendre la liberté de religion, pour la Scientologie et toutes les religions »[481] où sont repris les principaux arguments des défenseurs des droits de l'homme orientés vers la défense de la scientologie et tendant à contrer les arguments la présentant comme une secte.

D'autres églises utilisent des moyens détournés pour se faire connaître. Les mormons ou l'« Église de Jésus-Christ des saints des derniers jours » met à disposition un site de recherche généalogique utilisé par tous les adeptes de généalogie pour retrouver des informations à partir des photos numérisées des archives d'état civil collectées dans de nombreux pays[482]. L'accès à ce site a été fermé pour la France durant les négociations avec la Commission nationale de l'informatique et des libertés[483]. Suite au premier accord de 1960, signé avant la loi informatique et libertés, un nouvel accord a été signé entre la CNIL et Family Search International pour numériser, transférer vers les États-Unis d'Amérique et mettre en ligne les archives d'état civil français[484], archives également partiellement proposées par les départements dans le cadre de la loi CADA[485] puis, depuis 2015, du Code des relations entre le

[479] Les mentions légales du site précisent *"This website is owned and operated by The Church of Scientology International."* Domiciliée à Los Angeles en Californie (consulté le 5 mai 2012)
[480] Cf. supra.
[481] At http://www.libertedereligion.org/.
[482] https://familysearch.org/ consulté le 5 juin 2012.
[483] Constaté par l'auteur lors de recherches généalogiques.
[484] Commission nationale de l'informatique et des libertés, Délibération n° 2015-125 du 7 avril 2015 *autorisant la société FamilySearch International à mettre en œuvre plusieurs traitements automatisés de données à caractère personnel ayant pour finalités la numérisation et le transfert vers les États-Unis d'Amérique de copies d'archives publiques ainsi que la diffusion et l'indexation de l'image de ces documents sur son site Internet à visée généalogique et dans ses centres de consultation* (Demande d'autorisation n° 1625100).
[485] Loi nº 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* publiée au JORF du 18 juillet 1978 p. 2851.

public et l'administration[486]. Les actes de l'état civil sont accessibles en ligne s'ils ont plus de cent ans, environ, mais les dispenses catholiques de consanguinité ne sont accessibles en ligne que par l'intermédiaire du site de Family Search.

La mouvance salafiste utilise aussi les moyens du réseau Internet et les réseaux sociaux pour soit convertir à l'Islam de nouveaux adeptes, soit ramener dans l'Islam fondamental les brebis égarées, c'est-à-dire des musulmans trop occidentalisés[487]. Dans cette mouvance, des sites djihadistes existent et peuvent sous couvert de religion amener les nouveaux adeptes à des actes de terrorisme.

Au niveau européen, la notion de secte n'est pas harmonisée, l'Espagne reconnaît l'Église de scientologie comme une église[488], donc une religion légale, alors que la France la classe dans les mouvements sectaires. La Belgique s'est dotée d'une législation proche de celle existant en France[489].

B) La protection de la liberté religieuse face aux mouvements sectaires sur Internet

La liberté de pensée et de religion fut défendue par Voltaire[490] lors de l'affaire Calas (mars 1762). La liberté de religion reste synonyme de tolérance, elle est incluse dans les droits de l'homme, mais face à certaines pratiques de mouvements sectaires, la législation a été amenée à garantir la protection des individus contre les abus. Cette protection n'est pas universelle et en Europe, certains pays, comme la France, luttent contre les sectes indirectement via la protection de l'intégrité des individus[491], d'autres pays, comme l'Espagne[492], reconnaissent certaines sectes comme des églises.

La nécessité de combattre les pratiques sectaires abusives semble faire l'unanimité en Europe, mais elle se heurte à deux principes essentiels de notre démocratie : la liberté de croyance ou de religion et la liberté d'association[493]. La frontière entre intolérance et limitation des abus et

[486] Créé par l'Ordonnance n° 2015-1341 du 23 octobre 2015 *relative aux dispositions législatives du code des relations entre le public et l'administration*, publiée au JORF n°0248 du 25 octobre 2015 page 19872.
[487] Jean-Pierre Filiu, « Définir Al-Qaida », *Critique internationale*, 2010/2 (n° 47), pp. 111-133. URL : https://www.cairn.info/revue-critique-internationale-2010-2-page-111.htm consulté le 15 décembre 2017.
[488] Le 12 décembre 2007, conformément à une décision de la Cour Nationale de Madrid du 11 octobre 2007, le Ministère de la Justice espagnol a inscrit l'Église de Scientologie au Registre des Entités Religieuses.
[489] Loi du 26 novembre 2011, entrée en vigueur le 2 février 2012.
[490] Voltaire, *Traité sur la tolérance, A l'occasion de la mort de Jean Calas* 1763.
[491] Au travers de la Miviludes et de la loi nº 2001-504 du 12 juin 2001 dite loi About-Picard.
[492] Cf. supra
[493] Annick Dosner-Dolivet, « Loi sur les sectes », *Recueil Dalloz* 2002, p. 1086.

dérives sectaires n'est pas clairement définie, sans doute par absence de définition légale d'une secte ou d'un mouvement sectaire[494]. L'État laïque n'a aucune compétence pour apprécier la valeur d'un mouvement de pensée, et donc d'un courant religieux.

Avec Internet et l'utilisation contrôlée de cet outil de communication par les mouvements sectaires, pour la mission interministérielle de vigilance et de lutte contre les dérives sectaires ou Miviludes[495], il existe trois niveaux de préoccupations : le caractère séducteur d'Internet et son effet démultiplicateur du risque ; la possibilité de présenter « *sous forme de tromperies* » des projets, des prestations et des produits indépendamment du fonctionnement du réseau ou du mouvement sectaire et donc d'aménager l'irresponsabilité juridique de ces mouvements et réseaux ; le foisonnement de propositions mêlant quête de bien-être, d'accomplissement de soi, de développement personnel[496].

Après un travail parlementaire et gouvernemental commencé en 1983[497] avec le rapport Vivien, la France a opté en 2001 pour une législation répressive alors que d'autres pays européens ont décidé de reconnaître certaines sectes en tant qu'églises. Concernant les sites djihadistes, la répression ne relève pas de la lutte contre les mouvements sectaires, mais elle relève de la lutte antiterrorisme.

1) La liberté de culte en France et les mouvements sectaires

L'article 10 de la Déclaration des droits de l'homme et du citoyen dispose : « *Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi* ». Tout comme pour la liberté d'expression, la limite de la liberté de religion est d'ordre législatif et réside dans le trouble de l'ordre public. Depuis 1905, l'État français garantit la liberté de culte. Devant l'apparition de mouvements sectaires, des garde-fous législatifs ont été adoptés au début du XXIe siècle pour protéger les individus et l'ordre

[494] Constat présent dans Alain Gest, Jacques Guyard, Rapport no 2 468 *sur les sectes*, enregistré à la Présidence de l'Assemblée nationale le 22 décembre 1995

[495] La Miviludes est une mission interministérielle instituée auprès du Premier ministre par décret présidentiel du 28 novembre 2002 (Décret n° 2002-1392 du 28 novembre 2002 *instituant une mission interministérielle de vigilance et de lutte contre les dérives sectaires*).

[496] Miviludes « Internet : l'amplification du risque de dérives sectaires » in *Rapport au Premier ministre* 2008, La documentation française.

[497] Alain Vivien, *Les sectes en France, expression de la liberté morale ou facteurs de manipulations ?* Rapport au Premier Ministre, 1 983 La Documentation française at http://ns4005993.ip-192-99-13.net/rap83a.htm et http://ns4005993.ip-192-99-13.net/rap83b.htm.

public, la limite entre église et secte reste à définir. Historiquement les premiers chrétiens étaient plus proches d'un mouvement sectaire que d'une église.

La loi de séparation des Églises et de l'État en 1905[498], élément clé de la laïcité française, introduit la notion de « culte » qui désigne la pratique associée à une croyance au sens large. L'État s'interdit de définir ce qu'est ou n'est pas une religion ou une croyance[499]. Dans son article premier, cette loi dispose que « *la République assure la liberté de conscience. Elle garantit le libre exercice des cultes sous les seules restrictions édictées ci-après dans l'intérêt de l'ordre public* ». Selon l'article 1 de la Constitution française de 1958, « *La France est une République indivisible, laïque, démocratique et sociale. Elle assure l'égalité devant la loi de tous les citoyens sans distinction d'origine, de race ou de religion. Elle respecte toutes les croyances* ». La liberté de culte est ainsi constitutionnellement garantie.

Le 20 décembre 1995, une commission parlementaire d'enquête adopte à l'unanimité un rapport sur les sectes[500]. Ce rapport reconnaît la difficulté de définir une secte ou un mouvement sectaire et, plutôt que l'élaboration d'une loi spécifique, préconise de lutter contre les sectes en utilisant l'arsenal législatif existant relatif à la protection de l'individu et de l'ordre public. Sur la base des indices suivants : déstabilisation mentale, caractère exorbitant des exigences financières, rupture induite avec l'environnement d'origine, atteintes à l'intégrité physique, embrigadement des enfants, discours plus ou moins antisocial, troubles à l'ordre public, importance des démêlés judiciaires, éventuel détournement des circuits économiques traditionnels et tentatives d'infiltration des pouvoirs publics, le rapport liste 173 mouvements sectaires, dont les Témoins de Jéhovah. La France qui s'opposait, pour cette raison, à la nomination dans les prisons d'aumôniers représentant les témoins de Jéhovah a dû, sous la pression de la Cour européenne des droits de l'homme[501] et du Conseil d'État[502], accepter la nomination de tels aumôniers.

Le 12 juin 2001, une loi tendant à renforcer la prévention et la répression des mouvements sectaires est adoptée par le Parlement[503]. Cette loi permet par son article 1, la dissolution civile

---

[498] Loi du 9 décembre 1905 *concernant la séparation des Églises et de l'État* publiée au journal officiel de la République française du 11 décembre 1905 p. 7205.

[499] Annick Dorsner-Dolivet, *Loi sur les sectes*, Recueil Dalloz 2002, Page 1086.

[500] Alain Gest, Jacques Guyard, Rapport n° 2 468 *sur les sectes*, enregistré à la Présidence de l'Assemblée nationale le 22 décembre 1995, accessible via http://www.assemblee-nationale.fr/rap-enq/r2468.asp, consulté le 15 décembre 2017.

[501] Cour européenne des droits de l'homme, *Association Les Témoins de Jéhovah c/ France*, requête n° 8916/05, décision du 30 juin 2011.

[502] Conseil d'État, *Garde des Sceaux, ministre de la justice et des libertés c/ m. n... et autres*, décision du 16 octobre 2013.

[503] Loi n° 2001-504 du 12 juin 2001 *tendant à renforcer la prévention et la répression des mouvements sectaires portant atteinte aux droits de l'homme et aux libertés fondamentales* parue au JORF n°135 du 13 juin 2001 p. 9337,

de certaines personnes morales qui poursuivent « *des activités ayant pour but ou pour effet de créer, de maintenir* ou *d'exploiter la sujétion psychologique ou physique des personnes qui participent à ces activités »* après une condamnation définitive de la personne morale ou de l'un de ses dirigeants pour atteinte à l'intégrité physique ou psychique de la personne, atteinte aux libertés de la personne, atteinte à la dignité de la personne, exercice illégal de la médecine, publicité mensongère[504]. Ainsi la liberté de religion ou de culte n'est pas restreinte directement, seules certaines condamnations pénales peuvent entraîner la dissolution d'une personne morale représentant un mouvement sectaire[505].

Le 16 octobre 2013, soit quatorze ans après les premiers recours de victimes contre la Scientologie, la Cour de cassation[506] confirme le jugement de la Cour d'appel de Paris du 2 février 2012, condamnant deux structures de la Scientologie, le *Celebrity Center* et sa librairie SEL (Société Espace Librairie), à des amendes de respectivement 200 000 et 400 000 euros pour escroquerie en bandes organisées. Reprochant aux prévenus d'avoir profité de la vulnérabilité d'anciens adeptes pour leur soutirer de fortes sommes d'argent, la justice a également condamné cinq scientologues à des peines d'amende et de prison avec sursis. La Scientologie a aussitôt indiqué vouloir porter l'affaire devant la Cour européenne des droits de l'homme. Le 5 juin 2014, la Cour européenne des droits de l'homme a déclaré irrecevable la demande d'annulation de la condamnation pour escroquerie en bande organisée.

Toutefois, cette condamnation définitive ne peut entraîner de dissolution, car celle-ci, rétablie depuis, a été temporairement supprimée par un article de loi voté discrètement dans un texte « fourre-tout »[507], démontrant ainsi la puissance de lobbying de ce mouvement.

---

loi modifiée par la loi n°2007-1787 du 20 décembre 2007 *relative à la simplification du droit* parue au JORF n°0296 du 21 décembre 2007 p. 20639.

[504] L'article 19 de cette loi punit d'une amende de 7 500 euros le fait de diffuser par tout moyen des messages de promotion d'une telle personne morale.

[505] Commentaires : Florence Belivier, *RTD Civ*. 2001 p. 682, Annick Dorsnet-Dolivet, *Recueil Dalloz* 2002, p. 1086.

[506] Cour de cassation, chambre criminelle, Audience publique du 16 octobre 2013 N° de pourvoi : 03-83910 05-82121 12-81532.

[507] Loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures publiée au JORF n°0110 du 13 mai 2009 p. 7920.

2) La liberté de religion et les mouvements sectaires dans le Monde

Ce lobbying est visible au niveau mondial, où il n'existe aucune politique cohérente de lutte contre les mouvements sectaires. Peu de pays disposent d'une législation de lutte contre les sectes, celles-ci se protégeant par un appel sans restriction à la liberté de religion et à l'impartialité des États.

Aux États-Unis d'Amérique, le 1er amendement protège la liberté de religion. Les églises y bénéficient par ailleurs d'avantages fiscaux importants[508], expliquant la prolifération de mouvements minoritaires, voire de sectes.

La Fédération de Russie a adopté un régime relativement tolérant de façade[509], qui a établi une sorte de « protectionnisme religieux », officiellement destiné à faire face à l'arrivée des « sectes » dans le pays, mais qui assure en fait la prépondérance du Patriarcat orthodoxe[510], auquel des missions d'ordre social ont été confiées ainsi que l'établissement d'aumôneries, alors que la plupart des autres communautés sont placées dans une situation précaire. Les organisations religieuses ont une obligation d'enregistrement annuelle tant qu'elles ne disposent pas d'un document qui atteste leur existence depuis au moins quinze ans sur le territoire correspondant[511]. Dissoudre une communauté religieuse lui interdit de posséder ou louer des biens, d'avoir un compte bancaire, d'engager des employés et de se défendre juridiquement[512].

La liberté de pensée, de conscience et de religion est un droit fondamental, consacré par l'article 9 de la Convention européenne des Droits de l'Homme. Pour la Cour européenne des droits de l'homme, le contentieux États contre églises n'est guère important avec les religions majoritaires, car les dogmes sont connus et les relations avec les États sont stabilisées. En

---

[508] « *L'article 501 du code des impôts américains précise que ces associations sont exemptées de taxes, à condition qu'elles ne fassent pas de politique...* » cité par Authentiqua, « Pourquoi y-a-t-il autant de sectes aux États-Unis ? », 3 décembre 2017, *#traditions des pays Vivreaupresent,* URL : http://vivreaupresent.over-blog.com/pourquoi-y-a-t-il-autant-de-sectes-aux-etats-unis consulté le 15 décembre 2017.

[509] Loi *sur la liberté de conscience et les organisations religieuses*, adoptée le 26 septembre 1997.

[510] Moniak-Azzopardi Agnieszka, « Les religions et l'État en Russie », *Le Courrier des pays de l'Est* 5/2004 (nº 1045), pp. 28-38 at http://www.cairn.info/revue-le-courrier-des-pays-de-l-est-2004-5-p.-28.htm.

[511] Kathy Rousselet, « La liberté de conscience en Russie : du transfert d'un concept au conflit de normes », in Sylvie Martin (dir.) *Circulation des concepts entre Occident et Russie*, [en ligne], Lyon, ENS LSH, mis en ligne le 10 décembre 2008. à http://institut-est-ouest.ens-lsh.fr/spip.php?article147.

[512] Cour européenne des droits de l'homme, *Témoins de Jéhovah c/ Russie*, décision du 10 juin 2010.

revanche, la question est plus délicate avec les religions minoritaires et les nouveaux groupements religieux appelés « sectes »[513].

Saisie du problème des nouveaux mouvements religieux dans l'affaire Fédération chrétienne des témoins de Jéhovah de France c/ France[514], la Cour européenne des droits de l'homme a relevé que la loi française avait pour but de renforcer la prévention et la répression des mouvements sectaires portant atteinte aux droits de l'homme et aux libertés fondamentales. Précisant qu'elle « *n'a pas pour tâche de se prononcer in abstracto sur une législation* » et ne saurait donc exprimer un point de vue sur la compatibilité des dispositions du texte législatif français avec la Convention, la Cour a cependant donné de précieuses indications. Elle a, certes, relevé que, « *dans la mesure où elle vise les sectes - dont elle ne donne aucune définition - cette loi prévoit la dissolution de celles-ci ; mais cette mesure ne peut être prononcée que par voie judiciaire et lorsque certaines conditions se trouvent réunies, notamment lorsque les sectes ou leurs dirigeants ont fait l'objet de condamnations pénales définitives pour des infractions limitativement énumérées* ».

En Belgique, la publication d'un rapport d'enquête concernant les mouvements sectaires, enquête déroulée de 1996 à 1997[515], adopté le 28 avril 1997, a provoqué une violente controverse au Parlement qui a dû renoncer à définir une liste de sectes, et a valu à l'État belge une condamnation en justice en 2005[516], condamnation toutefois anéantie par la Cour de cassation[517]. En 2011, le Parlement belge a voté une nouvelle infraction[518], proche de celle de la loi About-Picard, réprimant l'abus de vulnérabilité, et érigeant la déstabilisation psychologique en circonstance aggravante. En Belgique, la loi du 2 juin 1998 a créé un Centre

[513] Extrait de Cour Européenne des droits de l'homme, Division de la Recherche, *Aperçu de la jurisprudence de la Cour en matière de liberté de religion,* 19 janvier 2011 mise à jour au 31 octobre2013, en ligne à l'URL : http://www.echr.coe.int/Documents/Research_report_religion_FRA.pdf consulté le 15 décembre 2017.

[514] Cour européenne des droits de l'homme, *Décision sur la recevabilité de la requête nº 53430/99 présentée par la Fédération Chrétienne des Témoins de Jéhovah de France contre la France* du 6 novembre 2001.

[515] Duquesne et Willems, *Enquête parlementaire visant à élaborer une politique en vue de lutter contre les pratiques illégales des sectes et le danger qu'elles représentent pour la société et pour les personnes, particulièrement les mineurs d'âge*, Chambre des Représentants de Belgique, 313/7 - 95/96 à http://www.dekamer.be/FLWB/pdf/49/0313/49K0313007.pdf et http://www.dekamer.be/FLWB/pdf/49/0313/49K0313008.pdf .

[516] Drieu Dodefridi, *Sectarisme parlementaire* in LaLibre.be publié le 28 octobre 2005 at http://www.lalibre.be/debats/opinions/sectarisme-parlementaire-51b88c0fe4b0de6db9ace680.

[517] Cour de cassation de Belgique, Arrêt nºC.05.0494.N *État Belge contre Église universelle du Royaume de Dieu, a.s.b.l., .O. J-C., B. K., D.B.B. A. N.*, 1 juin 2006.

[518] Loi du 26 novembre 2011, entrée en vigueur le 2 février 2012.

d'information et d'avis sur les organisations sectaires nuisibles, centre publiant un rapport d'activités tous les deux ans[519].

En février 2013, le Parlement luxembourgeois a adopté une législation similaire. Mais comme l'écrit Rudy Salles dans son rapport[520] « *Les divergences autour de la problématique des "sectes" démontrent qu'il est difficile de trouver un consensus européen sur ce sujet et dressent un constat d'échec de plusieurs initiatives européennes.* »

Dans son rapport 2008, la Miviludes[521] insiste sur le fait que la vigilance des États de droit, face aux mouvements sectaires, se joue sur Internet[522]. Internet est utilisé par les mouvements sectaires pour contester systématiquement le bien-fondé des actions de l'État contre leurs agissements répréhensibles ou dangereux. Ainsi en 2013, la Scientologie a systématiquement attaqué toutes les décisions judiciaires françaises prises à l'encontre de ses membres, personnes physiques ou morales, sous couvert de la liberté de religion. Un site spécifique existe même pour défendre cette liberté de religion[523] : « *Défendre la liberté de religion, pour la Scientologie et toutes les religions* », site apparaissant en tête de liste des recherches avec le critère de recherche « liberté de religion ». Les mouvements sectaires et leurs alliés aiment à porter le débat sur le terrain de la liberté religieuse en se positionnant ainsi comme les victimes des atteintes à cette liberté. Les argumentaires déployés par les uns et les autres devant l'ONU n'échappent pas à la règle[524]. À l'ONU comme ailleurs, il est question d'une supposée « violation de la liberté de religion » avec son corollaire, la discrimination dont sont accusés tous les acteurs de la lutte et de la vigilance contre les dérives sectaires qui mèneraient une « croisade » et qui sont, au passage, assimilés à des « instances sectaires de discrimination et de violence ». Comme coresponsables de cette discrimination, sont stigmatisées les initiatives parlementaires telles que les rapports de commission d'enquête, en particulier la « liste » des

[519] Le rapport d'activités 2015-2016 peut être consulté à l'adresse http://www.ciaosn.be/rapport_bisannuel2015-2016.pdf consulté le 15 décembre 2017.

[520]Commission des questions juridiques et des droits de l'homme, *La protection des mineurs contre les dérives sectaires*, Doc. 13 441, Assemblée parlementaire, Conseil de l'Europe, 17 mars 2014.

[521] Mission interministérielle de vigilance et de lutte contre les dérives sectaires, URL : http://www.miviludes.gouv.fr/ .

[522] Miviludes « Internet : l'amplification du risque de dérives sectaires » in *Rapport au Premier ministre* 2008, La documentation française.

[523] At http://www.libertedereligion.org/, consulté le 20 avril 2012.

[524] Lire à ce sujet le rapport transmis à la Commission des Droits de l'Homme de l'ONU par l'église de scientologie française : *Contribution to the Other Stakeholders Report - Submission by European Office for Human Rights of the Church of Scientology* de juin 2012, en ligne à https://www.ericroux.com/attachment/414726/ consulté le 15 décembre 2017.

mouvements publiée dans le premier rapport de commission d'enquête parlementaire « Les sectes en France », ainsi que la loi About-Picard, unanimement décriée par ces mouvements.

Sous-section 2. Les libertés de mouvement dans la société numérique

Dans la société numérique, à côté des libertés de la pensée, d'expression et de religion, d'autres droits fondamentaux peuvent être facilités ou entravés. Il en est ainsi de la liberté de réunion et de la liberté d'aller et venir. Internet permet l'organisation de réunions virtuelles. Certaines assemblées générales d'actionnaires sont ainsi relayées en direct sur le réseau. La faculté d'aller et venir d'un individu peut profiter de la technique, mais celle-ci peut aussi permettre en le localisant de le cantonner dans un espace restreint ou de surveiller ses déplacements[525].

Internet peut être utilisé pour créer des groupes de personnes, groupements d'intérêt ou groupes hétéroclites d'échange. Les réseaux sociaux sont un vecteur de création de groupes puisque chacun peut créer son propre groupe d'« amis », groupe virtuel[526]. Ils peuvent aussi être utilisés pour lancer des invitations à se retrouver dans un endroit précis à une heure donnée, donc d'organiser des rassemblements physiques.

La liberté d'aller et venir va profiter des moyens de se localiser sur un plan, de se déplacer vers un but précis. Mais le déplacement peut aussi être préparé en utilisant divers services disponibles sur Internet : réservation de moyens de transport, réservation de lieux de repos, réservations de repas, préparation des visites à effectuer. Les moyens pour favoriser ces libertés peuvent aussi se retourner contre elles en facilitant la localisation des individus qui les utilisent, ou en révélant des préparatifs de voyage. La société numérique permet aux individus de tenir des réunions virtuelles, participation aux assemblées d'actionnaires, réunions d'entreprises ou simples téléconférences[527].

---

[525] Myriam Quéméner, « La géolocalisation : un outil de protection ou de surveillance ? », *Sécurité et stratégie*, 2013/4 (15), pp. 11-17. URL : https://www.cairn.info/revue-securite-et-strategie-2013-4-page-11.htm consulté le 12 février 2018.

[526] Godefroy Dang Nguyen, Virginie Lethiais, « Impact des réseaux sociaux sur la sociabilité. Le cas de Facebook », *Réseaux*, 2016/1 (n° 195), pp. 165-195. URL : https://www.cairn.info/revue-reseaux-2016-1-page-165.htm consulté le 12 février 2018.

[527] Raluca Iugulescu-Lestrade, « Téléconférence et visioconférence ou les paradoxes des outils de simplification des réunions », *Revue française d'administration publique*, 2016/1 (N° 157), pp. 105-116. URL : https://www.cairn.info/revue-francaise-d-administration-publique-2016-1-page-105.htm consulté le 13 février 2018.

§ 1 - La liberté de réunion et d'association dans la société numérique

Les libertés de la pensée, d'expression, de communication, de culte, ne peuvent s'exprimer que si la liberté de réunion et la liberté d'association sont garanties[528]. Dans la société numérique, la possibilité d'organiser des réunions est favorisée par les moyens de communication mis à disposition des internautes ainsi que la possibilité de contacter rapidement un nombre important d'individus. Les réseaux sociaux permettent de constituer des groupements d'individus, groupements virtuels ou groupements associatifs avec rencontres et activités partagées. La liberté de réunion et d'association autorise l'individu à se réunir dans le cadre d'une association ou d'un syndicat, mais aussi à se réunir sur la voie publique pour une manifestation.

L'Internet et les réseaux sociaux accessibles depuis un smartphone sont des outils facilitateurs d'organisation de rassemblements. Un message court, donnant rendez-vous en un endroit précis, à une date donnée peut être envoyé à quelques dizaines de correspondants qui vont eux-mêmes relayer cette invitation à quelques dizaines d'autres. Après quelques itérations, ce sont plusieurs milliers d'individus qui ont reçu l'invitation, et ce en quelques heures voire minutes. Ces messages peuvent aussi être utilisés pour connaître les organisateurs de ces réunions, les premiers émetteurs des messages, et permettre leur arrestation dans les régimes policiers. Des alternatives de réseaux anonymisés existent, mais ils permettent aussi des déviances et des délits.

Au Brésil, en août et septembre 2011, une manifestation anticorruption a été organisée, au départ par quelques internautes, vite rejoints par plusieurs centaines d'autres, alertés par les réseaux sociaux et la diffusion des messages « d'amis à amis »[529].

En janvier 2011, ces mêmes réseaux ont facilité les rassemblements en Égypte sur la place Tahir[530]. Facebook a apparemment été vital à l'opposition en tant qu'outil de rassemblement et de communication libre, Twitter quant à lui, a permis de donner une dimension d'instantanéité à l'information. Les sites communautaires ont, aujourd'hui de façon indéniable, un réel pouvoir de rassemblement des foules dans tous les pays. Ils ont été également fortement utilisés en

[528] Le premier amendement de la Constitution des États-Unis d'Amérique garantit l'ensemble de ces libertés comme un tout.

[529] « Les Brésiliens se mobilisent contre la corruption », *LeMonde.fr*, 20 septembre 2011 à http://www.lemonde.fr/ameriques/article/2011/09/20/les-bresiliens-se-mobilisent-contre-la-corruption_1574614_3222.html consulté le 5 mai 2012.

[530] « *La révolution égyptienne ou le rôle des médias sociaux dans les soulèvements* », *Blog,* 11 avril 2011, URL : http://egypterevolution.wordpress.com/, consulté le 5 mai 2012.

Tunisie lors de la chute du régime de Ben Ali[531]. Bien sûr, ces réseaux ne créent pas l'événement, ils l'accompagnent et lui permettent de se développer, en quelque sorte, ils sont des catalyseurs des mouvements de contestation contre les régimes autoritaires, surtout qu'ils sont difficiles à censurer et à fermer. Le printemps arabe de 2011 a dû, en partie, son succès à ces nouvelles technologies[532] qui ont permis la préparation des rassemblements « spontanés » sans alerter les autorités dans des régimes autoritaires. Ainsi la lutte contre la corruption au Brésil ou la lutte contre un pouvoir autoritaire en Égypte, pour ne prendre que ces deux exemples, profitent de la technique mise à disposition des internautes avec l'émergence du WEB 2.0.

En France, les réseaux sociaux sont aussi utilisés pour regrouper des individus alertés par ces courts messages dans le cadre de l'organisation d'« apéros géants », rassemblements moins politiques, mais plus conviviaux ou de *rave-party* non autorisée[533]. Les libertés de réunion[534] et d'association[535] sont protégées en France, les réseaux sociaux ne sont qu'un moyen parmi d'autres de faire connaître le lieu de rassemblement d'une manifestation, la presse classique relayant souvent l'information. Ils ont aussi été utilisés pour préciser des lieux et dates de concerts géants non autorisés et éviter ainsi la mise en place de cordons de sécurité empêchant l'accès aux sites choisis.

Il est régulièrement fait état par la presse de rassemblements mal contrôlés, une invitation à un anniversaire qui devient un mégarassemblement[536] provoquant des nuisances de voisinage. Parfois, l'invitation échappe à son auteur, et le rassemblement tourne à l'émeute. En général, ces débordements sont dus à une mauvaise utilisation des outils, leur utilisation mal contrôlée pouvant provoquer ces dysfonctionnements. Dans le cas d'une invitation de 50 copains,

[531] Mokhtar Ben Henda, « Internet dans la révolution tunisienne », *Hermès, La Revue*, 2011/1 (n° 59), pp. 159-160. URL : https://www.cairn.info/revue-hermes-la-revue-2011-1-page-159.htm consulté le 12 février 2018.
[532] Yves Gonzalez-Quijano, « Internet, le "Printemps arabe" et la dévaluation du cyberactivisme arabe », *Égypte/Monde arabe*, 2015/1 (n° 12), pp. 67-84. URL : https://www.cairn.info/revue-egypte-monde-arabe-2015-1-page-67.htm consulté le 12 février 2018.
[533] Renaud Epstein, « Les raves ou la mise à l'épreuve underground de la centralité parisienne », *Mouvements*, 2001/1 (n°13), pp. 73-80. URL : https://www.cairn.info/revue-mouvements-2001-1-page-73.htm consulté le 12 février 2018.
[534] Loi du 30 juin 1881 *sur la liberté de réunion*, Recueil Duvergier, pages 379 à 390.
[535] Loi du 1er juillet 1901 *relative au contrat d'association* publiée au JORF du 2 juillet 1901 page 4025.
[536] « Anniversaire géant et tapage nocturne "monstre" à Vertou cette nuit », *Presse Océan*, 6 mai 2012, URL : http://www.presseocean.fr/actu/actu_detail_-Anniversaire-geant-et-tapage-nocturne-monstre-a-Vertou-cette-nuit_9182, 40 310,403 11, 12 028,120 27, 12 024,129 81, 9180-2073953_actu.Htm, consulté le 10 mai 2012.

devenue une invitation à 50 000[537], le père d'un adolescent a décidé de porter plainte pour usurpation d'identité, les invitations relayées ayant été faites au nom de son fils, après, semble-t-il, l'annulation de l'événement, montrant ainsi la difficulté d'arrêter un mouvement lancé sur ces réseaux sociaux et se propageant de manière exponentielle.

A) La liberté de réunion encadrée par la loi

La liberté de réunion, ou droit de réunion, est une liberté publique et politique généralement considérée comme fondamentale et en vertu de laquelle un groupe de personnes a la possibilité de se rassembler et de se réunir temporairement en un même lieu, de façon pacifique et sans armes, dans toute finalité licite et conforme à la loi. Au niveau national, les réunions sont libres[538]. Au niveau international, elle est mentionnée dans l'article 20 de la Déclaration universelle des droits de l'homme[539] et dans l'article 21 du Pacte international relatif aux droits civils et politiques[540]. Au niveau européen, ce sont l'article 11 de la Convention européenne des droits de l'homme[541] et l'article 12 de la Charte des droits fondamentaux de l'Union européenne[542] qui protègent cette liberté.

---

[537] « Près de 50 000 personnes s'invitent à un anniversaire via Facebook », *France Info,* 26 avril 2012, URL : http://www.franceinfo.fr/high-tech/pres-de-50-000-personnes-s%E2%80%99invitent-a-un-anniversaire-via-facebook-597821-2012-04-26 consulté le 10 mai 2012.

[538] Loi du 30 juin 1881, art. 1er : « *Les réunions publiques sont libres.*
Elles peuvent avoir lieu sans autorisation préalable, sous les conditions prescrites par les articles suivants ».

[539] Déclaration universelle des droits de l'homme, Article 20 « *1. Toute personne a droit à la liberté de réunion et d'association pacifiques.*
2. Nul ne peut être obligé de faire partie d'une association ».

[540] Pacte international relatif aux droits civils et politiques, Article 21 « *Le droit de réunion pacifique est reconnu. L'exercice de ce droit ne peut faire l'objet que des seules restrictions imposées conformément à la loi et qui sont nécessaires dans une société démocratique, dans l'intérêt de la sécurité nationale, de la sûreté publique, de l'ordre public ou pour protéger la santé ou la moralité publiques, ou les droits et les libertés d'autrui* ».

[541] Convention européenne des droits de l'homme, Article 11 – *Liberté de réunion et d'association*
« 1. Toute personne a droit à la liberté de réunion pacifique et à la liberté d'association, y compris le droit de fonder avec d'autres des syndicats et de s'affilier à des syndicats pour la défense de ses intérêts.
« 2. L'exercice de ces droits ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, 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, ou à la protection des droits et libertés d'autrui. Le présent article n'interdit pas que des restrictions légitimes soient imposées à l'exercice de ces droits par les membres des forces armées, de la police ou de l'administration de l'État ».

[542] Charte des droits fondamentaux de l'Union européenne, Article 12 *Liberté de réunion et d'association*
« *1. Toute personne a droit à la liberté de réunion pacifique et à la liberté d'association à tous les niveaux, notamment dans les domaines politique, syndical et civique, ce qui implique le droit de toute personne de fonder avec d'autres des syndicats et de s'y affilier pour la défense de ses intérêts.*
« *2. Les partis politiques au niveau de l'Union contribuent à l'expression de la volonté politique des citoyens de l'Union* ».

Dans de nombreux pays, les Autorités se réservent le droit d'interdire certaines réunions, notamment en cas de risque de trouble à l'ordre public ou d'atteinte aux personnes et aux biens, ce qui est susceptible d'être interprété comme une forme de censure.

1) L'encadrement de la liberté de réunion et de manifestation en France

Longtemps, les réunions publiques ont été organisées exclusivement sous l'égide de l'Église (processions, entrées princières, etc.), à l'exception des bans seigneuriaux. La situation évolue au XVIIIe siècle avec la mode des salons et des cafés, où s'élaborent en partie les idées des Lumières, et qui donne naissance aux premiers clubs : le club breton, le club des Jacobins, etc. préfigurant les partis politiques[543]. La Déclaration des droits de l'homme et du citoyen institutionnalise les clubs en proclamant en son article 11 la « libre communication des pensées et des opinions », mais les mots « liberté de réunion » ou « liberté de se rassembler » ne sont pas directement écrits dans la Déclaration de 1789[544]. La Constitution de 1791 garantit le droit des citoyens de se réunir paisiblement[545]. Une première mesure d'interdiction est le décret de fermeture du Club des Jacobins[546], le 12 novembre 1794, voté par la Convention nationale dans le cadre de la Réaction thermidorienne. Elle sera suivie, sous le Directoire, de l'interdiction du Club du Panthéon le 8 ventôse an IV (27 février 1796) par Bonaparte[547], et sous le Consulat, de

[543] Raymond Huard, « Chapitre 1. Retour sur un passé lourd de pesanteurs. La Révolution et l'Empire », dans *La naissance du parti politique en France.* Paris, Presses de Sciences Po (P.F.N.S.P.), « Académique », 1996, pp. 25-46. URL : https://www.cairn.info/la-naissance-du-parti-politique-en-france--9782724606833-page-25.htm consulté le 14 mars 2018.

[544] Pierre-Henri Prélot, *Droit des libertés fondamentales*, Hachette, 2e éd., 2010, pp. 289 et s.

[545] Extrait de l'article 1er de la Constitution de 1791, « *La Constitution garantit pareillement, comme droits naturels et civils : […] La liberté aux citoyens de s'assembler paisiblement et sans armes, en satisfaisant aux lois de police* »

[546] « *La fermeture du club des Jacobins, qui suivit de peu la condamnation à mort de Carrier, signifiait bien le démantèlement de l'héritage idéologique de la Révolution, la condamnation du mouvement qui avait conduit le système de régénération des Lumières à l'horreur. C'est bien ce qu'écrit, le 25 brumaire an II, la Gazette historique et politique de la France et de l'Europe à la double nouvelle de la condamnation à mort de Carrier et de la fermeture du club des Jacobins : "Ils ne nous noieront plus, ils ne nous mitrailleront plus, ils ne canonneront plus le peuple français pour le rendre meilleur".* » (Extrait de Jean-Marc Varaut, « 5 - Le tour de France de la Terreur », dans *La Terreur judiciaire. La Révolution contre les droits de l'homme*. Paris, Éditions Perrin, « Hors collection », 1993, pp. 221-270. URL : https://www.cairn.info/la-terreur-judiciaire--9782262010119-page-221.htm consulté le 14 mars 2018).

[547] « *Sur décision des directeurs, Bonaparte, commandant de l'armée de l'Intérieur et proche de Barras, ferme le club du Panthéon le 27 février 1796 et, dans le même mouvement, en fait autant pour les sociétés aristocratiques du Salon des princes, de la maison Serilly, de la Société des échecs. Les troupes parisiennes sont déplacées ou licenciées lorsqu'elles refusent. En juin, les chouans, Cadoudal, Scépeaux, Frotté se soumettent, laissant les directeurs face à des adversaires liés à la sans-culotterie et à la Montagne.* » (Extrait de Jean-Clément Martin, « Le nouveau régime », dans *Nouvelle histoire de la Révolution française.* Paris, Éditions Perrin, « Pour

la fermeture autoritaire du club du Manège par Fouché le 26 thermidor an VII (13 août 1799)[548]. Désormais, toute réunion publique est soumise à autorisation préalable. L'article 291 du Code pénal de 1810 prévoit notamment que « *Nulle association de plus de vingt personnes, dont le but sera de se réunir tous les jours ou certains jours marqués, pour s'occuper d'objets religieux, littéraires, politiques ou autres, ne pourra se former qu'avec l'agrément du Gouvernement, et sous les conditions qu'il plaira à l'autorité publique d'imposer à la société.* »

Ce point de vue est réaffirmé par tous les régimes successifs à de multiples reprises : article 20 de l'ordonnance des 5-6 juillet 1820, « loi d'inquiétude » du 10 avril 1834, etc.

Sous l'impulsion de Rouher, Napoléon III autorise en 1868 les réunions publiques sous réserve qu'on s'abstienne d'y délibérer de questions politiques ou religieuses[549]. Les réunions politiques seront toutefois autorisées pendant la campagne électorale (décision du 6 mai 1868). Dans un contexte de crise, le gouvernement de la défense nationale impose de nouveau (par décret du 22 janvier 1871) l'obligation d'autorisation des réunions publiques. L'autorisation est remplacée par une simple déclaration aux autorités vingt-quatre heures à l'avance avec la loi du 30 juin 1881 qui affirme dans son article 1[er] : « *les réunions publiques sont libres* ». La loi sur la liberté de réunion du 28 mars 1907[550] lèvera définitivement cette injonction de déclaration en disposant que « *Les réunions publiques, quel qu'en soit l'objet, pourront être tenues sans déclaration préalable* », les réunions publiques sont libres à la condition de ne pas se tenir sur la voie publique[551].

Pour toute manifestation sur la voie publique, défilé, concert, exposition, une autorisation de la commune ou de la préfecture reste nécessaire sous couvert du respect de l'ordre public et de la

---

l'histoire », 2012, pp. 488-521. URL : https://www.cairn.info/nouvelle-histoire-de-la-revolution-francaise--9782262041748-page-488.htm consulté le 14 mars 2018)

[548] Jean-Philippe Rey, « Brumaire », dans *Histoire du Consulat et du Premier Empire.* Paris, Éditions Perrin, « Synthèses historiques », 2016, pp. 17-36. URL : https://www.cairn.info/histoire-du-consulat-et-du-premier-empire--9782262069858-page-17.htm consulté le 14 mars 2018.

[549] « *Le Conseil d'État et les députés entourent la liberté de réunion accordée par le texte d'un grand luxe de précautions. Les réunions ne sont libres que si elles ne portent ni sur la politique ni sur la religion. Si l'on veut traiter de ces deux matières, il faut une autorisation préalable et la réunion doit se tenir en présence d'un fonctionnaire de l'ordre judiciaire qui peut la dissoudre à tout moment. Les réunions électorales sont autorisées sous certaines conditions.* » (Extrait de Jean-Claude Yon, « Une libéralisation mal maîtrisée », dans *Le Second Empire. Politique, société, culture.* Paris, Armand Colin, « U », 2012, pp. 59-81. URL : https://www.cairn.info/le-second-empire--9782200246075-page-59.htm consulté le 14 mars 2018).

[550] Loi du 28 mars 1907 *relative aux réunions publiques* publiée au journal officiel de la République française du 29 mars 1907 p. 2493.

[551] Loi du 30 juin 1881 sur la liberté de réunion, article 6. « *Les réunions ne peuvent être tenues sur la voie publique ; elles ne peuvent se prolonger au-delà de onze heures du soir ; cependant, dans les localités où la fermeture des établissements publics a lieu plus tard, elles pourront se prolonger jusqu'à l'heure fixée pour la fermeture de ces établissements* ».

sécurité publique[552]. L'autorisation peut être soumise à la mise en place d'un service d'ordre par les organisateurs. Ainsi, une manifestation « spontanée », organisée impromptu via les réseaux sociaux reste illégale. Si la liberté de réunion est reconnue et consacrée, la liberté de manifestation est contrainte par l'obligation de la préservation de l'ordre public.

2) La liberté d'association et d'affiliation à des syndicats

La liberté de réunion comprend aussi la liberté d'association et d'affiliation à des syndicats. La liberté d'association est régie par la loi du 1er juillet 1901[553]. En 1971, la loi Marcellin tente d'introduire un contrôle préalable qui sera rejeté par le Conseil constitutionnel car contraire à la libre constitution des associations[554] en s'appuyant sur le préambule de la Constitution. Dès 1950, le Conseil d'État a rangé la liberté d'association au nom des libertés publiques fondamentales[555], puis en 1956, il la qualifie de principe fondamental reconnu par les lois de la République[556]. Il existe des types d'associations particulières, en particulier les syndicats professionnels. Ils permettent aux professionnels de s'assembler pour défendre leurs intérêts. Le droit syndical est rappelé dans le préambule de la Constitution du 27 octobre 1946 : « *Tout homme peut défendre ses droits et ses intérêts par l'action syndicale et adhérer au syndicat de son choix* ». Dans la société numérique, les syndicats utilisent les techniques de communication comme la messagerie pour diffuser les informations syndicales en remplacement des distributions de tracts aux sorties des bureaux ou usines.

Alors que sous l'ancien régime, les professions se regroupaient en corporations avec des règles de fonctionnement très strictes, la loi Le Chapelier des 14 et 17 juin 1791 a prohibé tout groupement professionnel[557]. La loi du 21 mars 1884 reconnaît la liberté syndicale, liberté consacrée constitutionnellement[558] dans le préambule de la Constitution du 27 octobre 1946,

---

[552] Code la sécurité intérieure, articles L.211-1 à L.211-4.
[553] Loi du 1er juillet 1901 relative au contrat d'association, publiée au JORF du 2 juillet 1901 page 4025.
[554] Conseil constitutionnel, Décision n° 71-44 DC du 16 juillet 1971, *Loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association.*
[555] Conseil d'État, Décision du 1er février 1950, *Girard.*
[556] Conseil d'État assemblée plénière, Décision du11 juillet 1956, *Amicale des Annamites de Paris et sieur Nguyen-Duc-Frang.*
[557] René Mouriaux, « Les origines », dans *Le syndicalisme en France.* Paris, Presses Universitaires de France, « Que sais-je ? », 2009, pp. 9-25. URL : https://www.cairn.info/le-syndicalisme-en-france--9782130576112-page-9.htm consulté le 14 mars 2018.
[558] Conseil constitutionnel, Décision nº 89-257 DC du 25 juillet 1989, *Loi modifiant le code du travail et relative à la prévention du licenciement économique et au droit à la conversion*.

alinéa 6 à 8. Le Code du travail précise que tout salarié peut librement adhérer à un syndicat professionnel de son choix[559]. Cette liberté d'adhésion a pour corollaire la liberté de ne pas adhérer à un syndicat. En France, certaines catégories de fonctionnaires connaissent des restrictions à la liberté syndicale pour des raisons d'intérêt général[560]. La Cour européenne des droits de l'homme a jugé que l'interdiction absolue des syndicats au sein de l'armée française est contraire à l'article 11 de la Convention européenne des droits de l'homme[561]. Mais elle a reconnu à l'État français la possibilité de dissoudre une association de supporters d'une équipe de football dans un but d'intérêt général[562]. Et, alors qu'un avocat doit le respect aux autorités judiciaires et doit contribuer au respect de l'ordre, la cour reconnaît le droit à un avocat de participer à une manifestation non prohibée dès lors qu'il ne commet, lui-même, à cette occasion, aucun acte répréhensible[563].

Pour fonctionner correctement, un syndicat doit pouvoir communiquer librement avec ses adhérents et les informer. Concernant la diffusion des informations syndicales dans l'entreprise, l'article L.2142-6 du Code du travail prévoit que les outils numériques disponibles au sein d'une entreprise peuvent être utilisés dans les conditions et modalités de diffusion établies par un accord d'entreprise[564]. La diffusion de tracts ou d'informations syndicales en utilisant la messagerie de l'entreprise ou son intranet reste liée à la conclusion d'un accord d'entreprise[565]. La négociation de tels accords n'est pas imposée à l'entreprise, donnant ainsi la possibilité à l'employeur de s'y soustraire.

Sans accord particulier, les informations et tracts peuvent toutefois être mis à disposition sur un site syndical accessible par Internet, solution utilisée par tous les syndicats. Cette possibilité leur permet de diffuser des informations vers des employés non présents physiquement sur le site de l'entreprise, télétravail, détachement, etc. Les employés peuvent également s'inscrire sur ces sites pour recevoir dans leur messagerie personnelle ou professionnelle ces informations

---

Pierre Avril, Jean Gicquel, « Liberté syndicale et liberté personnelle du salarié » [Note sous décision n° 89-257 DC], *Pouvoirs*, janvier 1990, n° 52, p. 187, URL : http://www.revue-pouvoirs.fr/IMG/pdf/Pouvoirs52_p175-195_ccf.pdf consulté le 15 mars 2018.

[559] Code du travail, article L.2141-1.

[560] Loi n° 72-662 du 13 juillet 1972 portant statut général des militaires.
Code de la défense, article L.4121-4.

[561] Cour européenne des droits de l'homme, Affaire *Matelly c/ France* du 2 octobre 2014, requête nº 10609/10.

[562] Cour européenne des droits de l'homme, Affaire *Les Authentiks et Supras Auteuil 91 c/ France* du 27 octobre 2016, Requêtes nos 4 696/11 et 4 703/11.

[563] Cour européenne des droits de l'homme, Affaire *Ezelin c/ France* du 26 avril 1991, requête nº 11800/85.

[564] Conseil constitutionnel, Décision nº 2013-345 QPC du 27 septembre 2013, *Syndicat national Groupe Air France CFTC*.

[565] Antoine Cristau, « Vie syndicale et accès aux NTIC de l'entreprise », *LEGICOM*, 2002/2 (N° 27), pp. 57-67. URL : https://www.cairn.info/revue-legicom-2002-2-page-57.htm consulté le 14 mars 2018.

syndicales. Alors qu'une diffusion par messagerie est passive pour l'employé, la consultation d'un site syndical nécessite une action volontaire[566]. Les informations proposées sont diverses : aide à la négociation, information juridique, actualité des prud'hommes, conseil et formation des délégués et élus professionnels, etc. les sites des syndicaux peuvent être ouverts à tous pour certaines informations génériques ou réservées aux adhérents pour des informations ciblées[567].

B) La liberté de réunion et de manifestation hors de France

Le premier amendement de la Constitution des États-Unis d'Amérique protège la liberté de réunion et de rassemblement. Il garantit explicitement « *le droit des gens à s'assembler paisiblement, et à adresser des pétitions au gouvernement pour redresser des torts* »[568].
En Allemagne, ce droit est garanti par l'article 8 de la Loi fondamentale de la République fédérale d'Allemagne. En Espagne, l'article 21 de la Constitution espagnole de 1978 le protège. Elle est également garantie dans la République d'Irlande par l'article 40.6.1 de la Constitution d'Irlande. La liberté de manifestation n'a été reconnue positivement en droit britannique que par le *Human Rights Act* de 1998[569].
La liberté syndicale fait également l'objet d'une protection internationale[570], même si ce droit n'est pas universellement reconnu par les États[571]. Le droit de réunion est stipulé dans plusieurs accords internationaux : l'article 20 de la Déclaration universelle des droits de l'homme, l'article 21 du Pacte international relatif aux droits civils et politiques. Au niveau européen, la liberté syndicale est proclamée dans l'article 11[572] de la Convention européenne de sauvegarde

[566] Xavier Orgerit, « Le développement du "e-syndicalisme" et la liberté syndicale à l'ère de la communication numérique », *Lettre « Actualités Droits-Libertés »,* CREDOF, 2 octobre 2013.
[567] Biétry Franck, « Les syndicats à l'heure des réseaux », *Revue française de gestion*, 4/2005 (nº 157), pp. 79-102.
[568] "*the right of the people peaceably to assemble, and to petition the Government for a redress of grievances".*
[569] Aurélien Antoine, « La liberté de manifestation au Royaume-Uni », *Jus Politicum*, n° 17, URL : http://juspoliticum.com/article/La-liberte-de-manifestation-au-Royaume-Uni-1135.html consulté le 14 mars 2018.
[570] Nadjib Souamaa, « L'OIT d'un après-guerre à l'autre : entre modèle universel et régionalisme européen », *Les cahiers Irice*, 2012/1 (n° 9), pp. 23-46. URL : https://www.cairn.info/revue-les-cahiers-irice-2012-1-page-23.htm consulté le 15 mars 2018.
[571] Thomas Amossé, Jean-Michel Denis, « Discrimination syndicale et formes d'antisyndicalisme dans le monde. Repères internationaux et parcours de lecture », *Travail et emploi,* 2016/2 (n° 146), pp. 5-16. URL : https://www.cairn.info/revue-travail-et-emploi-2016-2-page-5.htm consulté le 15 mars 2018.
[572] Convention européenne des droits de l'homme, Article 11 - Liberté de réunion et d'association
« 1. Toute personne a droit à la liberté de réunion pacifique et à la liberté d'association, y compris le droit de fonder avec d'autres des syndicats et de s'affilier à des syndicats pour la défense de ses intérêts.
« 2. L'exercice de ces droits ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à la sûreté publique, à la défense

des droits de l'homme et l'article 12[573] de la Charte des droits fondamentaux de l'Union européenne, ainsi que par l'article 5 de la Charte sociale européenne du 18 octobre 1961 et par l'article 11 de la Charte communautaire des droits sociaux fondamentaux des travailleurs du 9 décembre 1989. Au niveau international, ce droit est consacré par la Convention de l'OIT n° 87 du 9 juillet 1948 avec création d'un Comité de la liberté syndicale chargé d'examiner les plaintes déposées par les organisations syndicales contre un État membre.

Malgré ces traités internationaux, il existe de par le Monde, des États qui ne garantissent pas le droit d'expression et de réunion. Afin de pallier ces restrictions et permettre à des dissidents de communiquer dans ces États, des logiciels de communication sur Internet ont été développés pour protéger l'identité des personnes. Ces logiciels ont créé un espace particulier, le Darknet, espace parallèle à l'Internet et non directement accessible par les outils classiques.

Le logiciel libre et gratuit Tor (acronyme de "*The Onion Router*") permet de naviguer sur Internet par l'intermédiaire d'autres ordinateurs du réseau Tor, basés aux quatre coins de la planète. Il en existe une version fonctionnant sous Android, le système d'exploitation développé par Google. Ainsi, l'adresse IP de l'ordinateur utilisé, véritable plaque d'immatriculation, apparaîtra, aléatoirement, au Japon, aux États-Unis ou en Grande-Bretagne, rendant sa localisation impossible ou plus difficile par les services de surveillance ou de police.

Originellement développé sous l'égide de la Navy américaine, Tor est aujourd'hui maintenu et développé par une organisation indépendante, le Tor Project. Pour l'année fiscale 2011, 60 % de son financement provenait du gouvernement américain, et 18 % de fondations et de subventions, comme l'indique son dernier rapport. Éternel paradoxe : la protection offerte par le réseau est à la fois utilisée par les militaires américains, à des fins de renseignement notamment, et combattue par la NSA et le GCHQ, son équivalent britannique[574].

Darknet a été créé à l'origine pour aider les dissidents chinois à communiquer entre eux sans pouvoir être identifiés. La création du Darknet a donc permis aux dissidents d'exister, de pouvoir communiquer entre eux et le reste du monde, et donc de faire suivre l'information à

de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. Le présent article n'interdit pas que des restrictions légitimes soient imposées à l'exercice de ces droits par les membres des forces armées, de la police ou de l'administration de l'État ».

[573] Charte des droits fondamentaux de l'Union européenne, Article 12 - Liberté de réunion et d'association
« *1. Toute personne a droit à la liberté de réunion pacifique et à la liberté d'association à tous les niveaux, notamment dans les domaines politique, syndical et civique, ce qui implique le droit de toute personne de fonder avec d'autres des syndicats et de s'y affilier pour la défense de ses intérêts.* »

[574] Voir Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 1. § 2 -B) La lutte contre le terrorisme au niveau international.

travers le WEB sans aucun risque pour leur sécurité, ou en minimisant ce risque. Les défenseurs de la vie privée considèrent le système Tor comme un bon outil pour les internautes désireux de se protéger. Des journalistes l'utilisent également pour ne pas être repérés par des régimes répressifs ou échanger avec des sources sensibles sans risquer de les compromettre[575]. Le Darknet est un outil idéal pour faire part d'événements réels, d'exactions commises par des gouvernements, des militaires proches du pouvoir ou même des dirigeants. Dans certains pays comme la Chine, l'Iran, le Pakistan ou la Turquie, le simple fait d'en discuter constitue un délit qui peut exposer à la prison, la torture et parfois même à l'exécution.

Se réunir, communiquer nécessite de pouvoir se déplacer. La technique numérique n'a pas encore fourni le moyen de transfert physique, mais elle fournit une assistance à la préparation de ses déplacements et à leur réalisation.

§ 2 - La liberté de se déplacer dans un univers numériquement cartographié

Un smartphone, outre l'accès au réseau Internet ou accessoirement au réseau téléphonique, permet à son possesseur d'emporter avec lui une carte numérisée des pays situés sur les cinq continents de notre planète. Associé au GPS, technique initialement développée pour les militaires et le guidage de certains missiles, ce smartphone devient un assistant soit pour se déplacer d'un point à un autre, soit pour trouver un service proche de son emplacement actuel ou de sa destination. Les États démocratiques ont érigé la liberté d'aller et venir comme une des libertés fondamentales et une composante de la liberté individuelle. La technique numérique contribue à cette liberté, mais elle peut aussi servir à localiser un individu.

A) La liberté de déplacement et la géolocalisation

La liberté d'aller et venir est avec la sûreté, un droit fondamental de l'individu. Il peut se déplacer sans être suivi, espionné. La géolocalisation peut être utilisée pour un voyage privé comme pour un voyage d'affaires. Dans des pays à la sécurité aléatoire, la géolocalisation peut

[575] « *Comment le Darknet peut-il améliorer la vie des gens ?* », publié le 18 janvier 2105 à https://lucieetval.wordpress.com/tag/edward-snowden/, consulté le 1 mars 2017.

être utilisée pour sécuriser un voyage[576]. Mais les moyens numériques utilisés lors d'un déplacement peuvent constituer une entrave avec ces droits, une liberté surveillée n'est plus la liberté[577].

1) Les sources de la liberté de déplacement

La liberté de se déplacer, d'aller et venir est une des libertés fondamentales[578]. En France, le Conseil constitutionnel lui a reconnu une valeur constitutionnelle[579]. Cette liberté se déduit de l'article 4 de la Déclaration des droits de l'homme et du citoyen de 1789[580]. Elle est garantie par l'article 66 de la Constitution du 4 octobre 1958[581]. Au niveau européen, cette liberté découle de l'article 5 « *Droit à la liberté et à la sûreté* » de la Convention européenne des Droits de l'Homme ou de l'article 6 de la Charte des droits fondamentaux de l'Union européenne[582]. Pour la Cour européenne des droits de l'homme, la privation de liberté ne se limite pas à l'emprisonnement, mais peut être liée à l'exiguïté de la zone de confinement et à une surveillance quasi permanente[583]. Pour déterminer si un individu se trouve « privé de sa liberté » au sens de l'article 5, la Cour part de sa situation concrète et prend en compte un ensemble de critères comme le genre, la durée, les effets et les modalités d'exécution de la mesure

---

[576] David Amsellem, Kevin Limonier, « L'utilisation des outils cartographiques dans la sûreté des déplacements d'affaires », *Sécurité et stratégie*, 2014/4 (19), pp. 5-12. URL : https://www.cairn.info/revue-securite-et-strategie-2014-4-page-5.htm consulté le 14 février 2018.

[577] Emmanuel Valjavec, « Internet, un nouvel espace de liberté sous surveillance », *Études*, 2013/3 (Tome 418), pp. 317-327. URL : https://www.cairn.info/revue-etudes-2013-3-page-317.htm consulté le 13 février 2018.

[578] Jean Rivero, Hugues Moutouh, *Libertés publiques,* Tome II, 7e édition, Presses universitaires de France, p.102.

[579] Conseil constitutionnel, Décision n° 79-107 DC du 12 juillet 1979 *Loi relative à certains ouvrages reliant les voies nationales ou départementales,* considérant no 3 « *[…] la liberté d'aller et venir est un principe de valeur constitutionnelle […]* ».
Conseil constitutionnel, Décision no 2004-492 DC du 2 mars 2004 *Loi portant adaptation de la justice aux évolutions de la criminalité,* considérant no 4 « *[…] l'exercice des libertés constitutionnellement garanties ; qu'au nombre de celles-ci figurent la liberté d'aller et venir, l'inviolabilité du domicile privé, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789, ainsi que la liberté individuelle, que l'article 66 de la Constitution place sous la surveillance de l'autorité judiciaire* ».

[580] Déclaration du 26 août 1789 des droits de l'homme et du citoyen. - Article 4 « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui. Ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la loi* ».

[581] Constitution du 4 octobre 1958 - Article 66 « *Nul ne peut être arbitrairement détenu.*
« L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi ».

[582] Charte des droits fondamentaux de l'Union européenne, article 6 : « *Toute personne a droit à la liberté et à la sureté* ».

[583] Cour européenne des droits de l'homme, *Affaire Guzzardi c/ Italie*, Requête no 7367/76, Arrêt du 6 novembre 1980.

considérée[584]. La notion de privation de liberté comporte un aspect objectif, l'internement d'un individu dans un espace restreint pendant un laps de temps non négligeable, et un aspect subjectif, le fait que cet individu n'a pas consenti à cet internement[585]. La privation de liberté peut exister dans des situations autres qu'une arrestation ou une incarcération, ce peut être un placement dans un hôpital psychiatrique[586], un confinement dans une zone de transit d'un aéroport[587], une assignation à domicile[588], etc.

Cette liberté peut être restreinte par le législateur pour des raisons de sauvegarde d'autres droits : prévention de l'ordre public, recherche d'auteurs d'infractions, etc. Les simples restrictions à la liberté de circulation sont régies par l'article 2 du Protocole nº 4, la différence restant une différence de degré ou d'intensité et non de nature. Les restrictions doivent être des mesures nécessaires « *à la sécurité nationale, à la sûreté publique, au maintien de l'ordre public, 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* », et prévues par la loi. Des mesures alternatives à l'emprisonnement existent et limitent la liberté de déplacement des individus sous le contrôle du juge des libertés : assignation à résidence, bracelet électronique[589]. Dans ces cas, l'individu ne peut sortir d'un périmètre défini et contrôlé, le bracelet électronique permettant de le localiser en temps réel.

Ce même protocole précise que toute personne présente régulièrement sur le territoire d'un État a le droit d'y circuler librement, toute personne est en droit de quitter n'importe quel pays y compris le sien. Le traité de Rome du 25 mars 1957 instituant la communauté européenne a reconnu la libre circulation des personnes au sein de la communauté, principe repris dans l'article 3 du traité de Lisbonne (Traité sur l'Union européenne) signé le 13 décembre 2007 : « *l'Union offre à ses citoyens un espace de liberté, de sécurité et de justice sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes* ».

---

[584] Ibid.
[585] Cour européenne des droits de l'homme, *Affaire Storck c/ Allemagne*, Requête no 61603/00, Arrêt du 16 juin 2005.
[586] Ibid.
[587] Cour européenne des droits de l'homme, *Affaire Amuur c/ France*, Requête no 19776/92, Arrêt du 25 juin 1996.
[588] Cour européenne des droits de l'homme, *Affaire Mancini c/ Italie*, Requête nº 44955/98, Arrêt du 2 août 2001.
[589] Dan Kaminski, Sonia Snacken, Michel van de Kerchove, « Mutations dans le champ des peines et de leur exécution », *Déviance et Société*, 2007/4 (Vol. 31), pp. 487-504. URL : https://www.cairn.info/revue-deviance-et-societe-2007-4-page-487.htm consulté le 4 avril 2018.

2) Les restrictions à la géolocalisation

La liberté de se déplacer implique que toute personne, en dehors des contraintes légales dues à une restriction de se déplacer prononcée par un juge des libertés, peut espérer ne pas être suivie dans ses déplacements. La géolocalisation permet de localiser dans l'espace un individu au travers d'un équipement qui lui est associé. Ainsi, l'individu faisant l'objet d'une liberté surveillée est localisé via son bracelet électronique fixé à sa cheville.

La géolocalisation existe dans notre société numérique au travers de nombreux équipements : le système GPS installé dans un véhicule, qui enregistre les déplacements de ce véhicule ; les smartphones qui utilisent plusieurs techniques de géolocalisation pour présenter des services proches du lieu où ils ont localisé leur porteur : restaurants de proximité, artisans, etc.[590], les appareils photo numériques ou les caméscopes qui utilisent le positionnement GPS pour situer le lieu de prise de vue sur une carte, les systèmes GPS autonomes utilisés par les randonneurs pour effectuer une randonnée sans risque de s'égarer[591].

Les smartphones utilisent plusieurs sources d'information pour géolocaliser leur position : le signal GPS provenant des satellites, le signal GSM de la téléphonie mobile provenant des antennes GSM, les identifiants Wi-Fi des bornes d'accès relevés et cartographiés par Google ou d'autres prestataires. Ainsi, même sans signal GPS, le smartphone peut à l'aide d'une base de données des identifiants connaître sa position avec précision pour offrir des services de proximité. Par exemple, l'application Pages Jaunes utilise cette localisation pour présenter des adresses proches du lieu de situation, avec calcul de la distance pour y parvenir.

La Commission de l'informatique et des libertés considère que les données de géolocalisation sont des données à caractère personnel et estime que la géolocalisation de terminaux de communication s'apparente à des interceptions de contenu des communications électroniques[592].

Dans sa décision du 25 mars 2014, le Conseil constitutionnel autorise la géolocalisation d'une personne ou d'un véhicule dans le cadre d'une enquête préliminaire sous le contrôle d'un procureur pour une durée limitée à quinze jours, d'un juge des libertés et de la détention ou

[590] Stéphane Bourliataux- Lajoinie, Arnaud Rivière, « L'enjeu des m-services en marketing touristique territorial : proposition d'un cadre d'analyse », *Recherches en Sciences de Gestion*, 2013/2 (N° 95), pp. 65-82. URL : https://www.cairn.info/revue-recherches-en-sciences-de-gestion-2013-2-page-65.htm consulté le 14 février 2018.
[591] Laëtitia Schweitzer, « Surveillance électronique », *Communications*, 2011/1 (n° 88), pp. 169-176. URL : https://www.cairn.info/revue-communications-2011-1-page-169.htm consulté le 4 avril 2018.
[592] Commission nationale informatique et liberté, Délibération n° 2013-404 du 19 décembre 2013 *portant avis sur un projet de loi relatif à la géolocalisation.*

d'un juge d'instruction[593]. Le Conseil d'État avait déjà validé[594] les dispositions d'une ordonnance de 2010 relative au dopage des sportifs et autorisant la localisation de ces sportifs dans le cadre de la lutte contre le dopage[595].

La géolocalisation peut être autorisée dans le cadre de certaines actions de prévention, limitant ainsi la liberté de déplacement des individus concernés. Ainsi, les outils puissants, mis à disposition des personnes pour les aider dans leurs déplacements, peuvent aussi servir à connaître les déplacements de ces personnes et ainsi contrôler ou surveiller leurs allées et venues. Des dispositifs de surveillance peuvent ainsi être installés dans des véhicules de livraison, pour optimiser les trajets de livraison, mais aussi contrôler ces trajets et les temps impartis à chaque livraison.

Les techniques de géolocalisation sont de plus en plus précises. Si avec l'apparition des premiers GPS, la localisation était réalisée avec une marge d'erreur de plusieurs dizaines de mètres, cette précision était de moins de dix mètres après l'arrêt du brouillage volontaire par l'armée américaine qui contrôlait tous les satellites de positionnement. Avec le nouveau système européen GALILEO en cours de déploiement, la précision de la localisation est inférieure à un mètre, voire quelques centimètres pour le service commercial[596].

La géolocalisation peut être utilisée dans le cadre d'une enquête préliminaire ou d'une enquête judiciaire. En 2013, la Cour de cassation, dans deux arrêts[597] portant sur la géolocalisation dans le cadre d'une procédure pénale, considère que la technique de géolocalisation d'une personne par suivi de son téléphone mobile est une ingérence dans la vie privée et doit être réalisée sous le contrôle d'un juge en conformité avec l'article 8 de la Convention européenne des droits de l'homme. En réaction à ces arrêts, un projet de loi sur la géolocalisation est adopté par le parlement[598]. L'objectif de ce texte est de mettre le droit français en conformité avec la

[593] Conseil constitutionnel, Décision n° 2014-693 DC du 25 mars 2014, *Loi relative à la géolocalisation*.
Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation publiée au journal officiel de la République française n°0075 du 29 mars 2014 p. 6123.
[594] Note sous Conseil d'État du 24 février 2011, n°340122, mentionné aux tables du recueil Lebon.
[595] Ordonnance n° 2010-379 du 14 avril 2010 *relative à la santé des sportifs et à la mise en conformité du code du sport avec les principes du code mondial antidopage* publiée au Journal officiel de la République française du 16 avril 2010 p. 7157.
[596] Nathalie Mayer, « Grâce au GPS, il est possible de se situer où que l'on se trouve sur le globe terrestre, et ce, parfois, avec une précision étonnante, pouvant aller... jusqu'au centimètre ! », *Futura Tech,* URL : https://www.futura-sciences.com/tech/questions-reponses/technologie-precision-gps-6801/ consulté le 5 avril 2018.
[597] Cour de cassation, Chambre criminelle, Audience publique du 22 octobre 2013, N° de pourvoi 13-81.945.
Cour de cassation, Chambre criminelle, Audience publique du 22 octobre 2013, N° de pourvoi 13-81.949
[598] Loi n° 2014-372 du 28 mars 2014 *relative à la géolocalisation,* publiée au JORF n° 0075 du 29 mars 2014 p. 6123.

Convention européenne des droits de l'homme[599] et les décisions précitées de la Cour de cassation. La géolocalisation n'est possible que lorsque les nécessités de l'enquête l'exigent pour des crimes ou des délits punis d'au moins de trois ans d'emprisonnement. Sa durée est limitée dans le temps.

La géolocalisation peut être également utilisée dans le cadre industriel pour suivre une flotte de véhicules, optimiser des tournées de livraison[600]. Pour la Commission de l'informatique et des libertés, cette utilisation doit respecter des règles afin de respecter la vie privée des salariés[601] : les salariés doivent être informés du dispositif, le système doit être justifié par une finalité précise et déclaré à la CNIL. Il ne doit pas être utilisé en dehors du temps de travail ni sur le trajet domicile-trajet de l'employé. Il ne doit pas être utilisé pour contrôler la vitesse du véhicule en temps réel et ne doit pas permettre la géolocalisation des représentants du personnel dans le cadre de leur mandat. En cas de non-respect de ces règles, l'employeur peut être obligé de désinstaller le dispositif sur sa flotte de véhicules[602].

La géolocalisation d'un employé expatrié peut aussi être utilisée pour sa sécurité et pour mesurer son exposition aux risques dans certains pays[603]. Outre la sécurité, les applications disponibles sur smartphone peuvent apporter des aides au déplacement des personnes physiques.

B) Les aides au déplacement apportées aux personnes physiques par les techniques numériques

Les techniques numériques ne permettent pas à un individu de se téléporter à un endroit donné, mais elles lui permettent de préparer son voyage, de le réserver, et durant le voyage de se localiser et repérer dans un site inconnu. Avec le calcul des trajets via le GPS, les techniques numériques sont aussi une aide pour arriver à destination, aide plus fiable et efficace que la

[599] Cour européenne des droits de l'homme, Affaire *Uzun c/ Allemagne*, Requête n° 35623/05, Arrêt du 2 septembre 2010.

[600] Myriam Quéméner, « La géolocalisation : un outil de protection ou de surveillance ? », *Sécurité et stratégie*, 2013/4 (15), pp. 11-17. URL : https://www.cairn.info/revue-securite-et-strategie-2013-4-page-11.htm consulté le 14 février 2018.

[601] Commission nationale de l'informatique et des libertés, « La géolocalisation des véhicules », *Travail & Vie privée*, URL : https://www.cnil.fr/sites/default/files/atoms/files/_travail-vie_privee_geolocalisation_vehicules.pdf consulté le 1er mars 2017.

[602] Cour d'appel de Paris, arrêt du 29 septembre 2016*, Orange / Sud PTT*.

[603] David Amsellem, Kevin Limonier, « L'utilisation des outils cartographiques dans la sûreté des déplacements d'affaires », *Sécurité et stratégie*, 2014/4 (19), pp. 5-12. URL : https://www.cairn.info/revue-securite-et-strategie-2014-4-page-5.htm consulté le 18 décembre 2017.

consultation d'une carte papier encombrante et parfois périmée. Sur place, le voyageur peut payer et acquérir de la monnaie locale via sa carte de crédit dans pratiquement toutes les grandes villes du monde et tous les aéroports internationaux.

1) La liberté de se déplacer dans un environnement numérique

La liberté de se déplacer consiste à pouvoir non seulement se déplacer à travers un pays, un État, mais aussi de pays à pays. Avec l'espace Schengen[604], l'Union européenne a créé un espace de libre circulation pour tous les citoyens européens et non européens entrés dans cet espace territorial, la société numérique aide à la réalisation et à la concrétisation de cet espace de liberté[605]. Le monde numérique facilite cette faculté de se déplacer à travers des sites de commerce en ligne de voyages, mais aussi des sites d'information fournissant toutes les données nécessaires à la préparation du voyage, voir aidant à réaliser certaines démarches. Certains pays, États-Unis d'Amérique, Canada, Australie, ont mis en place un site de demande électronique d'autorisation de voyage[606], remplaçant les visas pour les ressortissants de pays exemptés de visa. La préparation du voyage est une activité de service qui utilise Internet comme moteur de communication. Des sites de prestataires de service existent pour effectuer les demandes de visa vers certains pays en ligne, c'est-à-dire sans avoir à se déplacer vers un consulat[607]. Tous les sites des tour-opérateurs fournissent de tels données ou services ou a minima des liens vers les sites officiels fournissant les informations légales, les démarches à effectuer, voir les restrictions à apporter aux déplacements pour des raisons de sécurité locale. Le ministère des Affaires étrangères gère un tel site[608].

Mais, dans une société marchande virtualisée par le réseau Internet, l'achat d'une prestation liée à un voyage auprès d'une société sur Internet peut poser la question du droit applicable ainsi que celle de l'autorité judiciaire compétente. Ainsi, un couple allemand ayant acheté un séjour en Égypte via le site de lastminute.com souhaitait un dédommagement dû au non-respect

[604] L'espace Schengen, délimité par les pays signataires de la convention Schengen (1990) est un espace de libre circulation des citoyens de l'Union européenne, mais aussi des citoyens étrangers à l'Union européenne, les pays signataires ayant adopté une politique commune concernant les visas et renforcé le contrôle aux frontières de cet espace.

[605] Carine Eff, Isabelle Saint-Saëns, « liberté de circulation vs circulation libérale », *Vacarme*, 2007/4 (n° 41), pp. 84-85. URL : https://www.cairn.info/revue-vacarme-2007-4-page-84.htm consulté le 14 février 2018.

[606] En anglais *Electronic System for Travel Authorization* ou ESTA.

[607] Par exemple le site http://www.visa-en-ligne.com/, consulté le 5 juin 2012.

[608] À l'URL : http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/ consulté le 5 mai 2012.

du niveau des prestations hôtelières sur site. Dans les faits, la prestation était vendue par TUI Osterreich via Lastminute.com. Lastminute.com est une société allemande, donc de même nationalité que celle des acheteurs. TUI est autrichienne. Le problème posé consistait à savoir si le droit allemand seul s'appliquait ou s'il s'agissait d'un conflit international auquel cas la convention Bruxelles 1 était applicable. La Cour de justice de l'Union européenne a considéré qu'il s'agissait d'un conflit international avec application de la convention Bruxelles du 27 septembre 1968[609].

Le monde numérique fournit également une aide pour se rendre d'un endroit du globe à un autre via le GPS et bientôt le Galileo européen. Tout Smartphone fonctionne avec un système GPS, souvent gratuit, et des cartes couvrant quasiment la terre entière. Ce système peut aussi bien être utilisé pour se déplacer, sans erreur de trajet, autour de son domicile que pour effectuer des voyages dans des pays lointains. La précision des cartes disponibles peut varier d'un pays à un autre, mais elle varie aussi avec les cartes classiques sur support papier. Ces itinéraires sont calculés en fonction du moyen de transport utilisé, marche à pied, transport collectif ou individuel. Ils peuvent être utilisés sur un véhicule pour déterminer sa position et appeler des secours en cas d'accident, appel automatique, ou d'incident, appel volontaire[610].

D'autres services peuvent être offerts, ainsi Google Earth et Google Maps permettent de visualiser une localisation donnée sur la mappemonde, et d'effectuer virtuellement le trajet en visionnant les points remarquables.

Une autre aide au déplacement est fournie par les systèmes de paiement électronique. Un voyageur peut à l'aide d'une carte de paiement retirer des devises dans pratiquement tous les pays du monde, et ce dans la devise locale, évitant ainsi le transport important de fonds et améliorant ainsi la sécurité du voyageur. Les transferts de capitaux deviennent instantanés, sans la nécessité de lettres de change ou de chèques de voyage.

Revers de la médaille, ces systèmes GPS ou de paiement par cartes de crédit, enregistrent les déplacements effectués et produisent ainsi un historique qui peut éventuellement être consulté par quelqu'un ayant accès au dispositif[611].

---

[609] Cour de Justice de l'Union européenne, 8e chambre, Arrêt du 14 novembre 2013, Requête no C-478/12 *M. et Mme Maletic c/lastminute.com GmbH et TUI Osterreich.*

[610] À partir du 1er avril 2018, tous les nouveaux modèles de véhicules devront embarquer un système d'appel d'urgence nommé eCall. ECall transmet directement la position géographique, le sens de circulation, ou encore le type de véhicule en difficulté. (Léo Mingot, « eCall : l'appel d'urgence devient obligatoire dans les voitures », 1 avril 2018, *L'Argus.fr,* URL : http://www.largus.fr/actualite-automobile/ecall-lappel-durgence-devient-obligatoire-pour-les-voitures-neuves-9083396.html consulté le 5 avril 2018).

[611] Cf. Partie 1. Titre 2. Chapitre 2. Section 1. L'individu sous surveillance permanente.

2) Les restrictions à la liberté de déplacement facilitées par les échanges numériques des données PNR

Les États ont toujours souhaité contrôler les entrées des personnes physiques sur leur territoire. La délivrance des passeports pour quitter un pays ou la délivrance des visas pour entrer et séjourner dans un pays tiers, sont des moyens de réguler ces flux migratoires. Des accords de réciprocité existent pour faciliter les migrations touristiques sans visa. Mais depuis les attentats du 11 septembre 2001 sur Manhattan, de nouvelles techniques de contrôle de ces flux de personnes physiques ont été rétablies, contrôles utilisant les échanges d'information numérisée[612].

Ce contrôle est réalisé, entre autres, à partir des données d'enregistrement des passagers des compagnies aériennes, mais aussi des réservations dans les hôtels. Le registre des données des passagers (ou en anglais PNR, pour *Passenger Name Record*) contient des données personnelles, recueillies par les agences de voyages ou les transporteurs, concernant tous les détails d'un voyage réalisé ou prévu par des personnes physiques : transports utilisés, horaires, transit et correspondances. L'utilisation des systèmes centraux de réservation est étendue à un grand nombre d'acteurs de l'industrie du voyage ou du tourisme : hôteliers, loueurs de véhicules, transporteurs maritime et terrestre, etc. Ces derniers, comme les compagnies aériennes, écrivent dans le registre des données passager des informations supplémentaires qui peuvent permettre d'établir un profil du passager quant à ses affiliations religieuses[613] : repas casher, halal ou végétarien ; son état de santé : allergies, régimes, handicap ; ses ressources, etc. au travers de ses préférences, de ses demandes particulières ou celles des autres passagers

[612] Didier Bigo, Rob B. J Walker, « 1. Le régime de contre-terrorisme global », dans *Au nom du 11 septembre...Les démocraties à l'épreuve de l'antiterrorisme.* Paris, La Découverte, « Cahiers libres », 2008, pp. 11-35. URL : https://www.cairn.info/au-nom-du--9782707153296-page-11.htm consulté le 14 février 2018.

[613] Concernant l'échange des informations PNR avec les États-Unis, il faut relire l'avant-propos d'Alex Türk, président de la CNIL, dans le 28e rapport d'activité : « *Bourrasque d'abord, qui vint de l'ouest, de la volonté du Gouvernement américain d'imposer un effet extraterritorial à ses lois sécuritaires. Ainsi, en vertu d'un accord conclu entre l'Union européenne et le Gouvernement des États-Unis en juillet 2007, tous les passagers aériens à destination des États-Unis et recourant aux services de compagnies aériennes européennes voient, au nom de la légitime lutte contre le terrorisme, leurs données désormais transférées à plus d'une douzaine d'administrations américaines. Ce transfert des données passagers (dites PNR en anglais) est effectué sans contrôle de la part des Européens, pour une durée de 15 ans, et peut entraîner des refus d'embarquement pour des personnes qui auront bien des difficultés à obtenir des explications et à faire valoir leurs droits. De surcroît, les données transférées peuvent "en cas de nécessité", appréciée souverainement par les autorités américaines, porter sur des informations "sensibles" telles que les préférences alimentaires des personnes, leur état de santé, leurs opinions politiques ou leur origine ethnoraciale. En dépit de l'opposition résolue du Parlement européen et des "CNIL" européennes, ce nouvel accord a été signé. Il a le goût amer de l'échec pour notre modèle qui entend concilier la liberté et la sécurité, sans sacrifier l'une à l'autre* ».

voyageant avec lui et de ses moyens de paiement. En France, la loi du 23 janvier 2006[614] relative à la lutte contre le terrorisme a contraint les compagnies ferroviaires, aériennes, maritimes à transmettre les données du registre des données des passagers à la police et à la gendarmerie, données qui peuvent être comparées avec le fichier des personnes recherchées (FPR) ainsi qu'avec le système d'information Schengen (SIS).

La Directive 2004/82/CE du Conseil du 29 avril 2004[615] concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, adoptée sans l'avis du Parlement européen, qui se fonde sur l'accord de Schengen, règle aussi les échanges de données PNR, dans un but officiel de lutte contre le terrorisme d'une part, et d'autre part contre l'immigration illégale, en autorisant « *l'utilisation de ces données comme élément de preuve dans des procédures visant à l'application des lois et des règlements sur l'entrée et l'immigration, notamment des dispositions relatives à la protection de l'ordre public et de la sécurité nationale »*. Le Parlement européen a adopté le registre des données des passagers[616] le 14 avril 2016[617], mais il a validé en parallèle un texte imposant des conditions strictes pour l'utilisation de ces données à des fins policières ou judiciaires[618]. Le même jour, le Parlement européen a également accepté[619] le règlement 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.

[614] Loi nº 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, publiée au JORF nº20 du 24 janvier 2006 p. 1129.
[615] Directive 2004/82/CE du Conseil du 29 avril 2004 *concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers* publiée au Journal officiel nº L 261 du 06/08/2004 pp. 24 – 27.
[616] 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.*
[617] Parlement européen, *Utilisation des données des passagers (UE-PNR)*, P8_TA (2016) 0127, texte adopté le 14 avril 2016.
[618] Parlement européen, *Traitement des données à caractère personnel à des fins de prévention des infractions pénales,* P8_TA(2016)0126, texte adopté le 14 avril 2016.
[619] Parlement européen, *Protection des personnes physiques à l'égard du traitement des données à caractère personnel,* P8_TA(2016)0125, texte adopté le 14 avril 2016.

Ainsi, le Parlement européen a adopté deux textes importants[620] concernant la protection des données personnelles avant de valider l'utilisation du registre des données passager[621].

Le transfert des données personnelles des passagers en provenance d'Europe est exigé par les États-Unis depuis les attentats du 11 septembre 2001[622]. Le 8 octobre 2006, un accord portant sur le transfert de trente-quatre données personnelles par passager a été conclu entre l'Union européenne et les États-Unis. Cet accord a été renégocié et signé le 18 juillet 2007, suite à une décision d'annulation de l'accord initial par la Cour européenne de justice[623].

Ces échanges de données PNR ont permis à Israël d'interdire l'accès à son territoire de plusieurs ressortissants européens[624]. Ces échanges interétatiques permettent aux États de restreindre la liberté de déplacement en prévenant les compagnies aériennes qu'une personne physique donnée ne pourra pas descendre de l'appareil et devra être reconduite vers une autre destination. Ils posent le problème de la protection des données à caractère personnel. Ainsi, dans un document daté du 26 juillet 2017, sur 73 pages, la Cour de justice de l'Union européenne a formulé un avis négatif sur l'accord de PNR en cours de négociation entre l'Union européenne et le Canada[625]. Cet avis négatif est motivé pour incompatibilité avec la Charte des droits fondamentaux de l'Union européenne (articles 7, 8, 21 et 52 paragraphe 1) « *en tant qu'il n'exclut pas le transfert des données sensibles depuis l'Union européenne vers le Canada ainsi que l'utilisation et la conservation de ces données* », qu'il ne prévoit pas « *que les bases de données utilisées seront limitées à celles exploitées par le Canada en rapport avec la lutte*

[620] 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).*
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.*

[621] 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.*

[622] Valsamis Mitsilegas, « 8. Coopération antiterroriste États-Unis/Union européenne : l'entente cordiale », dans *Au nom du 11 septembre...Les démocraties à l'épreuve de l'antiterrorisme.* Paris, La Découverte, « Cahiers libres », 2008, pp. 118-130. URL : https://www.cairn.info/au-nom-du--9782707153296-page-118.htm consulté le 18 décembre 2017.

[623] Cour de justice, grande chambre, arrêt du 30 mai 2006, *Parlement européen c/ Commission et c. Conseil, affaires jointes C-317/04 et C-318/04*, in Recueil, 2006, p. I- 04721.

[624] « Israël interdit l'accès de son territoire à des centaines de militants pro-Palestiniens », *France 24,* 15 avril 2012, URL : http://www.france24.com/fr/20120415-israel-militants-pro-palestiniens-interdits-entree-cisjordanie-ben-gourion-bienvenue-palestine-tel-aviv consulté le 8 juin 2012.

[625] Cour de justice de l'Union européenne, Avis 1/15 de la Cour (grande chambre) 26 juillet 2017, en ligne à https://cdn2.nextinpact.com/medias/c_1_15.pdf, consulté le 4 aout 2017.

contre le terrorisme et la criminalité transnationale grave », qu'il ne limite pas « *la conservation des données des dossiers passagers après le départ des passagers aériens à celles des passagers à l'égard desquels il existe des éléments objectifs permettant de considérer qu'ils pourraient présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave* », qu'il ne soumet pas « *la communication des données des dossiers passagers par l'autorité canadienne compétente aux autorités publiques d'un pays tiers à la condition qu'il existe soit un accord entre l'Union européenne et ce pays tiers équivalent à l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers* », qu'il ne prévoit pas « *un droit à l'information individuelle des passagers aériens en cas d'utilisation des données des dossiers passagers les concernant pendant leur séjour au Canada et après leur départ de ce pays* » et qu'il ne garantit pas « *que la surveillance des règles prévues par l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, relatives à la protection des passagers aériens à l'égard du traitement des données des dossiers passagers les concernant, est assurée par une autorité de contrôle indépendante* ». Ainsi plutôt que faire reposer son avis sur la directive 95/46/CE obsolète en 2018 ou sur le règlement (UE) 2016/679 applicable en 2018, la Cour a préféré appuyer son avis sur le premier paragraphe du traité de l'Union européenne (traité de Lisbonne) qui reconnaît la valeur juridique de la Charte des droits fondamentaux de l'Union européenne[626]. Cette référence directe à la Charte des droits fondamentaux de l'Union européenne est novatrice, la Cour avait fait reposé l'invalidation de l'accord de Safe Harbor avec les États-Unis d'Amérique[627] sur la directive 95/46/CE alors que la demande de décision préjudicielle portait sur l'interprétation, au regard des articles 7, 8 et 47 de la charte des droits

[626] art. 6 du Traité de l'Union Européenne : « *1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités.*
Les dispositions de la Charte n'étendent en aucune manière les compétences de l'Union telles que définies dans les traités.
« Les droits, les libertés et les principes énoncés dans la Charte sont interprétés conformément aux dispositions générales du titre VII de la Charte régissant l'interprétation et l'application de celle-ci et en prenant dûment en considération les explications visées dans la Charte, qui indiquent les sources de ces dispositions.
« 2. L'Union adhère à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. Cette adhésion ne modifie pas les compétences de l'Union telles qu'elles sont définies dans les traités.
« 3. Les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, font partie du droit de l'Union en tant que principes généraux. »

[627] Cour de justice de l'Union européenne, Arrêt de la Cour (grande chambre) du 6 octobre 2015, Affaire C-362/14, *Maximillian Schrems contre Data Protection Commissioner.*

fondamentaux de l'Union européenne et des articles 25, paragraphe 6, et 28 de la directive 95/46/CE et la validité de la décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46. Il est à remarquer que la Cour ne remet pas en cause le principe de la transmission des données PNR au titre de la restriction de la liberté d'aller et venir, et accepte cette restriction au titre de la lutte contre le terrorisme et la grande criminalité.

Section 2. Les droits économiques dans la société numérique

Sans recourir au déplacement physique, Internet et la dématérialisation de nombreux documents, favorisent la création d'entreprises, que ce soient des entreprises de service traditionnelles, comptabilité, gestion des fournisseurs, ou des entreprises nouvelles, créées et fonctionnant grâce à la numérisation de notre société et à l'existence d'un réseau de communication mondial et quasi instantané[628]. De nombreuses sociétés marchandes sont apparues sur le réseau dominé par une entreprise américaine AMAZON.

Sous-section 1. La liberté de travailler et d'entreprendre dans une société dématérialisée

Les techniques numériques, en dématérialisant les documents et en facilitant les échanges d'information entre terminaux informatiques, permettent partiellement de s'affranchir des distances et favorisent ainsi l'apparition de nouvelles méthodes de travail ou l'émergence de nouveaux services.

§ 1 - Le télétravail dans la société numérique

Le droit au travail est inscrit dans le préambule de la Constitution de 1946, repris par la Constitution de 1958. La société numérique permet de concilier droit au travail et liberté du travail, en offrant la possibilité à un individu de travailler dans un lieu qu'il a choisi indépendamment de la situation géographique réelle des locaux de son employeur[629].

D'après l'article L.1222-9 du Code du travail, le télétravail désigne « *toute forme d'organisation du travail dans laquelle un travail qui aurait pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information et de la communication* ». Le Code du travail s'est ainsi adapté à la possibilité pour un employé de travailler hors des locaux de son employeur

[628] Gilles Paché, « La logistique de distribution du commerce électronique : des défis économiques, managériaux et écologiques à l'horizon », *Gestion*, 2002/5 (Vol. 27), pp. 39-45. URL : https://www.cairn.info/revue-gestion-2002-5-page-39.htm consulté le 20 décembre 2017.

[629] Ollivier Daniel, « Le succès du télétravail. Les effets de la nouvelle loi Travail », *Études*, 2017/12 (Décembre), pp. 33-46. URL : https://www.cairn.info/revue-etudes-2017-12-page-33.htm consulté le 20 décembre 2017.

tout en conservant le lien de dépendance vis-à-vis de cet employeur. Le 16 juillet 2002, un accord-cadre sur le télétravail a été signé au niveau européen par les partenaires sociaux[630]. Cet accord souligne que l'Europe doit encourager le développement du télétravail si elle veut tirer le meilleur parti de la société de l'information, et reconnaît que le télétravail peut répondre aux besoins des entreprises et des travailleurs. Cet accord a été suivi en France, par un accord interprofessionnel du 19 juillet 2005 sur le télétravail, accord étendu par un arrêté publié le 30 mai 2006[631]. Dans son préambule, cet accord considère que le télétravail constitue un moyen pour les salariés de concilier vie professionnelle et vie sociale[632]. Le télétravail doit être choisi par l'employé et ne peut pas être imposé par l'employeur qui ne peut utiliser les moyens mis à disposition pour le télétravail pour interférer avec la vie privée de l'employé. L'employeur et l'employé doivent fixer, par concertation, les plages horaires où l'employeur peut contacter l'employé. Si un moyen de surveillance est mis en place, il doit être proportionné et l'employé doit en être averti[633]. De plus, depuis la promulgation des ordonnances modifiant le droit du travail, l'employeur qui refuse à un employé le bénéfice du télétravail alors que l'employé occupe un poste éligible doit motiver son refus[634]. L'accident survenu sur le lieu de télétravail aux horaires déterminés pour ce télétravail est présumé être un accident du travail. Le télétravailleur bénéficie des mêmes droits d'information et de protection que le travailleur sur site de l'entreprise.

Si la société numérique permet le développement du télétravail, elle facilite aussi la création de micro-entreprise, entreprise unipersonnelle, pour tenter de développer une nouvelle activité sans risques majeurs ou de développer une entreprise existante en s'affranchissant des frontières terrestres.

---

[630] Accord - cadre européen sur le télétravail signé le 16 juillet 2002 par les partenaires sociaux (CES, l'UNICE/UEAPME et le CEEP) disponible à http://yves.lasfargue.pagesperso-orange.fr/documenttelecharges/accordcommente160802.pdf consulté le 2 mars 2017.

[631] *Arrêté du 30 mai 2006 portant extension de l'accord national interprofessionnel relatif au télétravail* publié au Journal officiel de la République française n°132 du 9 juin 2006 p. 8771.

[632] Simon Nadel, « La Responsabilité sociale de l'entreprise comme forme de justification : quels impacts sur le travail ? », *Revue Française de Socio-Économie*, 2013/1 (n° 11), pp. 165-179. URL : https://www.cairn.info/revue-francaise-de-socio-economie-2013-1-page-165.htm consulté le 20 décembre 2017.

[633] Monique Pontier, « Télétravail indépendant ou télétravail salarié : quelles modalités de contrôle et quel degré d'autonomie », *La Revue des Sciences de Gestion*, 2014/1 (n° 265), pp. 31-39. URL : https://www.cairn.info/revue-des-sciences-de-gestion-2014-1-page-31.htm consulté le 14 février 2018.

[634] Ordonnance n° 2017-1 387 du 22 septembre 2017 *relative à la prévisibilité et la sécurisation des relations de travail,* publiée au JORF n° 0223 du 23 septembre 2017, article 21.

§ 2 - La liberté d'entreprendre et d'établissement dans une société numérique

La création d'une entreprise de service ou de négoce est facilitée par les techniques numériques qui permettent à l'offreur et au demandeur de se rencontrer. Créer une entreprise de e-commerce ne nécessite pas d'avoir un local et un bail commercial. De nombreuses start-up de services spécialisés commencent à exister avec un ou deux employés connectés sur Internet. Xavier Niel a créé avec la Station F[635] une pépinière de start-up et leur offre des services mutualisés. La location est facturée au poste de travail.

La société numérique permet aux principes de l'Union européenne concernant la liberté d'entreprendre et la liberté d'établissement de s'épanouir.

A) La liberté d'entreprendre dans l'Union européenne et la localisation virtuelle d'une société commerciale ou de service dans une société numérique

L'Union européenne a institué la liberté d'établissement et de prestation de service, c'est-à-dire que le traité CE[636] pose le principe de la libération de l'activité non salariée sous ses deux formes : la personne ou l'entreprise peut, soit s'établir dans un autre État membre [liberté d'établissement[637]], soit offrir ses services par-delà les frontières dans d'autres États membres tout en restant établie dans son pays d'origine [liberté de prestation de services[638]]. Dès l'entrée en vigueur du traité, toute nouvelle mesure restrictive en la matière a été interdite et les restrictions existantes devaient être supprimées avant la fin de la période de transition sous forme de directives du Conseil selon un programme général progressif.

Deux programmes généraux, adoptés le 18 décembre 1961, prévoyaient les directives nécessaires à la suppression des restrictions à la liberté d'établissement et de prestation de services pour les différentes activités[639]. Bien que le Conseil en ait adopté un bon nombre, le

[635] Une description de la Station F et des services offerts est disponible à l'URL : https://stationf.co/ consultée le 5 avril 2018..

[636] *Traité instituant la Communauté européenne ou Traité de Rome* du 25 mars 1957, devenu le traité sur le fonctionnement de l'Union européenne selon le « traité modificatif » signé le 13 décembre 2007 à Lisbonne, dit traité de Lisbonne.

[637] Repris dans les articles 49 à 55 du Traité sur le fonctionnement de l'Union européenne.

[638] Repris dans les articles 56 à 62 du Traité sur le fonctionnement de l'Union européenne.

[639] Christian Gavalda, Gilbert Parleani, *Droit des affaires de l'Union européenne,* 6e édition, 2010, LexisNexis, pp.177-180.

travail était loin d'être achevé en 1974, lorsque la Cour de justice a décidé qu'en dépit de cette carence, les deux libertés avaient, aux termes mêmes du traité, un effet direct dès la fin de la période de transition, soit à partir du 1er janvier 1970 : ce sont les arrêts Reyners[640] pour la liberté d'établissement et Van Binsbergen[641] pour la libre prestation de services. La poursuite du travail de suppression des restrictions est donc devenue inutile et les directives en suspens ont été retirées[642].

Mais plus que par ces libertés instaurées par le traité instituant la Communauté européenne, la libre prestation de service est facilitée par Internet. En effet, à partir d'un site établi dans n'importe quel État membre de la Communauté européenne, toute entreprise peut proposer ses services dans les autres États membres, sans avoir la nécessité d'installer une représentation dans cet État. La démarche commerciale est assurée par Internet, la conclusion du contrat de service peut l'être également et la prestation assurée soit de façon dématérialisée sans nécessité de se déplacer dans l'État du client, soit de façon matérielle par détachement du personnel qui peut venir temporairement dans l'État membre y réaliser cette prestation, sans nécessité d'y avoir établi une représentation locale[643]. Le détachement de travailleurs dans l'Union européenne est permis et la protection des travailleurs garantie[644].

B) La liberté d'établissement numérisé

Dans l'espace économique de l'Union européenne, Internet et les libertés de circulation des marchandises, des capitaux et la liberté de prestation s'allient pour faciliter la création des entreprises de prestations de service ou commerciales.

---

[640] Cour de justice de la Communauté européenne, affaire 2/74, *Reyner contre État belge,* arrêt du 21 juin 1974

[641] Cour de justice de la Communauté européenne, affaire 33/74*, Johannes Henricus Maria van Binsbergen contre Bestuur van de Bedrijfsvereniging voor de Metaalnijverheid,* arrêt du 3 décembre 1974.

[642] Lire Commission européenne, *Guide de la Jurisprudence de la Cour de justice de l'UE relative aux Articles 56 s. du Traité FUE : La libre prestation de services* en ligne à l'URL : https://ec.europa.eu/docsroom/documents/16743/attachments/1/translations/fr/renditions/native , et *Guide de la Jurisprudene de la Cour de justice de l'UE relative aux articles 49 s. du Traité FUE : La liberté d'établissement* URL : https://ec.europa.eu/docsroom/documents/22543/attachments/1/translations/fr/renditions/native, consultés le 20 décembre 2017.

[643] Marc Morsa, « Le travail détaché dans l'Union européenne : enjeux juridiques et économiques », *Informations sociales*, 2016/3 (n° 194), pp. 82-94. URL : https://www.cairn.info/revue-informations-sociales-2016-3-page-82.htm consulté le 15 mars 2018.

[644] Directive 96/71/CE du parlement européen et du conseil du 16 décembre 1996 *concernant le détachement de travailleurs effectué dans le cadre d'une prestation de services* parue au Journal officiel nº L 018 du 21/01/1997 pp. 1-6.

1) L'éclosion de sociétés commerciales ou de services nouvelles

Les techniques numériques permettent la création d'une société de vente par correspondance ou de e-commerce sans nécessiter de disposer de fonds importants pour cette création. Un serveur et une adresse Internet suffisent. Certains sites se sont spécialisés dans cette fourniture. Par exemple, le site 1and1.fr propose une solution de e-commerce à partir de 19,99 euros par mois pour 1 000 articles, sans engagement de durée. De telles offres facilitent la création de microentreprises, sans mise de fonds initiale importante, mais aussi parfois, sans préparation[645]. D'autres prestataires, tel eBay, permettent à un particulier de mettre en vente un bien sans nécessité de création d'un site marchand personnel.

Le portail Proxima mobile[646] permet la diffusion d'applications développées pour des smartphones (iPhone ou Android principalement), après labélisation de ces applications qui doivent être diffusées gratuitement. La rémunération des développeurs étant alors assurée par les fournisseurs d'information ou des annonces publicitaires. De jeunes sociétés peuvent se développer via ce canal, en proposant des services accessibles à partir des terminaux mobiles que deviennent les téléphones.

Cette liberté a été facilitée par l'attribution de noms de domaines à des personnes physiques, l'attribution d'un nom de domaine en .fr est ainsi possible pour toute personne domiciliée en France, sans contrainte de nationalité, ou toute personne de nationalité française résidant à l'étranger[647]. Le Conseil constitutionnel a considéré que l'attribution d'un nom de domaine contribuait à la liberté d'entreprendre[648].

La technique numérique a permis l'éclosion de sociétés de services, véritables intermédiaires entre l'utilisateur final et le fournisseur[649]. Des sites de comparaison de prix que ce soit pour la vente électronique ou les services se développent. Lors de la recherche d'un produit sur Internet, les moteurs de recherche fournissent des adresses de sites de comparaison généralistes tels

---

645 « Le guide de l'e-commerce pour les débutants », *La Fabrique du Net,* URL : https://www.lafabriquedunet.fr/creation-site-ecommerce/ consulté le 5 avril 2018.

646 À l'URL http://www.proximamobile.fr/, consulté le 2 mars 2017.

647 AFNIC, *Charte de nommage du .fr, Règles d'attribution et de gestion des noms de domaine en .fr*, Article 6. Éligibilité du titulaire d'un nom de domaine, p. 9.

648 Conseil constitutionnel, Décision nº 2010-45 QPC du 06 octobre 2010, *M. Mathieu P. [Noms de domaine Internet* Journal officiel du 7 octobre 2010, p. 18156. Commentaire Frédéric Sardain, « Séisme pour le régime juridique des noms de domaine français », *Communication commerce électronique*, n° 1, janvier 2011, pp. 11-14.

649 Broussolle Damien, « Le commerce des services, un commerce en trompe-l'œil ? Une analyse fondée sur le point de vue de Hill », *Revue économique*, 2012/6 (Vol. 63), pp. 1145-1177. URL : https://www.cairn.info/revue-economique-2012-6-page-1145.htm consulté le 20 décembre 2017.

Kelkoo[650], Google products ou shopping[651], ou spécialisés comme clubic.com[652]. Mais aussi des sites proposant de fournir plusieurs devis pour des travaux, 123devis.com[653] ou e-travaux.com[654]. Après un développement anarchique[655], la loi pour une République numérique[656] tente de mettre un peu d'ordre et de rigueur autour de ces sites en créant la notion de « *loyauté des plateformes et information des consommateurs* » ajoutée au Code de la consommation. Tout opérateur de plateforme en ligne dont l'activité consiste en la fourniture d'informations permettant la comparaison des prix et des caractéristiques de biens et de services proposés par des professionnels, doit communiquer aux consommateurs les informations portant sur les éléments de cette comparaison et ce qui relève de la publicité[657].

Le commerce électronique connaît un engouement certain, il permet de consulter des catalogues et de commander aux meilleurs prix sans avoir à se déplacer. Il permet également à tout particulier de mettre en vente, sans avoir de site marchand propre à travers des sites comme eBay[658]. De tels sites permettent à une personne privée, non commerçante de mettre à disposition à la vente un ou plusieurs objets, parfois contrefaits. La France a protégé et favorisé le développement du commerce électronique dès 2004 avec la loi pour la confiance dans l'économie numérique[659] et son titre II intitulé « du commerce électronique ». Cette protection n'est pas parfaite, en cas de contrefaçon, seuls les ayant-droit peuvent obtenir la destruction des objets contrefaits, l'acheteur potentiel n'a quant-à-lui peu de recours envers un site souvent domicilié hors de l'Union européenne. Comme l'écrit André Le Roux, « *Pour le droit, l'acheteur d'une copie servile induit en erreur par la ressemblance est tout aussi répréhensible que le possesseur d'une imitation achetée délibérément* »[660].

---

650 http://www.kelkoo.fr consulté le 12 mai 2012.
651 http://www.google.fr/shopping?hl=fr&tab=wf consulté le 12 mai 2012.
652 http://www.clubic.com/ consulté le 12 mai 2012.
653 http://www.123devis.com/?gclid=CNiauMWx-q8CFUUhtAodpEjvGg consulté le 12 mai 2012.
654 http://www.e-travaux.com/?FROM=42&gclid=CMSustyx-q8CFcwNtAodx2nPEQ consulté le 12 mai 2012.
655 Sébastien Soriano, « Quelle régulation pour les plateformes ? », *Annales des Mines - Réalités industrielles*, 2016/3 (Août 2016), pp. 47-50. URL : https://www.cairn.info/revue-realites-industrielles-2016-3-page-47.htm consulté le 20 décembre 2017.
656 Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF nº 0235 du 8 octobre 2016.
657 Ronan Hardouin, « Plateformes 2.0 : de la notion de passivité à celle de loyauté ? », *I2D – Information, données & documents,* 2015/1 (Volume 52), pp. 27-27. URL : https://www.cairn.info/revue-i2d-information-donnees-et-documents-2015-1-page-27.htm consulté le 5 avril 2018.
658 http://www.ebay.fr/ consulté le 12 mai 2012.
659 Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* publiée au JORF nº0143 du 22 juin 2004 p. 11168.
660 André Le Roux, Marinette Thébault, François Bobrie, « Les consommateurs de contrefaçon : le prix n'est pas la seule motivation », *Recherches en Sciences de Gestion*, 2015/2 (N° 107), pp. 25-41. URL :

2) Les nouvelles offres de service

Le développement d'applications nouvelles, liées à Internet et aux moyens mis en œuvre, a fait apparaître de nouveaux métiers. De nouveaux sites mettent en relation des particuliers ou des professionnels proposant des services et des particuliers souhaitant disposer de tels services. Ce peut être pour la location d'appartements ou de chambres meublés[661], pour du covoiturage[662], pour réserver un véhicule de tourisme avec chauffeur[663]. Tous ces services entrent en concurrence avec des professions existantes : hôtelier, taxi, etc. En effet, dans une ville touristique, tout particulier disposant d'une chambre meublée peut, par l'intermédiaire d'un tel site proposer des locations à la nuit qui échappent aux taxes dont les hôtels sont soumis, taxes de séjour et TVA, et même contourner la loi sur les restrictions légales liées à la location de meublés. La particularité de ces nouveaux services, tout comme la mise en vente sur Internet de biens personnels, est que ces services échappent à tout contrôle légal et à la taxation supportée par les professionnels qu'ils concurrencent, et ceci en contradiction avec le principe de l'égalité devant la loi et l'impôt[664]. De plus, certains services proposés sur Internet utilisent des failles légales dues à la difficulté de légiférer rapidement face aux nouveaux entrepreneurs de l'Internet.

Airbnb, un site de location d'appartements ou de maisons, propose la mise en relation de propriétaires, ou locataires, avec des touristes ou des employés en déplacement pour une location temporaire en meublé[665]. Ce site, d'origine américaine, contourne la législation française concernant la location d'une résidence principale, limitée à quatre mois par an, la sous-location d'un appartement qui doit avoir l'aval du propriétaire, ou la législation restrictive sur les meublés. Pour éviter cet écueil, Airbnb passe des accords avec certaines collectivités locales pour collecter et reverser à ces collectivités les taxes de séjour ainsi collectées[666].

---

https://www.cairn.info/revue-recherches-en-sciences-de-gestion-2015-2-page-25.htm consulté le 20 décembre 2017.

[661] https://www.airbnb.fr/ .

[662] https://www.blablacar.fr/ .

[663] https://www.uber.com/fr/ .

[664] Maxime Lambrecht, « L'économie des plateformes collaboratives », *Courrier hebdomadaire du CRISP*, 2016/26 (n° 2311-2312), pp. 5-80. URL : https://www.cairn.info/revue-courrier-hebdomadaire-du-crisp-2016-26-page-5.htm consulté le 5 avril 2018.

[665] Nicolas Ferrary, « Les nouvelles formes de tourisme collaboratif : une demande en pleine expansion », *Annales des Mines - Réalités industrielles*, 2015/3 (Août 2015), pp. 50-53. URL : https://www.cairn.info/revue-realites-industrielles-2015-3-page-50.htm consulté le 5 avril 2018.

[666] Depuis le premier octobre 2015, après un accord avec la mairie de Paris, le site Airbnb a commencé à collecter la taxe de séjour relative à ces locations, soit selon les estimations de la mairie de Paris environ 5 millions d'euros par an. Cité par Guy Dutheil, *Airbnb : Paris veut éviter le syndrome de « Barceloneta »,* publié le 1 octobre 2015

Concernant les critiques liées au contournement des restrictions de nombre de nuitées et ayant été condamné à payer des amendes à Amsterdam et Barcelone, Airbnb a proposé de limiter le nombre de nuitées par an et par loueur à Paris, sauf en cas de loueurs professionnels. Mais en parallèle, Airbnb propose une carte de retrait domiciliée à Gibraltar qui permettrait à ses possesseurs de pouvoir sortir de leur fiscalité les revenus transitant par ce compte spécial[667].

Si le cas de Airbnb peut être régularisé, d'autres prestataires ont créé de nouvelles formes de travail posant quelques difficultés réglementaires. Uber gère des véhicules de transport avec chauffeurs qui ne sont pas des salariés d'Uber, mais qui sont formés succinctement par Uber. La réservation des véhicules est assurée via une application spécifique fonctionnant sur smartphone. Ainsi, Uber qui met en relation des conducteurs de véhicules de tourisme et des clients, recrute des chauffeurs qui sont des entrepreneurs indépendants et qui doivent investir dans leur véhicule. Ces « entrepreneurs » sont rémunérés à la course par Uber qui perçoit et fixe le coût de cette course et leur ristourne une partie des sommes collectées. Uber perçoit ainsi 25 % du prix de la course pour une mise en relation, le chauffeur-entrepreneur doit investir dans un véhicule et payer les charges dues par toute entreprise en fonction de son statut. Les chauffeurs restent dépendant de la plateforme gérée par Uber pour la mise en relation avec les clients. Le modèle de fonctionnement Uber a donné naissance à la notion d'« uberisation » d'une profession[668]. Une société développe une plateforme de mise en relation entre un professionnel et un client, elle fixe le coût de la prestation, se rémunère sur ce coût et verse le reliquat au professionnel qui n'a qu'un lien contractuel avec la société et n'est pas considéré comme un salarié de cette société. Ces pratiques se sont développées en utilisant les failles des réglementations[669], d'abord aux États-Unis d'Amérique, pays de la libre-entreprise, puis s'est généralisé au reste du monde grâce au réseau Internet et à la puissance des télécommunications.

http://www.lemonde.fr/economie/article/2015/10/01/pour-airbnb-paris-vaut-bien-une-taxe_4779202_3234.html consulté le 5 octobre 2015.

667 Les Echos, « Chez Airbnb, une carte de crédit permettrait d'échapper au fisc », *Les Echos.fr*, 1 décembre 2017, en ligne à https://www.lesechos.fr/industrie-services/immobilier-btp/030967160373-chez-airbnb-une-carte-de-credit-permettrait-dechapper-au-fisc-2135028.php consulté le 20 décembre 2017.

668 Ariel Kyrou, « L'*ubérisation* est un populisme », *Multitudes*, 2015/4 (n° 61), pp. 106-113. URL : https://www.cairn.info/revue-multitudes-2015-4-page-106.htm consulté le 5 avril 2018.

669 Cédric Diridollou, Thierry Delecolle, Leïla Loussaïef *et al.*, « Légitimité des business models disruptifs : le cas Uber », *La Revue des Sciences de Gestion*, 2016/5 (N° 281-282), pp. 11-21. URL : https://www.cairn.info/revue-des-sciences-de-gestion-2016-5-page-11.htm .

En Californie, un juge de San Francisco a validé la possibilité d'un recours en nom collectif de conducteurs Uber afin de se faire reconnaître comme salariés de l'entreprise, ce qui remettrait en cause le modèle économique de l'entreprise[670].

En juillet 2015, l'application UberPop a été interdite en France[671] après avoir fait l'objet d'une question prioritaire de constitutionnalité[672]. Elle avait déjà fait l'objet d'interdictions par plusieurs gouvernements européens, la Belgique, l'Allemagne et l'Espagne[673]. Cette application permettait de mettre en relation un conducteur non professionnel et un particulier, elle ne concernait pas un service de VTC[674]. Le conducteur non professionnel, simplement inscrit auprès d'Uber, utilisait son véhicule personnel et grâce à une application sur smartphone devenait un pseudo-chauffeur de taxi. Cette application fonctionnait sur la base du covoiturage, elle a été déclarée illégale, car elle ne pouvait pas être justifiée par du covoiturage : le conducteur ne partageait pas son véhicule pour un trajet commun avec le particulier, il était défrayé de la course sans que ce soit un partage des frais. Ce service avant d'être arrêté a revendiqué quelque 300 000 utilisateurs en France[675], montrant ainsi la difficulté de légiférer rapidement face à l'apparition de nouveaux services utilisant des failles de la législation existante.

Ces nouveaux établissements peuvent interférer avec l'économie classique, non numérique, et créer une concurrence déloyale qui n'utilise ou n'est pas soumise aux mêmes règles de par leur nouveauté et une législation passive ou mal adaptée à cette nouvelle économie. Des protections sont toutefois mises en place, avec une efficacité limitée.

---

[670] *Californie : recours autorisé pour des chauffeurs Uber réclamant un statut de salarié*, publié le 02/09/2015 in http://lexpansion.lexpress.fr/high-tech/californie-recours-autorise-pour-des-des-chauffeurs-uber-reclamant-un-statut-de-salarie_1711685.html, consulté le 5 octobre 2015.

[671] Philippe Delebecque, « L'illégalité du service UberPop confirmée par le Conseil constitutionnel », *Energie - environnement - infrastructures : actualité, pratiques et enjeux*, octobre 2015, n° 10, pp. 72-73.

[672] Conseil constitutionnel, Décision n° 2015-484 QPC du 22 septembre 2015 *Société UBER France SAS et autre (II) [Incrimination de la mise en relation de clients avec des conducteurs non professionnels]*.

[673] Daniel Vigneron, « En Europe, Uber a perdu des batailles, pas la guerre », », *myeurop.info*, 2 février 2016, URL : http://fr.myeurop.info/2016/02/02/en-europe-uber-a-perdu-des-batailles-pas-la-guerre-14476 consulté le 15 mars 2018.

[674] Le Figaro.fr, AFP agence, « Uber et UberPop : c'est quoi la différence ? », *Le figaro.fr*, publié le 3 juillet 2015 et mis à jour le 4 mai 2016 à http://www.lefigaro.fr/secteur/high-tech/2015/07/03/32001-20150703ARTFIG00177-uber-et-uberpop-c-est-quoi-la-difference.php, consulté le 2 mars 2017.

[675] France 3, « UberPop : 1 500 conducteurs et 300 000 utilisateurs », *Franceinfo,* 25 juin 2015, URL : https://www.francetvinfo.fr/economie/entreprises/uberpop-1-500-conducteurs-et-300-000-utilisateurs_969017.html consulté le 15 mars 2018.

3) Les limites liées à la protection industrielle et à la protection du consommateur

Si la concurrence induite par l'utilisation des nouvelles techniques est mal prise en compte par la législation ou les règlements, la contrefaçon et la protection du consommateur restent protégées et ne doivent pas être restreintes par cette création facile de sites commerçant. La contrefaçon est relativement protégée, mais le consommateur l'est peu face à un vendeur non professionnel.

a) La contrefaçon favorisée par l'e-commerce

Le droit des marques est l'objet de nombreux procès concernant Internet[676]. Il peut s'agir de noms de domaine prêtant à confusion ou de diffusion de contrefaçons ou de copies d'œuvres illégales. Des sites naissent sur la toile pour vendre un stock de produits contrefaits et disparaissent une fois le stock écoulé. Le consommateur en a connaissance via les sites de référencement et les comparateurs de prix. Abusé par les prix pratiqués, le consommateur n'a aucun moyen de recours contre ces « sites champignon ». En 2016, les douanes françaises ont saisi 9,2 millions de contrefaçons, et 8,4 millions en 2017[677]. Le consommateur peut également mettre sa santé en danger en achetant sur internet des médicaments contrefaits[678]. Une cellule « Cyberdouane » a été créée en 2009 pour lutter contre la contrefaçon, l'importation illégale d'armes et de médicaments[679]. Lors de sa création, cette cellule « Cyberdouane » était constituée de huit analystes et de sept personnels des services d'enquêtes de la DNRED[680], mobilisables en permanence[681].

---

[676] Éric Barbry, « Le droit des marques à l'épreuve de l'Internet », *LEGICOM*, 1997/3 (N° 15), pp. 91-109. URL : https://www.cairn.info/revue-legicom-1997-3-page-91.htm consulté le 5 avril 2018.

[677] Douanes et Droits indirects, *Agir pour protéger, Résultats 2017,* Ministère de l'action et des comptes publics, 13 mars 2018, URL : http://www.douane.gouv.fr/Portals/0/fichiers/information/publication-douane/bilans-resultats/resultats-2017.pdf consulté le 15 mars 2018.

[678] Entre le 12 et le 19 septembre 2017, l'opération PANGEA X a permis la saisie de plus de 433 000 produits de santé illicites et de 1,4 tonne de produits de santé en vrac. Au cours de l'opération 185 sites internet illégaux de vente de faux médicaments ont été identifiés. (Source Douanes et Droits indirects, « Résultats français de l'opération PANGEA X », 26 septembre 2017, URL : http://www.douane.gouv.fr/articles/a14472-resultats-francais-de-l-operation-pangea-x consulté le 15 mars 2018).

[679] Le Portail du gouvernement, *Cyberdouane, un nouveau service pour lutter contre la cyberdélinquance*, du 10 février 2009, URL : http://archives.gouvernement.fr/fillon_version2/gouvernement/cyberdouane-un-nouveau-service-pour-lutter-contre-la-cyberdelinquance.html consulté le 16 mars 2018.

[680] Direction nationale des recherches et enquêtes douanières.

[681] Direction générale des Douanes et Droits Indirects, « Cyberdouane », URL : https://www.economie.gouv.fr/files/cyberdouane.pdf consulté le 16 mars 2018.

Les particuliers peuvent écouler des marchandises via des sites de e-commerce. Des sanctions administratives et pénales existent contre les vendeurs qui diffusent des produits contrefaits par le biais de ces sites de e-commerce[682]. PriceMinister et 2xmoinscher.com ont signé une charte contre la contrefaçon sur Internet en décembre 2009[683], cette charte prévoit une « riposte graduée » contre les e-vendeurs écoulant des produits contrefaits : de 6 mois d'exclusion de la plateforme de vente en ligne à 5 ans en cas de récidive. Mais la principale plateforme de e-commerce de particulier à particulier eBay n'a pas signé cette charte. Deux nouvelles chartes ont été signées en février 2012 entre les ayants droit et les opérateurs de commerce en ligne ou de petites annonces.

Des sanctions pénales existent[684], les peines encourues sont sévères, mais peu appliquées. Les sites de e-commerce situés hors de l'Union européenne se trouvent *de facto* hors d'atteinte de cette protection, seules les marchandises saisies peuvent être détruites.

b) La protection du consommateur dans l'e-commerce

Le consommateur ne peut pas entamer de poursuites pour contrefaçon, celles-ci étant exclusivement réservées aux ayants droit[685].

Le code de la consommation protège le consommateur en instituant un délai de rétractation de 7 jours, qui a été porté à 14 jours par la réglementation européenne[686], pour toute vente en ligne. De plus, le remboursement doit être effectif dans le délai de 14 jours, ce remboursement doit être total et intégrer les frais de livraison[687]. Mais, le code de la consommation ne s'applique qu'entre un consommateur et un professionnel, même si l'opérateur de plateforme doit rappeler les droits et obligations des parties lises en relation[688]. Le consommateur n'est pas protégé lors d'une vente sur Internet avec un non-professionnel, les plateformes d'e-commerce ne sont que des intermédiaires non responsables des échanges réalisés via leur site. Les ventes sur Internet restent un moyen d'écouler des biens contrefaits sans encourir de sanctions significatives, de

[682] Code de la propriété intellectuelle, art. L.716-9, L.716-10, L.613-3 ; Code des douanes, art. 414.
[683] Charte disponible à l'adresse http://www.minefe.gouv.fr/actus/pdf/091216charteInternet.pdf .
[684] Loi n° 2007-1544 du 29 octobre 2007 *de lutte contre la contrefaçon*, parue au JORF n° 252 du 30 octobre 2007 p. 17775, dite loi Châtel, prévoit une peine de trois ans d'emprisonnement et de 300 000 € d'amende portée à cinq ans d'emprisonnement et à 500 000 € d'amende en cas de délit commis en bande organisée (Art. L.521-10 du Code de la propriété industrielle).
[685] Posséder un article provenant d'une contrefaçon est un délit de recel (Code pénal, Art. 321-1 al. 1).
[686] Transposée en France par la loi n° 2014-344 du 17 mars 2014 *relative à la consommation*, dite « loi Hamon ».
[687] Modifications apportées par la loi Hamon au Code de la consommation.
[688] Code de la consommation, art. L.111-7.

plus, de nombreux sites contrefacteurs sont implantés en Asie du Sud-Ouest. La facilité de création d'un site de e-commerce peut réduire la liberté d'entreprendre en créant ainsi une concurrence déloyale favorisant la contrefaçon.

Sous-section 2. La protection spécifique de la liberté de création

Les droits d'auteur ont été instaurés par deux décrets-lois révolutionnaires de 1791 et 1793 pour protéger la création des écrivains et des artistes. Le plagiat ou la copie illicite d'une œuvre devient un délit. Le code de la propriété intellectuelle a depuis la Révolution connu de nombreux aménagements. En 1996, un traité international a été adopté[689] face à « l'évolution et la convergence des techniques de l'information et de la communication » quant à leur « incidence considérable sur la création et l'utilisation des œuvres littéraires et artistiques ». L'Union européenne a adopté une directive pour harmoniser cette protection[690] en 2001. Avec les techniques numériques, la dématérialisation des œuvres artistiques a entraîné de nouveaux modes de copie et de diffusion des œuvres, copier une œuvre consiste à copier un fichier. La copie illicite est devenue phénomène de société[691]. En France, plusieurs lois ont tenté de limiter ce phénomène de copie illicite : lois HADOPI 1 et HADOPI 2[692], elles-mêmes précédées d'une loi DADVSI[693].

§ 1 - La protection physique des supports numériques

Les œuvres artistiques non numérisées peuvent être simplement reproduites : un livre ou une revue peut être photocopié et transformé en fichier, une œuvre musicale enregistrée sur disque vinyle ou diffusée par la radio peut être recopiée sur une bande magnétique à l'aide d'un

[689] Traité de l'OMPI sur le droit d'auteur (adopté á Genève le 20 décembre 1996).
[690] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 *sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information* publiée au Journal officiel n° L 167 du 22/06/2001 pp. 10-19.
[691] Antoine Gitton, « La copie privée numérique : vers une licence d'édition privée », *LEGICOM*, 2001/2 (n° 25), pp. 61-74. URL : https://www.cairn.info/revue-legicom-2001-2-page-61.htm consulté le 20 décembre 2017.
[692] Loi nº 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur Internet,* publiée au JORF nº 135 du 13 juin 2009 p. 9666.
Loi nº 2009-1 311 du 28 octobre 2009 *relative à la protection pénale de la propriété littéraire et artistique sur Internet* publiée au JORF nº0251 du 29 octobre 2009 p. 18290.
[693] Loi nº 2006-961 du 1 août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information* publiée au JORF nº 178 du 3 août 2006 p. 11529.

magnétophone, un film diffusé par la télévision peut être enregistré en utilisant un magnétoscope. Ces copies nécessitent un transfert de support et du matériel d'enregistrement. Avec l'apparition du Compact Disc, ou CD, les œuvres numérisées étaient réputées inviolables et non reproductibles, jusqu'à l'apparition de supports réinscriptibles et la généralisation des graveurs de CD sur les PC.

Un dispositif particulier est alors mis en place par SONY puis par d'autres producteurs de CD : le DRM ou *digital rights management*[694]. Ce dispositif offre plusieurs moyens de lutter contre les copies illicites : restreindre la lecture à certaines zones géographiques, restriction utilisée pour la diffusion des films sous forme de DVD, pour *digital versatile disc* ; empêcher la copie de l'œuvre sur un autre support, même identique[695]. Ces dispositifs qui pouvaient empêcher la copie privée prévue en France[696] ont fait l'objet d'actions en justice[697], mais ont été contournés par l'apparition sur le marché de logiciels permettant la reproduction de ces œuvres protégées. Concernant l'empêchement de réaliser une copie à usage privé, le tribunal de grande instance de Paris déboute en 2004, l'UFC Que Choisir et M. Perquin[698] de leur action contre les sociétés Alain Sarde, Studio Canal et Universal Pictures Video France qui diffusent sur DVD le film « Mulholland Drive », exposant que la copie privée est une exception qui doit céder devant l'atteinte à l'exploitation de l'œuvre interprétée en tenant compte de l'incidence économique que peut avoir une telle copie. La Cour d'appel donne raison au plaignant le 23 avril 2005 et fait interdiction à l'éditeur et au producteur d'apposer un dispositif anticopie sur le DVD, appel cassé par la Cour de cassation[699] qui statue en ces termes : « *l'atteinte à l'exploitation normale de l'œuvre, propre à faire écarter l'exception de copie privée s'apprécie au regard des risques inhérents au nouvel environnement numérique quant à la sauvegarde des droits d'auteur et de*

[694] Séverine Dusollier, « Les mesures techniques dans la directive sur le droit d'auteur dans la société de l'information : un délicat compromis », *LEGICOM*, 2001/2 (N° 25), pp. 75-86. URL : https://www.cairn.info/revue-legicom-2001-2-page-75.htm consulté le 20 décembre 2017.

[695] Marc Bourreau, Michel Gensollen, « L'impact d'Internet et des Technologies de l'Information et de la Communication sur l'industrie de la musique enregistrée », *Revue d'économie industrielle* [En ligne], 116 | 4e trimestre 2006, mis en ligne le 04 décembre 2007, URL : http://journals.openedition.org/rei/459 consulté le 05 avril 2018.

[696] « Rémunération pour copie privée numérique. Décision n° 1 du 4 janvier 2001 de la commission prévue à l'article L.311-5 du code de la propriété intellectuelle relative à la rémunération pour copie privée », *LEGICOM*, 2001/2 (N° 25), pp. 144-145. URL : https://www.cairn.info/revue-legicom-2001-2-page-144.htm consultée le 20 décembre 2017.

[697] En particulier l'affaire « *Mulholland Drive* » citée ci-après..

[698] Tribunal de grande instance de Paris, 3e chambre, 2e section, jugement nº03/08500 du 30 avril 2004 ;
Cour de cassation, 1ère chambre civile nº85-15.824 arrêt nº549 du 28 février 2006 ; Cour d'Appel de Paris, Chambre 04 A, jugement nº06/07506 du 4 avril 2007.

[699] Cour de cassation, Première chambre civile, Arrêt du 28 février 2006, pourvois Nº 05-15.824 et 05-16.002.

l'importance économique que l'exploitation de l'œuvre, sous forme de DVD, représente pour l'amortissement des coûts de production cinématographique ». Le dispositif anticopie empêche effectivement la copie privée, mais il est justifié pour des raisons économiques d'amortissement des coûts de production cinématographique[700]. Le DVD est reconnu comme un moyen d'amortir les coûts de production d'un film, amortissement qui ne peut plus être réalisé par la seule exploitation en salle de projection[701]. Par ailleurs, la Cour de cassation, comme la Cour d'appel l'avait fait, dit que la copie privée n'est pas un droit, mais une exception légale au principe de non-reproduction d'une œuvre protégée[702]. Ainsi, sous la pression des grands studios, les dispositifs de DRM restent légaux, ils ne doivent pas entraver la lecture du support, mais peuvent en empêcher la copie privée pour laquelle une taxe est perçue pour l'achat de tout support magnétique[703].

§ 2 - La création et Internet

La directive européenne 2001/29/CE[704] prévoit l'harmonisation de la protection juridique du droit d'auteur et des droits voisins dans les pays membres de l'Union européenne pour contribuer « *à l'application des quatre libertés du marché intérieur*[705] *et porte sur le respect des principes fondamentaux du droit et de la propriété intellectuelle, de la liberté d'expression et de l'intérêt général* »[706]. Cette harmonisation du droit d'auteur et des droits dérivés doit se fonder « *sur un niveau de protection élevé, car ces droits sont essentiels à la création*

[700] « Affaire *Mulholland Drive* : suite et fin ? », *LEGICOM*, 2007/3 (n° 39), pp. 161-163. URL : https://www.cairn.info/revue-legicom-2007-3-page-161.htm consulté le 5 avril 2018.
[701] Ariane Fusco-Vigne, « Le DVD : un produit culturel au destin contrarié ? », *LEGICOM*, 2006/2 (n° 36), pp. 141-152. URL : https://www.cairn.info/revue-legicom-2006-2-page-141.htm consulté le 5 avril 2018.
[702] Confirmé par Cour de cassation, Première chambre civile, Arrêt du 19 juin 2008, pourvoi N° 07-14.277.
[703] Taxe créée par la loi de 1985 sur les cassettes vierges, (Loi n° 85-660 du 3 juillet 1985 *relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle*), étendue aux disques magnétiques (Loi n° 92-597 du 1er juillet 1992 *relative au code de la propriété intellectuelle* (partie Législative)).
[704] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 *sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information* parue au Journal officiel n° L 167 du 22/06/2001 pp– 10-19.
[705] Ces quatre libertés sont : libre circulation des biens, libre circulation des capitaux, libre circulation des services, libre circulation des personnes.
[706] Considérant n° 3 de la directive 2001/29/CE.

intellectuelle »[707]. Cette directive autorise l'exception pour copie privée. La France a transposé cette directive dans la loi DADVSI[708].

A) De la loi DADVSI aux lois HADOPI

Lors de l'ouverture des débats sur le projet de loi DADVSI, des représentants de la FNAC et de VIRGIN[709], disposant de badges du ministère de la Culture, ont proposé aux députés des abonnements pour télécharger de la musique, après un rappel au règlement, ils ont été invités à quitter l'hémicycle[710]. Cet incident montre le lobbying exercé par les distributeurs afin de valider les dispositions prévues dans le projet de loi. Le projet prévoyait une licence globale[711] dès son article 1er. La licence globale permettait aux internautes d'accéder à des contenus protégés et de les échanger à des fins non commerciales en contrepartie d'une redevance reversée aux artistes. Cet article a été retiré par le gouvernement sous la pression des industriels du secteur culturel.

La loi DADVSI modifie le code de la propriété intellectuelle pour y introduire les modifications nécessaires pour la transposition de la directive 2001/29/CE. Un article 24 prévoyait une dépénalisation de la reproduction non autorisée à des fins personnelles d'une œuvre mise à disposition par des logiciels d'échange de pair à pair, article déclaré non conforma à la Constitution par le Conseil constitutionnel[712] pour rupture d'égalité, l'échange par un autre moyen restant un délit.

Un rapport fut demandé par le gouvernement à Denis Olivennes, Président-Directeur Général de la FNAC, enseigne diffusant des œuvres littéraires et artistiques. Le rapport remis au ministre de la Culture et de la Communication[713] porte sur des mesures pour désinciter au piratage numérique et inciter au développement de l'offre légale d'œuvres sur Internet. Le rapport préconise des « *réponses proportionnées, pragmatiques, respectueuses des libertés*

[707] Considérant nº 9 de la directive 2001/29/CE.
[708] Loi nº 2006-961 du 1er août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information* publiée au Journal officiel de la République française nº178 du 3 août 2006 p. 11529.
[709] Ces deux sociétés proposaient des accès à des sites de téléchargement légal.
[710] Relaté dans Thierry Stoehr, « Dossier DADVSI », 21 décembre 2005, *Pour les formats ouverts,* URL : https://formats-ouverts.org/post/2005/12/21/656-dossier-dadvsi consulté le 20 décembre 2017.
[711] Concept inventé et proposé par l'administration des droits des artistes et musiciens interprètes ou ADAMI et la Société de Perception et de Distribution Des Droits des Artistes-interprètes ou SPEDIDAM.
[712] Conseil constitutionnel, décision nº 2006-540 DC du 27 juillet 2006 *Loi relative au droit d'auteur et aux droits voisins dans la société de l'information* paru au Journal officiel du 3 août 2006, p. 11541.
[713] Denis Olivennes, *Le développemnt et la protection des œuvres culturelles sur les nouveaux réseaux,* Ministère de la culture et de la communication, Novembre 2007.

individuelles et compatibles avec la rapidité d'évolution des technologies ». Il propose de mettre en place une autorité publique qui aurait l'autorité d'avertir le titulaire de l'abonnement à Internet du piratage constaté et décider d'une sanction administrative en cas de récidive de ce piratage : amende et suspension ou résiliation de l'abonnement Internet.

Le 23 mai 2007, le Conseil d'État[714] annule quatre décisions de la Commission nationale de l'informatique et des libertés refusant à des ayants droit de collecter des adresses IP permettant de constater des téléchargements illégaux sur le réseau. En mai 2008, la Commission de l'informatique et des libertés est consultée par le gouvernement sur le projet de loi HADOPI, le rapport de la CNIL est gardé secret par le gouvernement. Ce rapport défavorable sera divulgué par la presse[715], les principaux griefs dont il fait état concernent : le motif purement économique du projet de loi, le fait que la coupure de l'Internet provoquera aussi la coupure du téléphone et de la télévision, l'HADOPI pourra accéder à des données personnelles sans l'intervention d'un juge, la limite entre vie privée et surveillance de l'Internet est mal définie.

Après plusieurs navettes entre l'Assemblée nationale et le Sénat, la loi HADOPI sera votée le 13 mai 2009. Le Conseil constitutionnel[716] saisi par les parlementaires déclarera que la libre communication des pensées et des opinions implique la liberté d'accéder aux services de communication en ligne, en conséquence la restriction d'accès à ces services ne peut être confiée à une autorité administrative. La collecte et le traitement des données devront faire l'objet d'une autorisation de la Commission de l'informatique et des libertés. La loi, amputée des articles déclarés non conformes à la Constitution sera promulguée le 12 juin 2009[717].

Le 24 juin 2009, un projet de loi complémentaire est présenté en conseil des ministres. Le texte de la loi HADOPI 2 sera voté en septembre 2009[718] et déclaré conforme à la Constitution par le Conseil constitutionnel[719].

---

[714] Conseil d'État, 10e et 9e sous-sections réunies, décision n°288149 du 23/05/2007.

[715] Délibération n°2008-101 du 29 avril 2008 *portant avis sur le projet de loi relatif à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet,* disponible sur le site de la Quadrature du Net, URL : https://wiki.laquadrature.net/HADOPI_avis_CNIL consulté le 20 décembre 2017.

[716] Conseil constitutionnel, Décision n° 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur internet.*

[717] Loi n° 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur Internet* publiée au Journal officiel de la république française n°0135 du 13 juin 2009 p. 9666.

[718] Loi n° 2009-1 311 du 28 octobre 2009 *relative à la protection pénale de la propriété littéraire et artistique sur Internet* publiée au Journal officiel de la République française n°0251 du 29 octobre 2009 p. 18290.

[719] Conseil constitutionnel, Décision n° 2009-590 DC du 22 octobre 2009, *Loi relative à la protection pénale de la propriété littéraire et artistique sur Internet*.

La Haute Autorité pour la Diffusion des Œuvres et de la Protection des droits sur Internet (HADOPI) est créée par décret le 31 décembre 2009[720]. Dans son premier rapport d'activité couvrant la période du 1er janvier au 30 juin 2011, la HADOPI y décrit les trois étapes de la « réponse graduée » : Envoi de la première recommandation avec saisine de la commission de protection des droits par les ayants droit, demande d'identification du titulaire de l'adresse IP aux fournisseurs d'accès à Internet (FAI), et envoi de la recommandation par voie électronique et par l'intermédiaire du FAI ; envoi de la deuxième recommandation et enfin Transmission du dossier au parquet. Elle y recense 1 023 079 demandes d'identification adressées aux fournisseurs d'accès, 470 935 premières recommandations envoyées aux abonnés et 35 003 échanges avec les abonnés concernés pour un cumul de 18 429 234 constatations des ayants droit. Dans le rapport d'activité 2012-2013, la HADOPI recense 759 387 premières recommandations envoyées à des abonnés Internet, 83 299 deuxièmes recommandations et 361 délibérations de la commission de protection des droits. Dans son rapport 2015-2016, la HADOPI constate un déplacement des usages du pair-à-pair vers le streaming[721], déplacement dû à l'évolution des techniques et de l'apparition du très haut débit[722]. La copie d'un flux, en anglais *streaming ripping*, échappe actuellement aux sanctions légales qui tendent à faire disparaître la copie illicite pair-à-pair.

B) La riposte graduée dans l'Union européenne

La riposte graduée adoptée par la France a connu en Europe des difficultés pour s'imposer. L'Espagne a adopté une loi plus sévère qu'en France[723], elle applique une répression à tous les niveaux et implique les hébergeurs. L'Allemagne ne mettra pas en place la riposte graduée[724].

---

[720] Décret n°2009-1773 du 29 décembre 2009 *relatif à l'organisation de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet* publié au Journal officiel de la République française n°0303 du 31 décembre 2009 p. 23348.

[721] Le streaming est une technique d'envoi d'un fichier en lecture continue, permettant de lire un flux audio ou vidéo à mesure qu'il est diffusé. Bien que cette technique ne permette d'accéder qu'en lecture à ces flux, certains logiciels de *streaming ripping* permettent de les enregistrer sur support magnétique.

[722] Haute Autorité pour la diffusion des œuvres et de la protection des droits sur Internet, Rapport d'activité 2015-2016, p. 20, en ligne à l'URL https://hadopi.fr/sites/default/files/HADOPI_RA%202015-16_web_0.pdf, consulté le 3 mars 2017.

[723] *Proyecto de Ley por la que se modifica el Texto Refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. 28 de octubre de 2014 Boletín Oficial de las Cortes Generales*.

[724] *La lutte contre le téléchargement illégal ailleurs dans le monde* publié dans Le Monde.fr le 9 mars 2009 à http://www.lemonde.fr/technologies/article/2009/03/09/la-lutte-contre-le-telechargement-illegal-ailleurs-dans-le-monde_1162567_651865.html, consulté le 3 mars 2017.

Au Royaume-Uni, la riposte graduée a été introduite par un accord dénommé *Memorandum of understanding* signé par les principaux fournisseurs d'accès à Internet. Cet accord permet l'envoi de messages d'avertissement aux internautes pratiquant le téléchargement illégal d'œuvres. Le 7 avril 2010, le parlement britannique a voté le *Digital Economy Act*[725]. Cette loi prévoit une restriction de la bande passante, donc un ralentissement des communications sur Internet, et une limite du téléchargement avant une suspension d'Internet qui ne peut être réalisée qu'après enquête. Ce sont les fournisseurs d'accès Internet qui ont l'obligation d'appliquer la riposte graduée après autorisation donnée par un juge. Bien que deux fournisseurs d'accès Internet, British Telecom et TalkTalk, aient déposé un recours contre le *Digital Economy Act* arguant qu'il ne respectait pas le droit européen, la cour de justice britannique l'a validé après deux ans de procédures en mars 2012[726].

Au sein de l'Union européenne, la riposte graduée initialement prévue par la loi française HADOPI et que la France souhaitait étendre à l'Union européenne a été contestée au sein du Parlement européen. Dans le cadre de la préparation du paquet télécom qui ne concernait pas la régulation des contenus, un amendement a été déposé par l'eurodéputé Guy Bono. Cet amendement, voté par le parlement le 8 mai 2009, stipule qu'« *aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux sans décision préalable des autorités judiciaires* ». Ainsi, la riposte graduée qui était prévue par le projet de loi HADOPI, en cours de discussion, et qui prévoyait que l'autorité administrative prévue par la loi pouvait décider de couper l'accès à Internet ne devenait plus possible. Le Conseil constitutionnel a retenu cette position dans sa décision nº 2009-580 DC du 10 juin 2009[727].

Le paquet télécom sera adopté le 24 novembre 2009[728], il vise à améliorer la concurrence et à protéger les droits des consommateurs dans le domaine des télécommunications. Le texte

[725] Publié sous le nom de *Digital Economy Act* 2010 le 8 avril 2010.

[726] Arik Benayoun, « Le Royaume-Uni valide son Hadopi », *DegroupNews*, 7 mars 2012, URL : https://www.degroupnews.com/Internet/royaume_uni-hadopi-telechargement-riposte_graduee-piratage, consulté le 3 mars 2017.

[727] Conseil constitutionnel, Décision n° 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur Internet*.

[728] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 *modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.*
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*

adopté dispose que l'accès à Internet des utilisateurs ne peut être restreint que si « *cela est jugé approprié, proportionné et nécessaire dans le cadre d'une société démocratique et si cette restriction est subordonnée à des garanties procédurales adéquates.* » Ainsi, l'accès à Internet devient un droit, sa restriction pour défendre un autre droit doit être proportionnée au but recherché.

associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.

Chapitre 2. Une législation spécifique protégeant l'individu sur le réseau

L'accès à Internet est devenu un droit protégé et garanti[729]. Il permet à l'individu de s'exprimer, d'échanger des informations ou des commentaires et de s'informer. Il peut être utilisé pour accéder à des bases de connaissance ou acheter des produits et services. Internet est devenu un outil omniprésent et omniscient[730].

Mais l'accès à Internet laisse des traces de toute activité réalisée, que ce soit des recherches d'information via un moteur de recherche, des achats ou des prévisions d'achats, des messages échangés entre destinataires ou toute information dématérialisée et transitant sur un réseau de télécommunications[731]. Lors d'une recherche dans une bibliothèque, seuls les livres consultés peuvent être notés par le bibliothécaire si ces livres ne sont pas en libre-service. Dans un moteur de recherche, la recherche elle-même et les résultats obtenus, ainsi que les compléments éventuels, seront stockés dans la mémoire des ordinateurs ayant participé à cette recherche. Non seulement la recherche est connue, mais une analyse des recherches connexes permet de déterminer le but de cette recherche[732].

Si une personne souhaite acheter un bouquet de fleurs pour offrir à une autre personne, en entrant chez un fleuriste, il peut effectuer son achat et payer en numéraire, ce qui rend la transaction anonyme. Le fleuriste saura que cette personne, qu'il peut ne pas connaître, a l'intention d'offrir des fleurs à une autre personne, mais il ne saura pas à qui. Si ce bouquet de fleurs est acheté sur Internet via un site de commerce en ligne, le moteur de recherche utilisé pour accéder au site marchand a l'information du souhait de la personne d'acheter des fleurs, mais le site marchand qui effectuera la livraison, connaîtra le nom et l'adresse de la personne

[729] Conseil constitutionnel, Décision nº 2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur Internet*.
[730] Rémy Rieffel, *Révolution numérique, révolution culturelle ?*, 2014, Éditions Gallimard, pp. 11-20.
[731] Tristan Nitot, *surveillance:// Les libertés au défi du numérique : comprendre et agir,* 2016, C&F éditions, pp. 13-17.
[732] Louise Merzeau, « Du signe à la trace : l'information sur mesure », *Hermès, La Revue*, 2009/1 (n° 53), pp. 21-29. URL : https://www.cairn.info/revue-hermes-la-revue-2009-1-page-21.htm consulté le 6 avril 2018.

destinataire du bouquet, de plus il aura accès à d'autres informations sur l'acheteur à travers le moyen de paiement utilisé. Le site pourra cibler cet acheteur à l'occasion d'une campagne de publicité ou de toute autre occasion, cette cible étant devenue une cible à fort potentiel, car déjà sensibilisée à l'achat de fleurs. L'information concernant l'acheteur est devenue une information commerciale à valeur ajoutée[733]. Le site marchand dispose de l'information, mais le moteur de recherche également et il peut vendre cette cible à d'autres sites marchands. L'achat du bouquet de fleurs sur Internet est devenu un acte à valeur ajoutée accessible par plusieurs entités, alors que l'achat chez le fleuriste reste un acte confiné à un petit cercle relationnel.

De même, l'échange de courrier entre deux personnes est un acte strictement privé non communiqué à un tiers, hors le cas rare de publication, souvent posthume, de cette correspondance. Seules deux personnes, le rédacteur de la missive et son destinataire, en connaissent la teneur, en principe, et sauf interception de ce courrier, interception décelable et répréhensible moralement et pénalement[734]. En utilisant une messagerie électronique, le message va transiter sur plusieurs ordinateurs qui vont, dans leur mémoire cache, stocker ce message le temps nécessaire du transit. Il est stocké sur le serveur de messagerie d'origine ainsi que sur celui de destination. Une interception est toujours techniquement possible, si l'émetteur ou le destinataire sont mis sous surveillance, une copie du message peut être réalisée sans trace sur le message pour l'émetteur ou le destinataire. Un cryptage du message est possible à l'initiative du serveur, mais ce cryptage n'est pas une protection absolue. Le contenu des messages stockés sur des serveurs peut être analysé par le responsable du site pour en extraire des informations personnelles[735].

Les actes de la vie privée peuvent ainsi voir, dans la société numérique et dématérialisée, leur statut modifié et devenir soit des actes commerciaux à valeur ajoutée soit des actes dévoilant

[733] Emmanuel Kessous, Bénédicte Rey, « Économie numérique et vie privée », *Hermès, La Revue*, 2009/1 (n° 53), pp. 49-54. URL : https://www.cairn.info/revue-hermes-la-revue-2009-1-page-49.htm consulté le 6 avril 2018.

[734] Code pénal, articles 223-15 et 432-9 ; Code des postes et des communications électroniques, article L.33-1 ; Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications*, publiée au Journal officiel n° L 024 du 30/01/1998 pp. 1-8.

[735] Google a scanné les messages transitant dans la messagerie gmail.com pour extraire des informations de ciblage publicitaire. Cette pratique était décrite dans les conditions générales d'utilisation : « *Nos systèmes automatisés analysent votre contenu (y compris les emails) pour vous diffuser des fonctionnalités pertinentes pour vous, comme des résultats de recherche personnalisés, de la publicité sur mesure, et détecter spam et malwares. Cette analyse a lieu à la réception, à l'envoi et lors du stockage du contenu* ». Officiellement, Google a renoncé à cette pratique en 2017 (Lucie Ronfaut, « Google ne lira plus les emails pour personnaliser ses publicités », 25 juin 2017, *Le Figaro.fr,* URL : http://www.lefigaro.fr/secteur/high-tech/2017/06/25/32001-20170625ARTFIG00112-google-ne-lira-plus-les-emails-pour-personnaliser-ses-publicites.php consulté le 27 décembre 2017).

des aspects privés de la vie des personnes, sans que cette mutation ne soit connue ou perçue par les personnes concernées[736]. Une protection des individus contre les abus et intrusions dans la vie privée est nécessaire.

La France, dès 1978, avec la loi informatique et libertés[737], a développé un droit spécial concernant le monde numérique et a créé une autorité administrative indépendante[738], la Commission nationale de l'informatique et des libertés, chargée de veiller au respect de ce droit et de proposer des règles encadrant cette activité. Elle lui a aussi donné un pouvoir de sanction. L'Union européenne a également légiféré et généralisé le besoin d'une telle autorité dans tous les pays de l'Union[739], et l'ensemble des autorités de protection des données personnelles forme le groupe G29, du nom de l'article qui prévoit cette coordination. Depuis 2016, un nouveau règlement a été publié concernant la protection des individus face aux traitements automatiques des données[740]. Ce règlement applicable en mai 2018 tient compte de l'évolution de l'Internet et de son utilisation depuis plus d'un quart de siècle. Le G29 devenu Comité européen de la protection des données est institué en tant qu'organe de l'Union européenne avec une personnalité juridique[741].

[736] Pascal Perez, « Liberté et vie privée à l'aube des nouveaux médias », *Après-demain*, 2013/3 (n ° 27-28, NF), pp. 49-52. URL : https://www.cairn.info/revue-apres-demain-2013-3-page-49.htm consulté le 6 avril 2018.
[737] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* publiée au JORF du 7 janvier 1978 p. 227.
[738] CNIL Commission nationale de l'informatique et des libertés, créée par la loi du 6 janvier 1978.
[739] Avec la 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.*
[740] 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).*
[741] Règlement général sur la protection des données, art. 68.

D'autres textes sont adoptés en France, concernant exclusivement le monde numérique : loi sur le commerce électronique[742], loi sur la signature électronique[743], loi sur les noms de domaine[744], lois HADOPI 1 et HADOPI 2[745], elles-mêmes précédées d'une loi DADVSI[746].

L'Union européenne a elle-même légiféré sur le domaine : directive sur la signature électronique[747], directive sur le commerce électronique[748], directive sur les données personnelles[749]. Ces directives, transposées dans la législation des pays membres, ont abouti à une certaine harmonisation des législations au sein des pays membres de l'Union européenne.

Ces textes spéciaux ont tous pour but de limiter et restreindre les conséquences de l'utilisation de l'Internet, ou des techniques numériques, afin de protéger des droits préexistants à l'expansion des techniques numériques, droits attaqués par ces nouvelles techniques : droit d'auteur, propriété intellectuelle, et aussi droits de la personne et libertés fondamentales, mais ces textes ont aussi pour but d'introduire dans le droit positif, certaines spécificités du numérique, le Code civil est ainsi modifié pour assurer la validité de la signature électronique et son équivalence avec la signature papier[750].

La protection de la vie privée à travers la protection des données personnelles fait l'objet d'une législation spécifique sur Internet et par tout système de traitement manuel ou automatique de données (Section 1.), et de nouveaux textes encadrent l'utilisation de techniques nouvelles pour certains actes de la vie privée (Section 2).

---

[742] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique, Titre II Du commerce électronique* publiée au JORF nº143 du 22 juin 2004 p. 11168.

[743] Loi nº 2000-230 du 13 mars 2000 *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* publiée au JORF nº62 du 14 mars 2000 p. 3968.

[744] Loi nº 2011-302 du 22 mars 2011 *portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques,* Chapitre III : Dispositions relatives aux communications électroniques publiée au JORF nº0069 du 23 mars 2011 p. 5186.

[745] Loi nº 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur Internet,* publiée au *JORF nº0135 du 13 juin 2009 p. 9666.*

Loi nº 2009-1 311 du 28 octobre 2009 *relative à la protection pénale de la propriété littéraire et artistique sur Internet* publiée au JORF nº0251 du 29 octobre 2009 p. 18290.

[746] Loi nº 2006-961 du 1 août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information* publiée au JORF nº178 du 3 août 2006 p. 11529.

[747] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999*, sur un cadre communautaire pour les signatures électroniques* publiée au JO L 13 du 19.1.2000, pp. 12-20.

[748] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000, *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« directive sur le commerce électronique ») publiée au Journal officiel nº L 178 du 17/07/2000 pp. 1-16.

[749] 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* publiée au Journal officiel nº L 281 du 23/11/1995 pp. 31-50.

[750] Code civil, Article 1316-4 créé par la loi no 2000-230 du 13 mars 2000 *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, publiée au JORF nº62 du 14 mars 2000 p. 3968.

Section 1. La protection de la vie privée au travers de la protection des données personnelles

« *La vie privée est cette sphère de chaque existence dans laquelle nul ne peut s'immiscer sans y être convié. La liberté de la vie privée est la reconnaissance, au profit de chacun, d'une zone d'activité qui lui est propre et qu'il est maître d'interdire à autrui*[751] ».

La liberté de la vie privée doit être garantie, chaque individu doit pouvoir exister sans que tous ses faits et gestes, voire ses pensées, soient visibles et connus de tous, et restent confinés à une sphère réduite, restreinte aux personnes que cet individu aura autorisées à en connaître. L'expression de cette liberté impose que toute personne physique jouisse d'une égalité de droits[752].

La notion d'atteinte à la vie privée trouve sa protection dans l'article 9 du Code civil[753], sans que cette notion de vie privée ne soit précisément définie par les textes. Le droit au respect de la vie privée et le droit à la protection des données à caractère personnel semblent indissociables, mais ne sont pas en France inscrits dans la Constitution ou ses préambules. Le Conseil constitutionnel a considéré « qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : *"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."* ; que la liberté proclamée par cet article implique le respect de la vie privée »[754]. Ces droits se trouvent donc indirectement protégés par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789. Cette protection n'est pas absolue et la limite entre vie privée et vie publique peut être l'objet d'une décision judiciaire. La Cour européenne des droits de l'homme a justifié ainsi la divulgation par l'hebdomadaire français Paris Match d'un fils illégitime du Prince Albert de Monaco[755], révélation jugée d'intérêt public

[751] Jean Rivero, *Libertés publiques*, Montchrestien, 1989, p. 74.
[752] Article 1er de la Déclaration des droits de l'homme et du citoyen de 1789 : « *Les hommes naissent et demeurent libres et égaux en droits* ».
[753] Code civil, article 9 : « *Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée ; ces mesures peuvent, s'il y a urgence, être ordonnées en référé.* », Article créé par la loi nº 70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens*, parue au Journal officiel de la république française du 19 juillet 1970 p. 6751.
[754] Conseil constitutionnel, Décision nº 99-416 du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle* (Journal officiel du 28 juillet 1999, p. 11250).
[755] Cour Européenne des Droits de l'Homme (Grande chambre) Arrêt du 10 novembre *2015 Couderc et Hachette Filipacchi associés c/ France* (requête nº 40454/07).

compte tenu du caractère héréditaire des fonctions de chef de l'État monégasque. Cet arrêt a privilégié la liberté d'expression et d'information, protégée par l'article 10 de la Convention, face au droit à la vie privée, objet de l'article 8 de la même Convention.

La protection des données à caractère personnel est aussi confrontée à la mondialisation des fournisseurs de services Internet, du réseau et des législations très différentes selon les pays[756]. En France, les données à caractère personnel sont protégées par des textes d'origine française, mais aussi européenne, toutefois le caractère mondial de l'Internet les rend parfois d'application difficile. Pour certains pays, dont les pays d'Amérique du Nord, les données à caractère personnel sont des données ayant une valeur marchande négociable, alors que pour d'autres pays, la France ou l'Allemagne, elles sont propres à l'individu et au respect de sa vie privée[757]. Il existe en France des auteurs qui préconisent un droit à la propriété des données, comme Alain Bensoussan[758] pour qui les données sont des biens incorporels et qui propose d'élaborer une convention des droits fondamentaux de l'homme virtuel[759]. De plus depuis plusieurs années, dans des domaines divers, la législation des États-Unis d'Amérique acquiert un statut d'extraterritorialité contraignant (embargo, normes comptables, corruption, etc.), statut accepté de facto par les États tiers, et qui interfère avec les législations étatiques ou européennes.

Sous-section 1. La protection de la vie privée, objet de textes nationaux et internationaux

La vie privée, même si elle n'est pas légalement définie dans les textes, fait l'objet de textes protecteurs, directement ou indirectement, tant dans les législations des États, comme en France avec la loi informatique et libertés ou le Code civil, que dans les textes internationaux ou européens. En France, la vie privée n'est pas directement protégée par la Déclaration des droits de l'homme, mais fait l'objet de l'article 9 du Code civil protégeant l'intimité de la vie privée

[756] Louise Cadoux, Pierre Tabatoni, « Internet et protection de la vie privée », *Commentaire*, 2000/1 (Numéro 89), p. 57-66. URL : https://www.cairn.info/revue-commentaire-2000-1-page-57.htm consulté le 27 décembre 2017.
[757] Arnaud Anciaux, Joëlle Farchy, Cécile Méadel, « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle*, 2017/2 (n° 158), pp. 9-41. URL : https://www.cairn.info/revue-d-economie-industrielle-2017-2-page-9.htm consulté le 6 avril 2018.
[758] Alain Bensoussan, avocat à la Cour d'appel de Paris, spécialiste en droit des nouvelles technologies de l'informatique et de la communication, ainsi qu'en droit international et de l'Union européenne.
[759] Sur son blog à l'URL : http://blog.lefigaro.fr/bensoussan/2013/01/le-profilage-commercial-est-inherent.html consulté le 13 novembre 2015.

créé par la loi de 1970[760]. La loi informatique et libertés protège l'utilisation des données personnelles qui peuvent révéler de nombreux aspects de la vie privée. Le Conseil de l'Europe a publié le 28 janvier 1981 la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, appelée Convention nº 108[761].

Au niveau européen, la vie privée est également protégée par la Convention européenne des droits de l'homme de 1950, dans son article 8, par la Charte des droits fondamentaux de l'Union européenne, dans ses articles 7 et 8, et au niveau international par la Déclaration universelle des droits de l'homme de 1948, dans son article 12. Dans certains pays européens, Allemagne, Espagne ou Italie, la protection est assurée par la Constitution.

§ 1 - La protection de la vie privée en France

La vie privée est la capacité pour une personne physique de s'isoler pour occulter de la vision du groupe certains aspects de sa personnalité : santé, sexualité, patrimoine, filiations, etc. Lorsque certains aspects sont connus de professionnels, médecins, ecclésiastiques, avocats ou notaires, ceux-ci sont tenus au secret professionnel et ne peuvent divulguer les informations qu'ils sont amenés de par leur activité à découvrir[762]. La séparation vie publique-vie privée[763] n'est pas toujours facile à définir et à respecter et peut faire l'objet d'une décision de justice, en particulier pour certains personnages publics dont la vie privée et la vie publique se trouvent fortement interdépendantes. Jean Rivero en donne la définition suivante : « *la vie privée est cette sphère où nul ne peut s'immiscer sans y être convié* »[764], mais relativise la définition de cette sphère.

---

[760] Loi nº70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens,* Troisième partie Protection de la vie privée, article 22, publiée au JORF du 19 juillet 1970 p. 6751.

[761] Conseil de l'Europe, Série des traités européens – nº 108, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981.

[762] Le secret professionnel est défini par l'article 226-13 du Code pénal : « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende* ».

[763] Michel Maffesoli. « Vie publique - Vie privée ». *Réseaux*, volume 1, n°3, 1983. *La communication au quotidien*. pp. 37-48, URL : http://www.persee.fr/doc/reso_0751-7971_1983_num_1_3_1094 consulté le 27 décembre 2017.

[764] Jean Rivero, Hugues Moutouh, *Libertés publiques, Tome II,* 7e édition mise à jour, Presses Universitaires de France, p. 87.

Dans une société fortement numérisée, la vie privée peut être dévoilée au travers des données personnelles des individus, des correspondances ou des communications. Aussi, la protection de l'intimité de la vie privée, protégée par l'article 9 du Code civil, passe par la protection des données personnelles et l'inviolabilité des correspondances privées ou des communications qui, aujourd'hui, sont véhiculées sur les réseaux de télécommunications sous forme numérique[765].

A) Une loi française innovante protégeant les données personnelles

À la fin des années soixante, des chercheurs ont mis en avant les risques liés aux libertés du fait du développement de l'informatique, notamment dans les administrations publiques. En se dotant, en 1978, d'une législation spécifique en matière d'informatique et de liberté ainsi que d'une autorité indépendante de contrôle, la France figure, après le Land de Hesse (Allemagne) en 1970 et la Suède en 1973[766], dans le « trio de tête » des États ayant légiféré pour protéger les personnes physiques des conséquences des traitements de données informatiques. Le but de cette législation était de reconnaître de nouveaux droits au profit des citoyens à l'égard des grands systèmes centralisés d'informations dont les administrations commençaient à se doter[767].
En janvier 1974, les États-Unis adoptent un *Privacy Act*[768] limité aux fichiers détenus par les administrations fédérales et prévoyant un droit d'accès pour les citoyens américains.
En 1974, en France apparaît aussi une réelle prise de conscience avec la révélation au public, du projet d'élaboration d'un « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus » ou SAFARI[769]. Ce système prévoit l'institution d'un identifiant unique (n° de sécurité sociale, devenu depuis NIR[770]) pour interconnecter les fichiers publics (dont les renseignements généraux, la direction de la sécurité du territoire et la police judiciaire). Devant l'indignation provoquée par ce projet, le Premier ministre le retire et crée une commission, présidée par M. Bernard Chenot, qui est chargée de proposer des mesures tendant

[765] Alain Rallet, Fabrice Rochelandet, Célia Zolynski, « De la *Privacy by Design* à la *Privacy by Using*. Regards croisés droit/économie », *Réseaux*, 2015/1 (n° 189), pp. 15-46. URL : https://www.cairn.info/revue-reseaux-2015-1-page-15.htm consulté le 27 décembre 2017.
[766] Loi du 11 mai 1973 *sur la protection des données*.
[767] Stéphane Tijardovic, « La protection juridique des données personnelles. Vers une nécessaire adaptation de la norme juridique aux évolutions du monde numérique », *Les Cahiers du numérique*, 2003/3 (Vol. 4), pp. 185-203. URL : https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-185.htm consulté le 27 décembre 2017.
[768] *Privacy Act* of 1974, 5 U.S.C. § 552 a.
[769] Philippe Boucher, « Safari ou la chasse aux français » in *Le Monde* du 21 mars 1974.
[770] NIRPP ou en abrégé NIR est le numéro d'inscription au répertoire des personnes physiques servant à identifier une personne dans le répertoire national d'identification des personnes physiques (RNIPP) géré par l'INSEE.

à concilier le développement de l'informatique dans les secteurs public, semi-public et privé et le respect de la vie privée, des libertés individuelles et des libertés publiques. Le rapport de la commission, rédigé par Bernard Tricot et le professeur Pierre Catala[771], remis en juin 1975, inspira la loi du 6 janvier 1978 « Informatique, fichiers et libertés ». La « Commission informatique et libertés » proposa, après de larges consultations et débats, de créer une autorité indépendante, création réalisée par la loi du 6 janvier 1978[772] qui institue la Commission nationale de l'informatique et des libertés[773]. La loi de 1978 a été modifiée à de nombreuses reprises et en particulier en 2004[774] pour transcrire en droit français la directive européenne 95-46 CE[775]. Une nouvelle loi est en cours de discussion au Parlement pour adapter la législation nationale au Règlement général sur la protection des données avant le 25 mai 2018.

Dans l'exposé des motifs du projet de loi de 1978, le gouvernement précise : « *Si la menace n'est pas encore grave, elle pourrait, si des mesures ne sont pas prises à temps, constituer un jour une des formes d'agression de la vie moderne.*

« Le Gouvernement a donc le devoir de prévenir ce risque en temps voulu et de définir les usages de l'informatique dans une société de progrès qui demeure une société de liberté. »

Le rapporteur de la commission des lois, M. Foyer qui donna son nom à cette loi, écrit : « *La conservation massive et systématique des données relatives à chaque personne tend à figer les situations en attachant aux individus des étiquettes jadis plus rares et plus approximatives et dont il leur était plus facile de se débarrasser* »[776]. Cette phrase semble prémonitoire et reste d'actualité avec la collecte et la conservation des données par les grands acteurs de l'Internet, Google, YAHOO!, Facebook, etc., mais aussi par certaines administrations, telles l'administration fiscale, la police et la gendarmerie. Déjà, il fait état de la difficulté d'effacer ou d'oublier des étiquettes qui se trouveraient accolées à des individus. Les premières

[771] Bernard Tricot, Pierre Catala, *Rapport de la commission informatique et libertés*, La documentation française, juin 1975, disponible à http://www.cil.cnrs.fr/CIL/IMG/pdf/rapport_tricot_1.pdf.

[772] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* publiée au JORF du 7 janvier 1978 p. 227.

[773] CNRS, « Origine de la loi Informatique et Libertés », 15 novembre 2015, URL : http://www.cil.cnrs.fr/CIL/spip.php?article1871 consulté le 27 décembre 2017.

[774] Loi nº 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, publiée au JORF nº182 du 7 août 2004 p. 14063.

[775] 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.*

[776] Jean Foyer, Rapport n° 3125 fait au nom de la commission des lois, déposé le 4 octobre 1977, Assemblée nationale.

législations concernant le droit à l'oubli n'apparaissent qu'en 2016 en France et au niveau de l'Union européenne[777].

Aujourd'hui, en France, le NIR n'est systématiquement utilisé que par les organismes de l'administration sociale. Mais la technique a évolué et la puissance de calcul disponible permet de contourner cette restriction à l'utilisation du NIR, par des recoupements et des rapprochements d'informations disponibles et multiples. Dans son étude publiée en 2014[778], le Conseil d'État, parmi ses 50 propositions, propose en n° 21, de créer un numéro national d'identification non signifiant, c'est-à-dire ne précisant pas directement ou indirectement le sexe, l'âge ou l'origine, soit en fait un retour à SAFARI.

Dès son article 1, la loi informatique et libertés du 6 janvier 1978[779] énonce : « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Cet article 1 résume en quelques lignes les risques inhérents à l'émergence de la société numérique. Écrit en 1978 alors que la technologie de l'Internet n'existait qu'en laboratoire, cet article se révèle prémonitoire, il pourrait avoir été écrit dans les années 2000 face à la montée des réseaux sociaux, voir au début du XXI^e^ siècle avec la promulgation des lois de lutte contre le terrorisme octroyant des droits exorbitants aux organes de renseignement[780].

L'informatique ne doit pas porter atteinte à la vie privée, en conséquence les données concernant un individu, enregistrées dans un fichier doivent l'être en informant l'individu de cet enregistrement et de plus ce dernier a un droit de consultation et de correction de ces données[781]. Le Règlement général sur la protection des données, applicable en mai 2018, substitue l'information des personnes physiques au consentement de ces personnes à la collecte

[777] Ce sont la Loi n° 2016-1 321 *pour une République numérique* du 7 octobre 2016 et le 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,* textes adoptés après l'arrêt Google Spain de la Cour de justice de l'Union européenne du 13 mai 2014 ayant reconnu un droit au déréférencement.

[778] Conseil d'État, *Étude annuelle 2014 – Le numérique et les droits fondamentaux*, La Documentation française, septembre 2014.

[779] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, publiée au Journal officiel de la République française du 7 janvier 1978 p. 227.

[780] Loi n° 2015-912 du 24 juillet 2015 *relative au renseignement* publiée au JORF n°0171 du 26 juillet 2015 page 12735.

[781] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, Chapitre II — conditions de licéité des traitements de données à caractère personnel.

et au traitement. Certaines données à caractère raciale, religieuse, sexuelle sont particulièrement protégées et ne peuvent pas être recueillies sauf pour des études anonymes et à but statistique[782].
La loi de 1978 énonce les grands principes relatifs à une société numérique : coopération internationale, car compte tenu de la particularité des techniques numériques et de la mondialisation des acteurs, la protection doit être internationale et ne peut se limiter aux frontières d'un État ; protection nécessaire de l'identité humaine et des droits de l'homme, la société numérique doit respecter les principes fondamentaux mis en place préalablement à l'émergence de cette technologie qui doit donc être neutre en termes d'identité humaine et droits de l'homme ; protection de la vie privée, la vie privée et les données personnelles doivent être protégées contre toute intrusion de la technologie ; et enfin protection des libertés individuelles et publiques, la société numérique doit continuer à protéger les libertés. La Commission nationale de l'informatique et des libertés est en charge de veiller au respect de ces principes.

1) La Commission nationale de l'informatique et des libertés (CNIL)

La loi n° 78-17 a créé une autorité administrative indépendante chargée du contrôle des traitements des données à caractère personnel : la Commission nationale de l'informatique et des libertés ou CNIL. Pour la Commission de l'informatique et des libertés, la protection des données personnelles est garantie par de nombreuses dispositions et leur non-respect peut être doublement sanctionné : administrativement et pénalement[783]. Mais, face aux sommes collectées par les grandes entreprises américaines de l'Internet, les montants des amendes prévues restent symboliques[784]. Ces montants sont largement réévalués par le nouveau Règlement général sur la protection des données.
La Commission de l'informatique et des libertés agrée les traitements lorsqu'une autorisation préalable est nécessaire, elle définit les cas de dispenses additionnelles autres que celles prévues

[782] Loi n° 78-17 du 6 janvier 1978, article 8 : « *I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ».
[783] Sanctions pénales prévues par : Articles 226-16 à 226-24 du Code pénal modifiés par la loi du 6 août 2004 ; Article 226-17-1 créé par l'article 39 de l'ordonnance n°2011-1012 du 24 août 2011 ; Articles R. 625-10 à R. 625-13 du Code pénal insérés par le décret du 20 octobre 2005.
[784] Jean Frayssinet, « La régulation du respect de la loi Informatique, fichiers et libertés par le droit pénal : une épée en bois », *LEGICOM*, 2009/1 (N° 42), pp. 23-33. URL : https://www.cairn.info/revue-legicom-2009-1-page-23.htm.

par la loi, et elle diffuse des guides vers les entreprises et les personnes physiques. L'actualité a montré que durant ces dernières années, cette obligation de déclaration n'était pas toujours respectée par les entreprises, mais aussi par des organismes publics chargés de la protection des individus et du respect des lois. Les fichiers de la police (STIC, Système de traitement des infractions constatées) et de la gendarmerie (JUDEX, système judiciaire de documentation et d'exploitation) ont été initialement créés sans autorisation et régularisés a posteriori par la loi[785]. Ces deux fichiers, STIC et JUDEX ont été remplacés par le nouveau fichier national des antécédents judiciaires[786]. Comme pour STIC et JUDEX, ce traitement des antécédents judiciaires permet de saisir et conserver des informations concernant les personnes mises en cause, personnes physiques ou morales, mais aussi les victimes, les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition[787]. De plus, les avis de la Commission de l'informatique et des libertés ne sont pas opposables à l'État qui peut, par arrêté ministériel, autoriser certains traitements automatiques qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté[788], l'avis motivé de la Commission de l'informatique et des libertés étant publié avec l'arrêté autorisant le traitement. Le gouvernement autorisait ainsi, par décret publié le 28 octobre 2016[789], la création du fichier TES, enregistrant les informations recueillies pour la délivrance des cartes d'identité ou des passeports, l'avis de la CNIL[790] demandait l'organisation d'un débat parlementaire.

---

[785] Le STIC créé par la loi n°95-73 du 21 janvier 1995 entre en activité officielle sans ses décrets d'application. Le décret qui officialise le STIC date du 5 juillet 2011, le STIC a donc fonctionné 6 ans en toute illégalité. Quant à JUDEX il aurait été mis en place en 1985/1 986 clandestinement, son existence n'a été officialisée que le 20 novembre 2006.

[786] Décret n° 2012-652 du 4 mai 2012 *relatif au traitement d'antécédents judiciaires* publié au JORF du 6 mai 2012 p. 8047.

[787] Alain Bauer, Christophe Soullez, « Des fichiers, pour quelles finalités ? », dans *Les fichiers de police et de gendarmerie.* Paris, Presses Universitaires de France, « Que sais-je ? », 2011, pp. 7-29. URL : https://www.cairn.info/les-fichiers-de-police-et-de-gendarmerie--9782130591160-page-7.htm consulté le 27 décembre 2017.

[788] 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,* publiée au JORF n°182 du 7 août 2004 p. 14063, articles 26, 27, 28.

[789] Décret n° 2016-1 460 du 28 octobre 2016 *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*, publié au JORF n° 0254 du 30 octobre 2016.

[790] CNIL, Délibération n° 2016-292 du 29 septembre 2016 *portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (saisine n° 1979541)*, disponible en ligne à https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318979, consulté le 4 mars 2017.

a) Le statut de la Commission de l'informatique et des libertés

La Commission de l'informatique et des libertés est créée par l'article 11 de la loi n° 78-17 : « *La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante* ». Les missions de la Commission de l'informatique et des libertés y sont définies[791] : elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ; elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi ; à la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements, elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis et elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ; elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er (droits de l'homme, vie privée, libertés individuelles ou publiques).

Depuis le 1er septembre 2012, la fonction de Président de la CNIL est devenue incompatible avec toute activité professionnelle, tout mandat électif national, tout autre emploi public et toute détention, directe ou indirecte, d'intérêts dans une entreprise du secteur des communications électroniques ou de l'informatique[792]. Les ministres, autorités publiques, dirigeants d'entreprises, publiques ou privées, ne peuvent s'opposer à son action. Les décisions de la Commission de l'informatique et des libertés peuvent faire l'objet de recours devant la juridiction administrative. Toute personne peut s'adresser à la Commission de l'informatique et des libertés pour se faire aider à faire respecter ses droits (droit d'information, droit d'accès, droit de rectification ou de radiation, droit d'opposition et droit d'accès indirect) en cas de difficulté ou d'opposition.

[791] Loi n° 78-17, art. 11.
[792] Loi n° 78-17, art. 13.

b) Les avis de la Commission de l'informatique et des libertés

Comme le Conseil d'État, la Commission de l'informatique et des libertés peut être consultée pour avis[793]. Certains traitements mis en œuvre par des organismes publics doivent, nécessairement, recueillir l'avis de la CNIL[794]. Cette procédure concerne les traitements mis en œuvre par des organismes publics ou des organismes privés gérant un service public et qui concernent : la sûreté, la défense ou la sécurité publique ; la prévention, la recherche, la constatation ou la poursuite d'infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ; l'utilisation du NIR (nº de sécurité sociale) ou la consultation du RNIPP (lorsque les organismes ne sont pas déjà habilités) ; l'utilisation de données biométriques (empreintes digitales, contour de la main, iris de l'œil, etc.) ; le recensement de la population ; les téléservices de l'administration électronique.

Par un avis du 11 décembre 2007[795], la Commission de l'informatique et des libertés s'est prononcée sur le projet de décret permettant la délivrance des nouveaux passeports biométriques. Ce décret prévoit également la constitution d'une base de données contenant empreintes digitales et photographie numérisée des demandeurs de passeport. La Commission a estimé que le ministère n'avait pas apporté d'éléments convaincants de nature à justifier la constitution d'un tel fichier centralisé, et que la conservation dans un fichier central des photographies et des empreintes digitales (données biométriques) était disproportionnée au regard des finalités du fichier.

La Commission de l'informatique et des libertés a formulé des remarques lors de l'examen d'un projet de loi alors qu'elle n'était saisie d'aucune demande d'avis. À l'occasion du débat parlementaire sur la proposition de loi relative à la protection de l'identité, la CNIL a estimé nécessaire de faire connaître son analyse en la matière[796]. Du fait de ses responsabilités en tant que régulateur de la vie privée et de l'importance des enjeux en matière de lutte contre la fraude, elle a souhaité s'exprimer sur ce sujet majeur. Lors de sa séance plénière du 25 octobre 2011,

[793] Dans le projet de loi de modification de la loi n° 78-17 pour compléter le règlement général sur la protection des données, la demande d'avis est obligatoire dès qu'un texte concerne les données à caractère personnel, cet avis peut aussi être demandé par le Président de l'Assemblée nationale ou du Sénat. Les avis de la CNIL sont publics et doivent être publiés.

[794] Articles 26 et 27 de la loi du 6 janvier 1978 modifiée.

[795] Commission nationale de l'informatique et des libertés, Délibération n° 2007-368 du 11 décembre 2007 *portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques*, publié au JORF n° 109 du 10 mai 2008.

[796] Commission nationale de l'informatique et des libertés, *Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité*, examinée en séance plénière le 25 octobre 2011.

elle a examiné une note d'observations en faisant des propositions concrètes et pragmatiques afin de contribuer au débat et d'alimenter les réflexions en cours. Cette note s'appuie essentiellement sur les positions qu'elle a déjà adoptées s'agissant des passeports biométriques en 2007, des cartes d'identité électroniques et biométriques en 2008 et plus généralement en matière d'administration électronique et de téléservices. La Commission estime entre autres, tout comme dans le cadre de son avis sur le projet de loi présenté en 2008 par le ministère de l'Intérieur, que la proportionnalité de la conservation sous forme centralisée de données biométriques, au regard de l'objectif légitime de lutte contre la fraude documentaire, n'est pas à ce jour démontrée. Si une telle base centralisée de données biométriques était néanmoins envisagée, des garanties supplémentaires de nature à assurer la protection des données personnelles des citoyens français devraient être introduites[797]. En 2016, le gouvernement, par décret[798], autorisera la création du fichier TES qui regroupera les données fournies pour l'obtention d'un passeport et de la carte nationale d'identité, malgré l'avis peu favorable de la Commission de l'informatique et des libertés[799]. En janvier 2017, le ministre de l'Intérieur a rendu public un rapport d'audit de sécurité élaboré conjointement par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), rapport qui démontre que « *le système peut techniquement être détourné à des fins d'identification biométrique des personnes concernées* » et que son inviolabilité ne peut être garantie[800], rejoignant ainsi les critiques formulées lors de la discussion parlementaire relative au projet de fichier des « gens honnêtes » et les remarques formulées par la CNIL.

[797] L'Assemblée nationale a voté la création du fichier « des honnêtes gens » le 6 mars 2012 (Loi nº 2012-410 du 27 mars 2012 relative à la protection de l'identité), cette disposition a été censurée par le Conseil constitutionnel (décision du Conseil constitutionnel nº 2012-652 DC du 22 mars 2012).
[798] Décret nº 2016-1 460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, publié au JORF nº 0254 du 30 octobre 2016.
[799] Commission nationale de l'informatique et des libertés, Délibération n° 2016-292 du 29 septembre 2016 *portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité* (saisine n° 1979541), publiée au JORF n°0254 du 30 octobre 2016.
[800] *Audit du système « Titres Electroniques Sécurisés »,* Ministère de l'Intérieur en ligne à l'URL : http://mobile.interieur.gouv.fr/content/download/100011/786238/file/rapport-commun-public-tes-13-01-20172.pdf, consulté le 19 novembre 2017.

Le pouvoir de la CNIL face aux volontés sécuritaires des gouvernements est pratiquement inopérant[801] et cette faiblesse apparente nuit à sa notoriété dans le public[802]. Mais la CNIL a le pouvoir de défendre les nouveaux droits des personnes physiques en relation avec la protection de leurs données à caractère personnel.

2) Les droits des personnes physiques protégés par la CNIL

La loi informatique et liberté a créé plusieurs droits pour les personnes physiques dans le but de les protéger des dérives des traitements de leurs données personnelles. Ces droits ont été repris par la directive 95/46/CE. Ces droits sont : le droit à l'information, le droit d'opposition, le droit d'accès et le droit de rectification. De plus, elle distingue les données personnelles « *qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* »[803], la collecte de ces données étant interdite. De nouveaux droits, le droit à l'effacement et le droit à la portabilité des données sont introduits par le nouveau règlement général sur la protection des données.

a) Le droit à l'information

Toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée[804]. Ce droit de regard sur ses propres données personnelles vise aussi bien la collecte des informations que leur utilisation. Ce droit d'être informé est essentiel, car il conditionne l'exercice des autres droits tels que le droit d'accès ou le droit d'opposition.
Dans le cadre d'une utilisation de réseaux, les personnes doivent être informées de l'emploi éventuel de témoins de connexion (cookies, variables de session…), et de la récupération

[801] Jean-Marc Manach, « "Défavorablement connus" », *Pouvoirs*, 2018/1 (n° 164), pp. 49-61. URL : https://www.cairn.info/revue-pouvoirs-2018-1-page-49.htm consulté le 6 avril 2018.
[802] Jérôme Huet, Pierre Leclercq, « La CNIL a-t-elle accompli les missions dévolues par le législateur ? », *LEGICOM*, 2009/1 (n° 42), pp. 13-21. URL : https://www.cairn.info/revue-legicom-2009-1-page-13.htm consulté le 27 décembre 2017.
[803] Loi n° 78-17, Article 8.
[804] Loi n° 78-17, Article 32 modifié par l'ordonnance n° 2011-1012 du 24/08/2011.

d'informations sur la configuration de leurs ordinateurs (systèmes d'exploitation, navigateurs)[805].

Ce droit à l'information est repris et confirmé dans le nouveau règlement européen qui conditionne ces collectes à un consentement explicite de la personne concernée, tant pour la collecte que pour le traitement envisagé. Ainsi, toute utilisation de données autre que celle acceptée devient illicite, d'où une nécessité d'information et de transparence sur la finalité des traitements[806].

Ce droit à l'information n'est pas facile à mettre en œuvre et à respecter. En effet, si pour les cookies un message apparaît pour indiquer que le site utilise des cookies et donc peut enregistrer des données liées à la navigation sur le site, certains cookies peuvent enregistrer d'autres types d'informations à caractère personnel, données disponibles sur un ordinateur personnel ou un smartphone, tels la localisation, l'adresse IP, le type de système, etc. Actuellement, sur de nombreux sites, la poursuite de la navigation vaut acceptation implicite de l'installation des cookies.

De plus, les achats, effectués dans un magasin ou une chaîne de magasins où le client dispose d'une carte de fidélité, sont systématiquement enregistrés et peuvent être utilisés pour en déduire le profil de l'acheteur et lui suggérer des achats ciblés, sans information préalable du client.

Dans la pratique, et une émission de télévision[807] l'a montré, il est difficile à un individu de savoir qu'il fait l'objet d'un traitement automatique de ces données, d'autant plus que les sociétés qui constituent ces fichiers peuvent le faire hors de toute légalité[808] et parfois utilisent un numéro d'autorisation de la CNIL non détenu par elles-mêmes[809].

---

[805] Pierre Bellanger, « Les données personnelles : une question de souveraineté », *Le Débat*, 2015/1 (n° 183), pp. 14-25. URL : https://www.cairn.info/revue-le-debat-2015-1-page-14.htm consulté le 27 décembre 2017.

[806] Yann Algan, Maya Bacache-Beauvallet, Anne Perrot, « Administration numérique », *Notes du conseil d'analyse économique*, 2016/7 (n° 34), pp. 1-12. URL : https://www.cairn.info/revue-notes-du-conseil-d-analyse-economique-2016-7-page-1.htm consulté le 27 décembre 2017.

[807] CASH Investigation du mardi 6 octobre 2015, diffusée par France 2.

[808] L'affaire Cambridge Analytica dévoilée en mars 2018, porte sur plus de 87 millions d'utilisateurs de Facebook dont les données personnelles ont été détournées et utilisées pour influencer les électeurs américains. Une société peut utiliser des données personnelles hors de tout contrôle des utilisateurs dans un but étranger à l'objet de la collecte. Cette pratique, illicite en Union européenne au titre de la directive 95/46/CE l'est également au titre de Règlement général sur la protection des données qui nécessite le consentement explicite de la personne pour tout traitement autre que celui initialement prévu (Le Monde.fr avec AFP, « Cambridge Analytica : 2,7 millions d'utilisateurs européens de Facebook pourraient être concernés », *LeMonde.fr*, 6 avril 2018, URL : http://www.lemonde.fr/pixels/article/2018/04/06/cambridge-analytica-2-7-millions-d-utilisateurs-europeens-de-facebook-pourraient-etre-concernes_5281717_4408996.html consulté le 6 avril 2018).

[809] Démontré dans la même émission de CASH Investigation.

b) Le droit d'opposition

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier[810]. Toute personne peut refuser, sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection, en particulier commerciale.

Ce droit d'opposition ne peut être utilisé que si la personne a connaissance de cette possibilité d'utilisation commerciale, en a conscience et connaît le moyen de faire jouer ce droit d'opposition. Depuis septembre 2011, le ministère de l'Intérieur peut vendre à des fins de prospection commerciale le contenu du fichier national des cartes grises - le système d'immatriculation des véhicules (SIV) - à des sociétés agréées qui obtiennent une licence[811]. Cette possibilité est rétroactive et concerne aussi les véhicules immatriculés avant cette date, sans que leurs propriétaires aient conscience de cette nouvelle possibilité. Concrètement, une entreprise peut acheter des informations concernant les propriétaires de tel type ou telle marque de véhicule. L'adresse étant fournie en prime, les services de marketing n'ont plus ensuite qu'à expédier tantôt une offre sur des pneus, tantôt un rabais sur des rétroviseurs avec l'envoi du nouveau catalogue des futurs modèles de la marque. Depuis 2009, le conducteur est censé être informé. La demande de certificat d'immatriculation d'un véhicule comporte en effet un encadré spécifique. Il n'est à remplir que si le conducteur s'oppose « à la réutilisation de ses données personnelles à des fins de prospection commerciale ». Selon le Ministère de l'Intérieur, 52 % des automobilistes se sont opposés à cette réutilisation. Or depuis la mise en place du SIV, les demandes de carte grise sont réalisées via des entreprises agréées, de nombreux acheteurs de véhicules automobiles ignorent la possibilité de s'opposer à cet usage de prospection et donc ne font pas jouer leur droit d'opposition, celui-ci étant délégué implicitement à l'intermédiaire agréé[812]. Cette opposition devant être exprimée (*opt-out*), plusieurs organismes réclament plutôt un système d'adhésion (*opt-in*) explicite. Avec l'introduction du consentement dans le règlement général sur la protection des données, le système de l'adhésion devrait être généralisé.

---

[810] Loi n° 78-17, Article 38.

[811] Arrêté du 1er septembre 2009 *portant création d'un traitement automatisé de données à caractère personnel dénommé « Système d'information décisionnel du système d'immatriculation des véhicules »* publié au JORF du 22 septembre 2009.

[812] Angélique Négroni, « Le juteux business du fichier des cartes grises », 16 février 2012, *Le Figaro.fr,* URL : http://www.lefigaro.fr/actualite-france/2012/02/15/01016-20120215ARTFIG00570-le-juteux-business-du-fichier-des-cartes-grises.php consulté le 27 décembre 2017.

En principe, toute personne peut décider elle-même de l'utilisation de données la concernant. En ce sens, elle peut refuser d'apparaître dans certains fichiers ou de voir communiquer des informations sur elles à des tiers. Ce droit d'opposition est actuellement difficilement mis en œuvre faute d'information suffisante, le Règlement général sur la protection des données peut y pallier en imposant le principe du consentement et en créant un droit de rétractation par dénonciation de ce consentement. Mais cette rétractation ne rend pas illicites les traitements déjà effectués et pour lesquels le consentement avait été accordé.

c) Le droit d'accès

Toute personne justifiant de son identité a le droit d'interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication[813]. Toute personne peut prendre connaissance de l'intégralité des données la concernant et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction. Toute personne est en droit d'obtenir des explications sur le procédé informatique qui a contribué à produire une décision la concernant (*scoring*, segmentation, profil, …).

Mais si un responsable de traitement estime qu'une demande est manifestement abusive, il peut ne pas y donner suite[814]. Toutefois si l'affaire est portée devant un juge il devra apporter la preuve du caractère manifestement abusif de la demande en cause. Le droit d'accès ne s'exerce pas lorsque les données sont conservées sous une forme ne présentant aucun risque d'atteinte à la vie privée et pendant une durée n'excédant pas celle nécessaire à l'établissement de statistiques ou à la recherche scientifique ou historique. L'exercice du droit d'accès ne doit pas porter atteinte au droit d'auteur.

Dans certains cas, le droit d'accès peut être indirect[815]. Le droit d'accès indirect est une procédure spécifique qui concerne : les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique (fichiers de police judiciaire, fichiers des services de l'information générale - « ex renseignements généraux » -, fichiers de renseignement de la direction générale de la sécurité extérieure, fichier Schengen), certains fichiers du ministère de la Justice (fichier des détenus dans les prisons). Dans ce cas, la Commission de l'informatique et des libertés est l'interlocuteur de la personne qui souhaite faire jouer son droit d'accès pour ces fichiers. La

[813] Loi nº 78-17, Article 39.
[814] Même article, II.
[815] Loi n° 78-17, art. 41.

CNIL ne gère pas les fichiers concernés et n'a donc pas connaissance des personnes qui y figurent. Un magistrat de la Commission exerce le droit d'accès et de rectification pour le compte de la personne sollicitant son droit d'accès. Il peut demander à ce que les informations incomplètes, obsolètes ou non conformes aux textes régissant le fonctionnement des fichiers en cause soient complétées, mises à jour ou supprimées.

d) Le droit de rectification

Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations qui la concernent lorsque sont décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite[816]. Le droit de rectification constitue un complément essentiel du droit d'accès. Lorsque des modifications sont apportées aux données concernant une personne qui a exercé son droit de rectification, le responsable du traitement doit justifier, sans frais pour la personne qui en a fait la demande, des opérations qu'il a effectuées.

Les héritiers d'une personne décédée peuvent exiger que le responsable d'un traitement comportant des données concernant le défunt prenne en considération le décès et procède aux mises à jour. Alors que le régime des données relatives à une personne décédée n'était pas prévu par la législation[817], la loi pour une République numérique[818] et le Règlement général sur la protection des données[819] ont modifié ce régime, créant ainsi une mort numérique[820].

e) Le droit à l'effacement

Ce droit a d'abord été introduit par les juges de la Cour de justice de l'Union européenne sous la forme d'un droit au déréférencement[821]. Ce droit permet à une personne physique de

[816] Loi nº 78-17, art. 40

[817] Fiorenza Gamba, « Rituels postmodernes d'immortalité : les cimetières virtuels comme technologie de la mémoire vivante », *Sociétés*, 2007/3 (n° 97), pp. 109-123. URL : https://www.cairn.info/revue-societes-2007-3-page-109.htm consulté le 27 décembre 2017.

[818] Loi n° 2016-1321, Art. 40-1.

[819] Le considérant nº 27 renvoie aux règles édictées par les Etats concernant les données à caractère personnel des personnes décédées.

[820] Cf. Partie 2. Titre 2. Chapitre 1. Section 1. Sous-section 2. § 1 -B) Le droit à l'oubli des personnes décédées ou la mort numérique.

[821] Cour de justice de l'Union européenne, Arrêt de la Cour (grande chambre) du 13 mai 2014, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, Demande de décision préjudicielle, introduite par l'Audiencia Nacional.

demander à un moteur de recherche de supprimer les liens vers un site qui présente une information pouvant porter indûment atteinte à l'honneur ou l'image de la personne.

Ce droit a été complété par l'introduction d'un droit à l'effacement pour les jeunes adultes ayant autorisé la collecte ou publié des informations ou des images pouvant nuire à leur réputation lorsqu'ils étaient mineurs[822]. Le droit à l'effacement, ou « droit à l'oubli », est défini par le Règlement général sur la protection des données[823]. Ce droit à l'effacement s'applique : si la personne concernée retire son consentement ; si les données ont fait l'objet d'un traitement illicite ; pour respecter une obligation légale ; si la personne concernée s'oppose au traitement sans qu'il existe un besoin impérieux d'effectuer ce traitement.

Mais tous ces droits ne peuvent être exercés que si la personne concernée est informée. Or, certains traitements restent illicites et non déclarés, ou aucune information n'est fournie lors de la collecte des informations, malgré l'obligation légale. L'efficacité de ces droits dans la protection des données personnelles des personnes physiques s'en trouve, de ce fait, réduite[824].

3) Les plaintes auprès de la CNIL et les sanctions

La personne physique qui se voit refuser l'accès aux informations ou à leur correction peut saisir la Commission de l'informatique et des libertés ou le juge des référés en cas de risque de dissimulation ou de disparition des données[825]. La Commission de l'informatique et des libertés peut : intervenir auprès du responsable de fichier ; contrôler sur place les organismes qui exploitent des données personnelles ; prononcer des sanctions ; dénoncer à la Justice des infractions graves. En 2010, la Commission de l'informatique et des libertés a reçu un nombre record de plaintes (4 821) pour non-respect de la loi « Informatique et Libertés ». Ce chiffre représente une hausse de 13 % par rapport à 2009[826]. Aucune étude n'analyse les raisons objectives de cette augmentation : meilleure information du public, augmentation effective des traitements contentieux.

---

[822] Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, article 63.

[823] 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),* Article 17.

[824] Yves Poullet, « La loi des données à caractère personnel :. un enjeu fondamental pour nos sociétés et nos démocraties ? », *LEGICOM*, 2009/1 (N° 42), pp. 47-69. URL : https://www.cairn.info/revue-legicom-2009-1-page-47.htm consulté le 27 décembre 2017.

[825] Loi nº 78-17, Art. 39.

[826] CNIL, Rapport d'activité 2010, p. 14.

Les sanctions possibles, en cas de non-respect des obligations liées à la loi, sont soit des sanctions administratives, soit des sanctions pénales. Les sanctions administratives du ressort et de la compétence de la Commission de l'informatique et des libertés sont des sanctions pécuniaires ou une injonction de cesser le traitement ou un retrait de l'autorisation accordée[827]. Le montant de la sanction pécuniaire est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement, mais elles restent symboliques face aux sommes retirées de l'exploitation de ces données par les responsables de ces traitements litigieux. Avant la promulgation de la loi n° 2016-1321 pour une République numérique, lors du premier manquement, il ne pouvait excéder 150 000 €. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, son montant maximal était de 300 000 € ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 €[828]. La loi pour une République numérique, anticipant le Règlement général sur la protection des données a porté le montant maximum de la sanction pécuniaire à 3 millions d'Euros[829]. La Commission de l'informatique et des libertés peut préférer à la sanction une publication de son avertissement, ce qui peut être plus dissuasif qu'une sanction pécuniaire sans publicité.

Les sanctions pénales pour traitement de données illicites, frauduleux, ou portant atteinte à la considération ou à l'intimité d'une personne physique, sont prévues et réprimées par les articles 226-16 à 226-24 du Code pénal (peine d'emprisonnement de cinq ans et amende de 300 000 €). Si une sanction pécuniaire administrative a été rendue définitive avant le jugement pénal, le juge peut décider de déduire du montant de l'amende la sanction pécuniaire[830]. En 2010, la Commission de l'informatique et des libertés a prononcé 11 sanctions (interruption de traitement, sanction pécuniaire, etc.)[831].

Mais, une limite aux poursuites existe[832], les pouvoirs de la CNIL, prévus pour le contrôle de la mise en œuvre des traitements, ainsi que les sanctions administratives, ne peuvent être exercés qu'à « *l'égard des traitements dont les opérations sont mises en œuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre État membre de la Communauté européenne* ». Ainsi, les traitements

[827] Loi nº 78-17, Article 45.
[828] Loi nº 78-17, Article 47.
[829] Même article après modification par la loi n° 2016-1321 du 7 octobre 2016.
[830] Loi n° 78-17 art. 47.
[831] CNIL, Rapport d'activité 2010, p. 58.
[832] Loi nº 78-17, Article 48.

effectués hors du territoire de l'Union européenne échappent au pouvoir de la CNIL, Google, Facebook et autres sites mondiaux restent en dehors de la protection mise en place sur le territoire de l'Union européenne. Toutefois, le 17 mars 2011, la CNIL a prononcé à l'encontre de Google une première amende de 100 000 € pour collecte des informations concernant les points d'accès Wi-Fi par le biais des « Google cars ». De nouveau, le 3 janvier 2014, la CNIL a prononcé une nouvelle sanction de 150 000 € à l'encontre de la société Google Inc.[833] pour non-respect par les règles de confidentialité mises en œuvre depuis le 1er mars 2012 de la loi informatique et liberté. Cette sanction est assortie d'une obligation de publication de cette décision sur la page d'accueil de Google.fr. Après que le Conseil d'État ait rejeté la requête de Google faisant appel de cette publication, Google a publié pendant un week-end cette décision, mais poursuit son recours sur le fond auprès du Conseil d'État. Comparées au chiffre d'affaires annuel de Google qui se mesure en dizaine de milliards de dollars, les amendes infligées par la CNIL restent non dissuasives. Le Règlement général sur la protection des données prévoit des amendes plus dissuasives proportionnelles au chiffre d'affaires annuel des sociétés[834] et permet de poursuivre les responsables d'un traitement effectué sur le territoire de l'Union européenne ou dès que ce traitement concerne une offre de biens ou de services destinée à des personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou au suivi du comportement de ces personnes[835].

Depuis le 1er octobre 2015[836], la Cour de justice de l'Union européenne a précisé les conditions dans lesquelles une disposition légale nationale pouvait être applicable à une société étrangère exerçant dans un État membre. Dans son arrêt, la Cour rappelle que « *chaque État membre doit appliquer les dispositions qu'il a adoptées en vertu de la directive [95/46 CE], dès lors que le traitement de données est effectué dans le cadre des activités menées sur son territoire par un établissement du responsable du traitement* ». La Cour précise que la présence d'un seul représentant stable est suffisante pour constituer un établissement et que la notion d'établissement s'étend à toute activité réelle et effective exercée au moyen d'une installation stable. Mais la Cour ajoute qu'au cas où aucun établissement stable n'existe, il appartient à

[833] At http://www.cnil.fr/linstitution/actualite/article/article/la-formation-restreinte-de-la-cnil-prononce-une-sanction-pecuniaire-de-150000-EUR-a-lencontre/ publié le 8 janvier 2014.
[834] L'article 81 du RGPD prévoit des amendes administratives pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu. Ces chiffres pouvant être doublés en cas de non-respect d'une injonction émise par une autorité de contrôle.
[835] Règlement général sur la protection des données, art. 3.
[836] Cour de justice de l'Union européenne, 3ème Chambre, Arrêt du 1er octobre 2015, affaire C-230/14 *Weltimmo.*

l'autorité de contrôle d'un État de demander à l'autorité de contrôle de l'autre État membre de constater l'éventuelle infraction au droit de cet État et d'imposer les sanctions prévues par ce droit. La Cour a ainsi interprété dans un sens non restrictif la limite territoriale de l'action des autorités de contrôle et rappelé l'obligation de poursuite et de sanction existant dans l'État membre abritant l'établissement du responsable de traitement[837].

Le Règlement général sur la protection des données abrogeant la directive 95/46/CE tente de pallier cette impunité extraterritoriale et à lier le montant des pénalités à un pourcentage du chiffre d'affaires annuel de la société, mesure qui deviendrait ainsi plus contraignante. La protection des personnes physiques dans la société numérique s'enrichit des évolutions techniques et sociétales apparues en fin du XX^{e} siècle.

B) La protection dans une société numérique mature et omniprésente

Depuis le début du XXI^{e} siècle, la société est pleinement devenue numérique et de nouvelles lois sont venues protéger les personnes physiques dans ce nouvel environnement. Ce sont la loi de transposition de la directive 95/46/CE[838] qui a réécrit la loi n^{o} 78-17, la loi pour la confiance dans l'économie numérique[839] déjà évoquée pour la modification de la loi sur la presse de 1881, la loi pour une République numérique[840] et la loi relative à l'égalité et la citoyenneté[841], également évoquée pour son durcissement sur la répression des discriminations et du racisme.

1) L'assouplissement de la loi informatique et libertés

Ces lois prennent en compte la progression du numérique et son omniprésence dans la société.

[837] Mais comme le constate la Commission nationale de l'informatique et des libertés dans l'avis du 30 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)), elle souligne « *les difficultés opérationnelles qui pourraient naître avec les pays ayant retenu des critères différents et incompatibles avec ceux retenus par le projet de loi* » et autorisés par les marges de manœuvre des États membres..

[838] Loi n^{o} 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^{o} 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, publiée au JORF n^{o} 182 du 7 août 2004 p. 14063.

[839] Loi n^{o} 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique*, publiée au JORF n^{o} 0143 du 22 juin 2004 p. 11168.

[840] Loi n^{o} 2016-1 321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF n^{o} 0235 du 8 octobre 2016.

[841] Loi n^{o} 2017-86 du 27 janvier 2017 *relative à l'égalité et à la citoyenneté*, publiée au JORF n^{o} 0024 du 28 janvier 2017.

Mais il arrive que certaines protections des personnes physiques soient atténuées par les nouvelles dispositions. Ainsi le texte initial de la loi nº 78-17 stipule dans son article 15 qu'en cas d'avis non conforme de la Commission de l'informatique et des libertés concernant un traitement automatique de données à caractère personnel prévu pour le compte de l'État, d'un établissement public ou d'une communauté territoriale, ce traitement doit être approuvé par un décret pris sur avis conforme du Conseil d'État[842]. L'article 26 de la loi modifiée pour la transposition de la directive 95/46/CE atténue cette disposition puisque les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique, ainsi que ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté sont autorisés par arrêté du ou des ministres compétents en annexant l'avis de la CNIL qu'il soit favorable ou défavorable. L'avis conforme du Conseil d'État n'est plus requis. Seuls les traitements portant sur les données raciales, ethniques, d'opinion ou syndicales nécessitent un décret en Conseil d'État[843]. Il en est de même pour les traitements de données qui contiennent le numéro d'identification national des personnes physiques ou NIR, ce numéro à l'origine de la loi informatique et libertés. En novembre 1998, un amendement à la loi de finances 1999 permet à l'administration fiscale d'utiliser le NIR et d'échanger des informations avec les organismes sociaux afin de pouvoir vérifier les déclarations de revenus. Cette possibilité a été acceptée par le Conseil constitutionnel avec des réserves d'interprétation[844] quant à l'utilisation et la transmission de ce NIR. La lutte contre la fraude fiscale remet ainsi en cause partiellement la loi de 1978, vingt-cinq ans après, portant ainsi atteinte aux libertés individuelles. Les échanges entre l'INSEE et l'administration fiscale sont entérinés par la Commission de l'informatique et des libertés en

[842] Loi nº 78-17, Article 15 : « *Hormis les cas où ils doivent être autorisés par la loi, les traitements automatisés d'informations nominatives opérés pour le compte de l'État, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par une loi ou par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés.*
« Si l'avis de la commission est défavorable, il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'État ou, s'agissant d'une collectivité territoriale, en vertu d'une décision de son organe délibérant approuvée par décret sur avis conforme du Conseil d'État ».
[843] Loi n° 78-17, Article 26.
[844] Conseil constitutionnel, Décision nº 98-405 DC du 29 décembre 1998, *Loi de finances pour 1999*.

2007[845]. Pour la Cour de justice de l'Union européenne, cet échange d'informations personnelles entre administrations doit être réalisé après information des intéressés[846].
Si la loi n° 78-17 est assouplie pour l'État et l'administration, de nouveaux droits apparaissent pour les individus.

2) L'affirmation de nouveaux droits individuels

La loi pour la confiance dans l'économie numérique se contente de définir techniquement la notion de courrier électronique, sans affecter le régime de la correspondance privée laissant à l'autorité judiciaire le soin de se prononcer sur la qualification de correspondance privée de ce courrier électronique[847], donc de sa protection. D'outil technique, le courrier électronique est devenu un outil de communication omniprésent[848]. Il remplace le courrier traditionnel pour les échanges tant scientifiques ou professionnels que privés[849]. Le courrier privé reste protégé contre les interceptions, tandis que le courrier professionnel peut être lu par une autre personne de l'entreprise[850].
La loi pour une République numérique[851] crée de nouveaux droits pour les personnes physiques : l'affirmation du principe de la maîtrise par l'individu de ses données personnelles ; le droit à l'oubli pour les mineurs ; la possibilité d'organiser le sort de ses données personnelles

[845] CNIL, Délibération nº 2007-216 du 10 juillet 2007 *autorisant la mise en œuvre, par le ministère de l'économie, des finances et de l'industrie, d'un traitement automatisé de données à caractère personnel ayant pour objet l'identification des contribuables dénommé « PERS »* (demande d'avis nº 1168820), en ligne à https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=F2EF68872778CE3C541DFCB26F5E500D.tpdila15v_1?cidTexte=JORFTEXT000018008615&idArticle=&categorieLien=id, consulté le 6 mars 2017.
[846] Cour de justice de l'Union européenne, Arrêt de la Cour (troisième chambre) du 1er octobre 2015, Affaire C-201/14 *Smaranda Bara e.a. c/ Preşedintele Casei Naţionale de Asigurări de Sănătate e.a. : « Les articles 10, 11 et 13 de la 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, doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales, telles que celles en cause au principal, qui permettent à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement ».*
[847] Conseil constitutionnel, Décision nº 2004-496 du 10 juin 2004, *Loi pour la confiance dans l'économie numérique*.
[848] Emmanuel Cauvin, « Courrier électronique », *Médium*, 2009/1 (N°18), pp. 50-59. URL : https://www.cairn.info/revue-medium-2009-1-page-50.htm consulté le 28 décembre 2017.
[849] Aleida Assmann, « De la correspondance épistolaire au courrier électronique », *Esprit*, 2006/5 (Mai), pp. 128-130. URL : https://www.cairn.info/revue-esprit-2006-5-page-128.htm consulté le 28 décembre 2017.
[850] Voir Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 2. L'inviolabilité des correspondances et des communications
[851] Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF nº 0235 du 8 octobre 2016.

après la mort et la possibilité d'exercer ses droits par voie électronique. L'introduction de ces droits dans la loi nº 78-17 permet de les rendre effectifs avant que le règlement de protection des données personnelles qui les y incorpore ne soit applicable. La maîtrise par l'individu de ses données personnelles est introduite dès l'article 1er de la loi nº 78-17, article qui n'avait pas été modifié depuis la première publication de la loi. Le droit à l'oubli pour les mineurs permet à toute personne physique de demander la suppression de données problématiques présentes sur une plateforme, si celles-ci ont été collectées alors qu'elle était mineure. De son vivant, toute personne physique peut demander que les données personnelles la concernant soient détruites ou conservées après sa mort en désignant une personne de confiance chargée de ces actes, à défaut les héritiers bénéficient de certains droits : droit d'accès et droit d'opposition.

§ 2 - La protection de la vie privée au niveau européen et international

La protection de la vie privée a pour corollaire la protection des données à caractère personnel. Si la France a été un des premiers États à légiférer sur la protection des données personnelles[852] et l'intrusion dans les systèmes de traitement automatique des données (STAD)[853], d'autres États se sont dotés d'une telle protection, et au niveau européen, le Conseil européen a publié la Convention nº 108[854], l'Union européenne a harmonisé la législation européenne des États membres par la publication d'une directive en 1995[855] et un règlement abrogeant cette directive en mai 2017[856]. L'article 8 de la Convention européenne des droits de l'homme[857] protège la vie privée des personnes. La Charte des droits fondamentaux[858] consacre également dans son

[852] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés.*
[853] Loi nº 88-19 du 5 janvier 1988*, relative à la fraude informatique.*
[854] Conseil de l'Europe, traité nº 108, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 janvier 1981.
[855] 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.*
[856] 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).*
[857] Conseil de l'Europe, *Convention de sauvegarde des droits de l'homme et des libertés fondamentales,* Rome, 4 novembre 1950.
[858] Charte des droits fondamentaux de l'Union européenne (2000/C 364/01) du 18 décembre 2000, Article 8. « *Protection des données à caractère personnel.*
« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

article 8 le droit d'une personne à la protection des données comme un droit fondamental. Avant la signature du traité de Lisbonne[859] qui intègre la Charte, il n'existait pas de proclamation générale du droit à la protection de ses données personnelles[860]. Grâce à cet article 8, l'individu se retrouve au centre du dispositif. Ce droit est consacré dans le règlement européen[861] qui reconnaît le droit à l'autodétermination informationnelle, notion reconnue initialement par la Cour constitutionnelle fédérale de l'Allemagne en décembre 1983. Ce droit est reconnu par la loi pour une République numérique[862], dans son article 54 qui complète l'article 1er de la loi nº 78-17[863] par l'alinéa suivant : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ». Ces textes récents utilisent une notion issue du droit privé : le consentement[864].

A) Un besoin d'harmonisation supranational des législations

Au début des années 80, la multiplication de lois comparables suscite la crainte de certains États de voir les législations sur la protection des données entraver la libre circulation de ces données et les échanges commerciaux dont elles font l'objet. Au niveau international, deux conceptions existent en matière de protection des données personnelles. Le modèle européen est imposé, réglementaire et contraignant. Il est très protecteur et prévoit un contrôle par une entité

« 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 ».

[859] *Traité instituant la Communauté européenne ou Traité de Rome* du 25 mars 1957, devenu le traité sur le fonctionnement de l'Union européenne selon le « traité modificatif » signé le 13 décembre 2007 à Lisbonne, dit traité de Lisbonne.

[860] Anne Débet, « La protection des données personnelles, point de vue du droit privé », *Revue du droit public* nº 1 du 1 janvier 2016, p. 17.

[861] 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).*

[862] Loi nº 2016-1 321 du 7 octobre 2016 pour une République numérique, publiée au JORF nº 0235 du 8 octobre 2016.

[863] Cet article était le seul article non modifié par la loi nº 2004-801 du 6 août 2004 qui avait transposé la directive 95/46/CE en droit français.

[864] Anne Débet, « La protection des données personnelles, point de vue du droit privé », *Revue du droit public* nº 1 du 1 janvier 2016, p. 17. Op. cit..

indépendante. Le modèle nord-américain est fondé sur le pragmatisme, l'autorégulation et la confiance dans la convergence des intérêts individuels[865].

1) Les lignes directrices de l'OCDE

Le 23 septembre 1980, l'OCDE adopte les « *lignes directrices régissant la vie privée et le flux transfrontalières des données à caractère personnel* » pour « *favoriser la libre circulation de l'information entre les pays membres et à éviter la création d'obstacles injustifiés au développement des relations économiques et sociales entre ces pays* ». Ces lignes directrices énoncent plusieurs principes : principe de la limitation en matière de collecte des données à caractère personnel obtenues par des moyens licites après information et avec le consentement de la personne concernée ; principe de la limitation de l'utilisation de ces données non divulguées ni utilisées sans le consentement de la personne concernée ou la permission d'une règle de droit ; principe des garanties de sécurité contre les risques d'accès, d'utilisation ou de divulgation non autorisés de ces données ; principe de la participation individuelle permettant à toute personne d'obtenir du maître du fichier confirmation de la détention ou non de ces données et de se les faire communiquer et d'en obtenir l'effacement, la rectification ou la correction ; principe de la responsabilité du maître de fichier du respect de ces principes.
C'est la Convention n° 108 qui établit le premier cadre international sur la protection des données personnelles[866].

2) La Convention nº 108

Adopté par le Conseil de l'Europe le 28 janvier 1981, le traité nº 108 intitulé « *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* » est plus connu sous le nom de « Convention nº 108 ». Le résumé de la Convention est disponible sur le site du Conseil de l'Europe[867] : « *La Convention est le premier instrument international contraignant qui a pour objet de protéger les personnes contre l'usage abusif du*

[865] Stéphane Tijardovic, « La protection juridique des données personnelles. Vers une nécessaire adaptation de la norme juridique aux évolutions du monde numérique », *Les Cahiers du numérique*, 2003/3 (Vol. 4), pp. 185-203. URL : https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-185.htm consulté le 28 décembre 2017.
[866] Ibid.
[867] http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108, consulté le 6 mars 2017.

traitement automatisé des données à caractère personnel, et qui réglemente les flux transfrontaliers des données.

« Outre des garanties prévues en ce qui concerne le traitement automatisé des données à caractère personnel, elle proscrit le traitement des données "sensibles" relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle, aux condamnations pénales, etc., en l'absence de garanties offertes par le droit interne. La Convention garantit également le droit des personnes concernées de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications.

« Seule restriction à ce droit : lorsque les intérêts majeurs de l'État (sécurité publique, défense, etc.) sont en jeu.

« La Convention impose également des restrictions aux flux transfrontaliers de données dans les États où n'existe aucune protection équivalente ».

Le traité a été ratifié par 51 États[868]. Cette convention consacre les principes énoncés par la loi nº 78-17 : collecte des données loyale et proportionnée au but déclaré ; restrictions concernant des données sensibles ; sécurité des enregistrements ; droit de consultation, modification et effacement en cas de collectes non conformes ; sanctions en cas de violation des règles ; flux transfrontaliers de données soumis à une protection équivalente dans l'État de destination. Elle est applicable depuis le 1er octobre 1985 et dès son préambule, elle évoque « *la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples* ».

Une révision de la convention est en cours, cette révision prend en compte les nouveaux risques apparus en 30 ans et harmonise certaines définitions et concepts avec la directive 95/46/CE[869] : le concept de « fichier automatisé » est remplacé par la notion de « traitement de données », effaçant toute connotation technologique ; le « maître du fichier » devient le « responsable de traitement » et la notion de sous-traitant apparaît ; le texte révisé utilise la notion de « juridiction » d'un État en lieu et place de « territoire ». Le préambule mentionne expressément

[868] Dont 9 États non membres du Conseil de l'Europe (source Conseil de l'Europe, « Etat des signatures et ratifications du traité 108, Situation au 16/03/2018 », disponible à https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=pSG7TTpG consulté le 16 mars 2018).

[869] Cécile De Terwangne, « La réforme de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », in *Quelle protection des données personnelles en Europe ?* Larcier Bruxelles, 2015. pp. 81-120. URL : http://www.crid.be/pdf/public/7635.pdf consulté le 16 mars 2018.

le droit à l'autonomie personnelle, le droit de chacun de contrôler ses propres données à caractère personnel[870].

Deux points de vue coexistent, points de vue compatibles, mais correspondant néanmoins à deux sensibilités différentes : tandis que les droits allemands, français ou suédois font de la protection de l'individu face aux dangers de l'informatique une fin en soi, le droit international et le droit européen font de cette protection la contrepartie du principe de libre circulation de l'information.

B) La directive nº 95/46/CE et sa transposition

Le 24 octobre 1995, l'Union européenne adopte la directive nº 95/46/CE[871] 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. Cette directive tend à assurer un niveau de protection harmonisé entre les États membres. Après transposition de cette directive, tous les États membres disposent d'une loi « informatique et liberté » ainsi que d'une autorité de contrôle indépendante. Régulièrement, ces autorités indépendantes se réunissent à Bruxelles aux fins d'harmonisation de leurs pratiques ou recommandations au sein d'une instance qui se prononce par des avis destinés à la Commission européenne et qui rend public un rapport annuel d'activité. Cette instance qui ne représente pas les gouvernements des États membres, mais leur autorité de contrôle est appelée « le groupe de l'article 29 » ou G29, par référence à l'article de la directive européenne qui l'institut[872].

Avec les progrès de la technologie informatique et l'évolution des réseaux de télécommunications, les systèmes de traitement automatisé de données à caractère personnel sont de plus en plus utilisés dans la vie quotidienne des citoyens européens. Pour s'inscrire à la bibliothèque ou au club de gymnastique, ouvrir un compte bancaire ou un dossier médical, faire des achats avec sa carte de crédit en magasin ou sur Internet, le citoyen européen doit communiquer des informations personnelles nominatives à caractère privé, telles que son nom,

---

[870] « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [STE n° 108] – Projet de rapport explicatif », 2 juin 2016, p.5. URL : https://rm.coe.int/16806b11a4 consulté le 15 mars 2018.

[871] 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,* publié au Journal officiel L 281 du 23.11.1995, p. 31.

[872] L'article 68 du Règlement général sur la sécurité des données institue le Comité européen de la protection des données en tant qu'organe de l'Union avec une personnalité juridique. Ce Comité remplace le G29.

son prénom, son adresse, son numéro de téléphone, de compte bancaire ou sa photographie. En facilitant la dissémination de ces données, ces nouveaux systèmes informatiques ont, par la même occasion, augmenté les risques de leur exploitation abusive et illégale. Afin de remédier à ce problème, les pays de l'Union européenne ont adopté des législations nationales et communautaires visant à assurer la protection des données relatives à la vie privée des citoyens européens.

Une directive du 15 décembre 1997[873] prévoit le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Elle sera suivie par une nouvelle directive le 12 juillet 2002[874] relative au traitement des données à caractère personnel dans le secteur des communications électroniques. Cette nouvelle directive abroge la directive de décembre 1997.

1) Le traitement des données à caractère personnel au sein de l'Union européenne

Pendant longtemps, les niveaux de protection des données personnelles entre les pays européens étaient très différents. Ces différences législatives constituaient des risques supplémentaires à la diffusion malhonnête de données personnelles, les « organismes malfaisants » ayant la possibilité de se déplacer vers des zones géographiques n'accordant peu ou presque pas de protection aux renseignements personnels.

En 1995, le Parlement européen et le Conseil européen ont adopté une Directive communautaire 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 au sein de l'Union européenne » (Directive 95/46/CE), visant à harmoniser les différents systèmes européens. Cette directive constitue aujourd'hui le texte de référence, au niveau européen, en matière de protection des données à caractère personnel. Elle a notamment permis et permet toujours aux pays candidats à l'adhésion à l'Union européenne d'adapter leur législation à celles des pays où la protection

[873] Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications* publiée au Journal officiel n° L 024 du 30/01/1998 pp. 1-8.

[874] 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)* publiée au Journal officiel n° L 201 du 31/07/2002 pp. 37-47.

des données personnelles avait été développée depuis plus longtemps. La directive 95/46/CE exige, entre autres, que chaque État membre prévoie la création d'une ou de plusieurs autorités publiques indépendantes, chargées de surveiller l'application, sur son territoire, des dispositions relatives à la protection des données personnelles. Depuis l'entrée en vigueur de la directive, plusieurs pays européens ont pu renforcer leur législation relative à la protection des données personnelles et créer des autorités de régulation nationale « gardiennes des libertés fondamentales ». Ainsi, en Pologne par exemple[875], pays où les organes publics avaient pris l'habitude à l'époque communiste d'abuser de leur pouvoir et de leurs compétences, la transposition de la directive européenne a permis d'instaurer un nouveau système relatif à la protection des données permettant de contrôler ces organes.

L'Union européenne face à l'informatisation toujours croissante de nos sociétés continue à développer une stratégie commune de sécurité pour la protection des données à caractère personnel. Récemment, en 2002, une nouvelle directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive 2002/58/CE : « vie privée et communications électroniques ») a été adoptée. Cette directive régit notamment le transfert de données à caractère personnel de l'Union européenne vers des pays tiers. Elle définit de nouvelles clauses contractuelles types que les entreprises peuvent utiliser pour assurer des garanties adéquates dans leurs échanges de données avec des pays tiers.

Depuis 2014, la Cour de justice de l'Union européenne s'appuie sur une interprétation large de la directive 95/46 CE pour ses arrêts concernant le « droit au déréférencement »[876], la compétence d'un État membre[877] ou l'échange de données administratives[878].

[875] Éric Salvat, « *Digital Single Market* : le point de vue d'une entreprise polonaise de récolte et d'analyse de données personnelles de consommateurs de pays d'Europe centrale », *Annales des Mines - Réalités industrielles*, 2016/3 (Août 2016), pp. 8-12. URL : https://www.cairn.info/revue-realites-industrielles-2016-3-page-8.htm consulté le 5 avril 2018.
[876] Cour de Justice de l'Union Européenne Arrêt du 13 mai 2014, affaire C-131/12 *Google Spain SL et Google Inc. v Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*.
[877] Cour de Justice de l'Union Européenne, Arrêt du 1er octobre 2015, affaire C-230/14 *Weltimmo*.
[878] Cour de Justice de l'Union Européenne, Arrêt du 1er octobre 2015, affaire C-201/14 *Bara e. a.*

2) La transposition de la directive nº95/46/CE dans les États membres

En 1995, certains États membres s'étaient dotés d'une législation propre pour protéger le traitement des données personnelles. Aussi, en ce qui concerne la mise en œuvre de la directive[879], la première série de pays qui l'appliquèrent fut la Grèce (Loi nº 2472 sur la protection des personnes à l'égard du traitement des données à caractère personnel en 1997) et l'Italie (Loi nº 675 sur la protection des données personnelles[880] en 1996, modifiée par plusieurs décrets législatifs en 1997, 1998 et 1999) avec une transposition de la directive dans son intégralité. Dans une deuxième série, ce seront l'Espagne (Loi organique de protection des données à caractère personnel[881] en 1999 après une loi du 29 octobre 1992 réglementant le traitement automatisé de données personnelles), le Portugal (Loi nº67/98 relative à la protection des données à caractère personnel[882] en 1998 après la loi nº 10/91 du 29 avril 1991 sur la protection des données à caractère personnel face à l'informatique, amendée par une loi du 29 août 1994), la Finlande (Loi de protection des données personnelles[883] en 1999 après la loi du 30 avril 1987 sur les fichiers de données à caractère personnel, modifiée par une loi du 7 avril 1995 concernant la police), la Suède (Loi nº 98/204 sur la protection des données[884] en 1998 après la loi du 11 mai 1973 sur la protection des données) et le Royaume-Uni (Loi de protection des données[885] en 1998 après la loi sur la protection des données du 12 juillet 1988), ces pays ayant complété une loi existante pour la transposition de la directive. Dans les autres pays, des études et des mesures de transposition de la directive devant les Parlements nationaux ont été prises. En janvier 2000, la France, le Luxembourg, les Pays-Bas, l'Allemagne et l'Irlande n'avaient pas transposé la directive dans leur législation. Le Luxembourg disposait de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, amendée en 1992, et a réalisé la transposition par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel[886]. Cette

[879] Information disponible sur le site de la CNIL, *La protection des données personnelles dans l'Union européenne*, mise à jour le 22 avril 2002, non accessible le 6 mars 2017.
[880] *Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.*
[881] *Ley Organica* 15/99 *de Protección de Datos de Carácter Personal.*
[882] *Lei da protecçao de dados pessoais* nº67/98.
[883] *Personuppgiftslag* 22.4.1999/523.
[884] *Personuppgiftslagen* 1998:204.
[885] *Data Protection Act* 1998.
[886] Loi modifiée du 2 août 2002 *relative à la protection des personnes à l'égard du traitement des données à caractère personnel.*

loi a été modifiée en 2007 puis 2011 pour prendre en compte la protection de la vie privée dans les communications électroniques et modifiant la liberté d'expression dans les médias[887]. Les Pays-Bas disposaient de la loi du 28 décembre 1988 sur la protection des données, complétée par une loi du 21 juin 1990 sur les fichiers de police avant de réaliser une transposition de la directive dans la loi de protection des données[888] de 2001. Cette loi est basée sur l'article 10 paragraphe 2 de la Constitution néerlandaise, article 10 qui protège la vie privée et les données personnelles[889]. L'Allemagne disposait de lois dans les Länder et de la 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, la transposition a été réalisée par la loi fédérale de protection des données en 2001[890]. La loi de transposition ne fait aucune référence explicite à Internet[891]. L'Irlande disposait de la loi sur la protection des données du 13 juillet 1988 et a transposé la directive en 2001[892] avec une entrée en vigueur en avril 2002. La France qui disposait de la loi informatique et libertés de 1978, a transposé la directive par réécriture complète de cette loi en 2004[893]. Cette loi renouvelée permet la régularisation de deux actions : elle permet, d'une part, la transposition de la directive européenne nº 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, et d'autre part, d'adapter la réglementation aux modifications technologiques survenues depuis la loi de 1978 en tenant compte notamment des nouveaux moyens de diffusion de la micro-informatique, à la multiplication des télétransmissions ainsi qu'au développement considérable d'Internet.

---

[887] Commission nationale pour la protection des données, « Droit Luxembourgeois », Grand-Duché de Luxembourg, URL : https://cnpd.public.lu/fr/legislation/droit-lux.html consulté le 16 mars 2018.

[888] *Wet bescherming persoonsgegevens* (WBP) 2001.

[889] « Pays-Bas – Mondialisation et Internet », La Haye, 30 mars 2016, Rapport rédigé par le Cabinet Spiegeler Advocaten BV, sous la supervision de Me Brigitte Spiegeler et de Me Camille Radeau, URL : http://www.henricapitant.org/storage/app/media/pdfs/evenements/mondialisation_internet_2016/Pays-Bas_0.pdf consulté le 16 mars 2018.

[890] *Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001,* dans Bundesgesetzblatt Jahrgang 2001 Teil I Nr. 23, ausgegeben zu Bonn am 22. Mai 2001, pp. 904-928.

[891] « La transposition de la 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 en Droit allemand », Juin 2002, *Juriscope 2002,* URL : http://www.juriscope.org/uploads/etudes/Allemagne/Droit%20adminsitratif_Transposition%20directive%2095-46%2024%2010%2095%20Protection%20pers%20physiques%20a%20l%20egard%20du%20traitement%20des%20donnees_Allemagne_2005.pdf consulté le 16 mars 2008.

[892] *European Communities (Data Protection) Regulations*, 2001.

[893] Loi nº 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* parue au Journal officiel nº182 du 7 août 2004 p. 14063.

Pratiquement, neuf années ont été nécessaires pour une transposition de la directive dans la législation des États membres.

Aujourd'hui, tous les pays membres de l'Union européenne ont transposé dans leur législation cette directive nº 95/46/CE. Les trois pays de l'Espace économique européen, l'Islande, le Liechtenstein et la Norvège, ont également transposé cette directive.

Tenant compte de la difficulté de transposition de la directive, la protection des données à caractère personnel fait l'objet d'un règlement général, ne nécessitant pas de transposition dans le droit des États membres. Un délai de deux ans entre la publication du règlement en 2016 et son application en 2018 permet aux entreprises, aux États et aux organes de contrôle de se préparer et se mettre en conformité avec les nouvelles obligations.

3) La libre circulation des données à caractère personnel

Pour l'Union européenne, la protection des données à caractère personnel doit permettre une libre circulation de ces données sur le territoire de l'Union[894], et sous contrôle, vers d'autres États tiers.

L'Union européenne face à l'informatisation toujours croissante de nos sociétés continue à développer une stratégie commune de sécurité pour la protection des données à caractère personnel. En 2002, une nouvelle directive dite « vie privée et communications électroniques » concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[895] a été adoptée. Cette directive régit notamment le transfert de données à caractère personnel de l'Union européenne vers des pays tiers. Elle définit de nouvelles clauses contractuelles types que les entreprises peuvent utiliser pour assurer des garanties adéquates dans leurs échanges de données avec des pays tiers hors de l'Union européenne. En principe, ces transferts de données à caractère personnel hors du territoire de

[894] Roberto Viola, Olivier Bringer, « Vers un marché unique numérique : faire de la révolution numérique une opportunité pour l'Europe », *Revue d'économie financière*, 2017/1 (n° 125), pp. 239-254. URL : https://www.cairn.info/revue-d-economie-financiere-2017-1-page-239.htm consulté le 28 décembre 2017.

[895] 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)* publiée au Journal officiel nº L 201 du 31/07/2002 pp. 37–47.

l'Union européenne sont interdits[896] à moins que le pays ou le destinataire n'assure un niveau de protection suffisant, dit « adéquat ».

Cette interdiction de transferts ne concerne pas l'Islande, le Liechtenstein et la Norvège, puisque ces pays qui appartiennent à l'Espace économique européen, ont transposé les dispositions de la directive 95/46/CE dans leur législation nationale. De même, cette interdiction ne concerne pas les transferts vers les pays reconnus comme « adéquats » par la Commission européenne, l'Andorre, l'Argentine, le Canada, les îles Féroé, les îles de Man, de Guernesey, de Jersey, Israël, l'Uruguay et la Suisse[897].

Pour les transferts hors de ces pays, plusieurs outils ont été développés pour permettre aux acteurs d'apporter un niveau de protection suffisant[898] : les règles internes d'entreprise (ou BCR, en anglais « *Binding Corporate Rules* »), les Clauses Contractuelles Types (modèles de clauses contractuelles adoptées par la Commission européenne qui permettent d'encadrer les transferts de données personnelles hors de l'Union européenne)[899] et l'adhésion aux principes du « *Safe Harbor* » (ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux États-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne). Cet accord a fait l'objet de critiques dues à la moindre protection des données personnelles sur le territoire américain que dans l'Union européenne.

Rappelant que « *les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales et, en particulier, au droit au respect de la vie privée doivent nécessairement être interprétées à la lumière des droits fondamentaux garantis par la Charte* » dans ses articles 7 et 8, ainsi que l'article 1er de la directive qui garantit une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, la Cour de justice de l'Union européenne a invalidé la décision 2000/520 qui permet le transfert des données vers les sociétés ayant adhéré

[896] Éric Barbry, « Cohérences et incohérences des législations », *Hermès, La Revue*, 2009/1 (n° 53), pp. 145-151. URL : https://www.cairn.info/revue-hermes-la-revue-2009-1-page-145.htm consulté le 15 février 2018.

[897] Il est possible d'obtenir sur le site de la CNIL, une liste des États et leur niveau de protection, à l'URL : https://www.cnil.fr/sites/default/files/atoms/files/niveau_de_protection-fr-jan2015.xls consultée le 28 décembre 2017.

[898] Commission nationale de l'informatique et des libertés, *Transferts de données à caractère personnel vers des pays non membres de l'Union européenne*, juin 2008, URL : http://www.cil.cnrs.fr/CIL/IMG/pdf/Guide-tranfertdedonnees.pdf, consulté le 29 décembre 2017.

[899] Éric Barbry, « Cohérences et incohérences des législations », *Hermès, La Revue*, 2009/1 (n° 53), pp. 145-151. Op. cit.

aux principes du Safe Harbor[900]. Le 1er août 2016, le principe du *Safe Harbor* a été remplacé par le *Privacy Shield*[901] après renégociation entre l'Union européenne et les États-Unis d'Amérique[902].

Outre les transferts autorisés par la directive 95/46/CE, la loi nº 78-17 prévoit également des exceptions permettant de transférer des données vers des pays tiers sans qu'il n'existe pour autant un niveau de protection suffisant[903].

Devant les évolutions de la technique et l'importance des données collectées, l'Union européenne a adopté un nouveau cadre de réglementation de la protection des données personnelles.

C) Un nouveau règlement applicable en 2018 : le règlement général sur la protection des données ou RGPD

Le cadre européen de la protection des données personnelles, mis en place par la directive datant de 1995, est aujourd'hui devenu obsolète, du fait des évolutions technologiques et de l'émergence de nouveaux usages.

La pièce maîtresse de la législation de l'Union européenne en matière de protection des données à caractère personnel, à savoir la directive 95/46/CE, a été adoptée en 1995 avec deux objectifs : protéger le droit fondamental à la protection des données et garantir la libre circulation des données à caractère personnel entre les États membres[904]. Elle a été complétée par la décision-cadre 2008/977/JAI destinée, à titre d'instrument général, au niveau de l'Union, à protéger les données à caractère personnel dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale.

La rapide évolution des technologies a créé de nouveaux enjeux pour la protection des données à caractère personnel. Le partage et la collecte de données ont connu une augmentation spectaculaire. Les nouvelles technologies permettent tant aux entreprises privées qu'aux

---

[900] Cour de justice de l'Union européenne (Grande cour), Arrêt du 6 octobre 2015, Affaire C-362/14 *Maximilien Schrems c/Data Protection Commissioner et Digital Rights Ireland Ltd*.

[901] Marie-Andrée Weiss, « De la sphère au bouclier : qu'est-ce que le Privacy Shield ? », *I2D – Information, données & documents*, 2016/3 (Volume 53), pp. 20-22. URL : https://www.cairn.info/revue-i2d-information-donnees-et-documents-2016-3-page-20.htm consulté le 5 avril 2018.

[902] European Commission, *Commission implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, C(2016) 4176 final.

[903] Exceptions prévues à l'article 69 de la loi informatique et libertés du 6 janvier 1978 modifiée.

[904] Objectifs rappelés dans les considérants nos 1 à 3 de la Directive 95/46/CE.

pouvoirs publics d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus de personnes physiques rendent des informations les concernant accessibles à tout un chacun, où qu'il se trouve dans le monde. Les nouvelles technologies ont ainsi transformé l'économie et les rapports sociaux.

L'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE), introduit par le traité de Lisbonne, établit le principe selon lequel toute personne a droit à la protection des données à caractère personnel la concernant. En outre, avec l'article 16, paragraphe 2, du TFUE, le traité de Lisbonne a créé une base juridique spécifique pour l'adoption de règles en matière de protection des données à caractère personnel. L'article 8 de la charte des droits fondamentaux de l'Union européenne consacre la protection des données à caractère personnel en tant que droit fondamental.

Dans ce cadre et après une vaste consultation des principales parties prenantes sur l'opportunité de réviser le cadre juridique actuel de la protection des données à caractère personnel, qui a duré plusieurs années, la commission a proposé une révision de la protection des données à caractère personnel au travers d'un règlement et d'une directive publiés le même jour :

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)*,

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*,

ainsi qu'une directive concernant l'adoption du registre des données passager au niveau de l'Union européenne[905].

Ainsi, le même jour, l'Union européenne se dotait d'un règlement général sur la protection des données et adoptait deux directives de traitement de ces données dans un cadre de lutte contre la délinquance et le terrorisme. Le nouveau règlement, fruit d'une longue négociation, modifie le cadre juridique de la protection des données à caractère personnel.

[905] 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.*

Il renforce les droits des personnes au travers du consentement. Ce consentement doit être le résultat d'une information claire, intelligible et accessible aux personnes[906]. Le consentement doit pouvoir être prouvé par le responsable de traitement et il n'est pas illimité, mais donné pour l'objectif déclaré du traitement, en cas d'abus, la personne peut révoquer son consentement et demander l'effacement des données collectées[907] suite à ce consentement abusif. Le règlement crée un droit à la portabilité des données, c'est-à-dire que la personne peut récupérer les données fournies sous une forme réutilisable. Ce droit étant nouveau, il sera intéressant de voir son application pratique.

Le règlement prévoit des dispositions spécifiques concernant les mineurs[908]. Le consentement doit ici être récupéré auprès du titulaire de l'autorité parentale. Devenue adulte, la personne peut retirer son consentement et demander l'effacement des données collectées[909].

Les associations ont la possibilité d'introduire des recours collectifs en matière de protection des données personnelles[910], comme elles peuvent le faire en matière de consommation.

Toute personne a droit à réparation du responsable de traitement ou du sous-traitant en cas de dommage matériel ou moral du fait d'une violation du règlement. Les données transférées[911] hors de l'Union européenne restent soumises au droit de l'Union tant pour leur transfert que pour leur traitement[912].

La responsabilité des responsables de traitement[913] n'est plus liée à des « formalités préalables » comme avec la directive 95/46/CE, mais elle repose sur un principe de conformité et d'éthique sous le contrôle des organes de régulation, au travers d'un registre des traitements mis en œuvre, une certification des traitements et des études d'impact sur la vie privée. Les sanctions administratives sont revues à la hausse et peuvent s'élever à 10 ou 20 millions d'euros, ou, pour une entreprise, de 2 % à 4 % de son chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu[914]. Cette augmentation des sanctions était demandée depuis plusieurs années, les sommes prévues par la directive étant négligeables par rapport au chiffre annuel des géants de

[906] RGPD, Article 7, 12, 13, 14.
[907] RGPD, Article 17.
[908] RGPD, Article 8.
[909] L'effacement des données collectées auprès d'un mineur est prévu en droit français dans la loi pour une République numérique.
[910] RGPD, Article 80.
[911] RGPD, Chapitre V, article 44 et suivants.
[912] Ainsi les données collectées par les réseaux sociaux d'origine nord-américaine ou par les moteurs de recherche doivent respecter les principes de protection prévus par le Règlement général sur la protection des données.
[913] RGPD, Chapitre IV, Articles 24 et suivants.
[914] RGPD, Article 83.

l'Internet qui sont visés. Les pouvoirs de sanction de la Commission de l'informatique et des libertés étaient limités. Elle pouvait prononcer une amende de 150 000 € maximum, ou 300 000 en cas de récidive, soit des sommes non significatives pour de grands groupes comme Facebook ou Google. Google n'a pas pris la peine de répondre à la CNIL après une enquête dont il a fait l'objet. La Commission de l'informatique et des libertés s'était associée aux autres autorités de protection des données européennes pour mener cette investigation dans le cadre du groupement appelé Groupe de travail « article 29 » ou plus simplement G29. Dans ce contexte, fin février 2013, Viviane Reding plaidait pour une autorité européenne : « *Ce régulateur à guichet unique pourrait menacer une société qui n'obéit pas aux règles, d'amendes allant jusqu'à 2 % de son chiffre d'affaires mondial* ». Et elle ciblait Google, « *un cas d'école* » selon elle. Le chiffre d'affaires de Mountain View a atteint 50 milliards de dollars en 2012. À titre d'exemple, en cas d'amende allant jusqu'à 2 %, la sanction pourrait représenter 1 milliard de dollars dans le cas de Google.

Le G29 est remplacé par un Comité européen de la protection des données (CEPD), il devient un organe de l'Union avec la personnalité juridique[915]. Le comité se compose du chef d'une autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données. Son président et deux vice-présidents sont élus au sein de ses membres à la majorité simple, pour un mandat de cinq ans, renouvelable une fois.

§ 3 - Une harmonisation mondiale difficile

Si l'Union européenne, au travers d'une directive puis d'un règlement, a réussi à mettre en place de façon harmonisée une véritable protection des données à caractère personnel, il n'en est pas de même au niveau international.

En 1989, l'ONU, dans sa décision 44/132 du 15 décembre 1989[916], demande à la commission des droits de l'homme d'examiner le projet de principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel. Le 14 décembre 1990, dans

[915] RGPD, Article 69.

[916] Assemblée générale de l'Organisation des Nations unies, résolution 44/132 *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel*, 15 décembre 1989, disponible à http://www.un.org/french/documents/view_doc.asp?symbol=A/RES/44/132&Lang=F, consulté le 29 décembre 2017.

sa résolution 45/95[917], l'assemblée générale adopte les principes directeurs pour la réglementation des fichiers informatisés dans leur version révisée suite aux commentaires et suggestions transmis par les gouvernements au Secrétaire général. Les principes énoncés sont le principe de licéité et de loyauté, le principe d'exactitude, le principe de finalité, le principe de l'accès par les personnes concernées, le principe de non-discrimination, la faculté de dérogation pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publique, le principe de sécurité. Les informations doivent pouvoir circuler entre plusieurs pays sans restriction si les législations présentent des garanties comparables au regard de la protection de la vie privée, sinon des limitations ne peuvent être imposées que si la stricte protection de la vie privée l'exige.

Un panorama des législations établi en juin 2008[918], montre que sept pays avaient un niveau de protection adéquat pour l'Union européenne, dans ces sept pays, les États-Unis y figuraient au titre du Safe Harbour[919], par déclaration du respect des principes internationaux de protection des données, aucune législation globale fédérale n'est mise en place seules des lois sectorielles relatives à la protection des données existent : *the fair credit reporting act* 1970, *the video privacy protection act* 1988, *electronic freedom of information act* 1996, *children's online privacy protection act* 1998.

D'autres pays disposent d'une législation, l'Afrique du Sud avec une loi de promotion de l'accès à l'information de 2000, l'Australie avec une loi fédérale sur la vie privée de 1988 ne concernant que le secteur public, le Brésil avec une loi réglementaire de l'habeus data nº 9 507 de 1997, le Japon avec une loi sur la protection des données personnelles informatisées dans le secteur public de 1988, le Mexique avec une loi de transparence et d'accès à l'information publique gouvernementale du 30 avril 2002.

Au niveau européen, la Commission a reconnu comme adéquats les États suivants[920] : Andorre, Argentine, Canada, États-Unis d'Amérique, Guernesey, île de Man, îles Féroé, Israël, Jersey,

---

[917] Assemblée générale de l'Organisation des Nations unies, résolution 45/95 *Principes directeurs pour la réglementation des fichiers personnels informatisés,* 14 décembre 1990, disponible à http://www.un.org/french/documents/view_doc.asp?symbol=A/RES/45/95&Lang=F, consulté le 28 décembre 2017.

[918] Commission nationale de l'informatique et des libertés, *Transferts de données à caractère personnel vers des pays non membres de l'Union européenne*, juin 2008, URL : http://www.cil.cnrs.fr/CIL/IMG/pdf/Guide-tranfertdedonnees.pdf, consulté le 29 décembre 2017.

[919] Invalidé depuis par l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015, Affaire C-362/14, *Maximilliam Schrems c/ Data Protection Commissionner*.

[920] Source CNIL, http://www.cil.cnrs.fr/CIL/IMG/pdf/pays_loi_il.pdf, consulté le 7 mars 2017 ou https://www.cnil.fr/sites/default/files/atoms/files/niveau_de_protection-fr-jan2015.xls déjà cité.

Nouvelle-Zélande, Suisse, Uruguay. L'adéquation des États-Unis d'Amérique est reconnue au travers du *Privacy shield* ou bouclier de protection des données personnelles depuis le 12 juillet 2016 après que le Safe Harbor a été invalidé par la Cour de justice de l'Union européenne. Cet accord n'a pu être entériné qu'après que la loi sur la réparation judiciaire[921] ait été signée par le président Barack Obama, cette loi permet aux citoyens européens d'intenter une action aux États-Unis d'Amérique lors d'une violation du droit de la protection des données personnelles[922]. Mais, un décret signé par Donald Trump en janvier 2017[923] pourrait remettre en cause cet accord. La clause numéro 14 du décret indique que « *les agences [la NSA et le FBI] devront, dans la mesure permise par la loi en vigueur, s'assurer que leurs politiques de protection des données personnelles excluent les non-citoyens américains et les non-résidents permanents autorisés, des protections offertes par le Privacy Act au regard des informations personnelles identifiables* », alors qu'un accord complémentaire, l'*Umbrella Agreement*[924], entre en vigueur suite au vote par le Congrès d'une loi, le *Judicial Redress Act*[925], qui étend les bénéfices du *Privacy Act*[926] aux Européens en leur donnant accès aux juridictions américaines. L'évaluation annuelle du *Privacy Shield* doit permettre de valider la pertinence de l'accord dans ce contexte nouveau[927].

[921] *Redress mechanism*.
[922] Lire à ce sujet European Commission, COM (2016) 117 final, Communication from the Commission to the European Parliement and the Concil Transatlantic, "*Data Flows : Restoring Trust through Strong Safeguards*" du 29 février 2016, disponible à http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf, consulté le 7 mars 2017.
[923] Donald J. Trump, *Executive Order: Enhancing Public Safety in the Interior of the United States*, January 25, 2017, Sec. 14. "*Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information".* In line at URL: https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/ consulté le 28 décembre 2017.
[924] *Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses*, draft for initialling at http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf, consulté le 29 décembre 2017.
[925] *Judicial redress act of 2015*, public law 114-126-Feb. 24, 2016.
[926] *Privacy Act of 1974*, 5 U.S.C. § 552a.
[927] Stéphane Le Calme, « Le CNNum estime que le Pivacy Shield, l'accord entre l'UE et les USA sur les transferts de données, doit être renégocié », *Développez.com*, 21 septembre 2017, en ligne à https://www.developpez.com/actu/161504/Le-CNNum-estime-que-le-Privacy-Shield-l-accord-entre-l-UE-et-les-USA-sur-les-transferts-de-donnees-doit-etre-renegocie/, consulté le 20 novembre 2017.

Sous-section 2. L'inviolabilité des correspondances et des communications

La vie privée peut être dévoilée au travers de la correspondance échangée. L'inviolabilité des correspondances est protégée au titre du respect de la vie privée. Le secret des correspondances trouve ses sources dans la loi et la jurisprudence, et à ce titre, tout message échangé peut être susceptible de protection. Cette inviolabilité peut, comme toute liberté individuelle, se voir restreinte de par la loi pour des raisons d'ordre public.

§ 1 - Les sources de la protection des correspondances

Au niveau international, la Déclaration universelle des droits de l'homme de 1948[928] est une référence en matière des droits de l'homme, elle évoque la protection de la vie privée et de la correspondance[929]. L'article 17 du pacte international relatif aux droits civils et politiques des Nations-Unies du 16 décembre 1966[930] reprend les mêmes notions sous une présentation quasi identique[931] en invoquant la protection de la loi. Le Pacte a été ratifié par de nombreux pays dont l'Allemagne et la France, mais non par les États-Unis d'Amérique qui considèrent qu'il existe une incompatibilité entre certains articles du Pacte et le premier amendement de la Constitution américaine protégeant la liberté d'expression.

La Convention européenne de sauvegarde des droits de l'homme[932], à travers son article huit protège également le secret de la correspondance et la vie privée. L'article 8 de la Convention européenne des droits de l'homme commence par « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.* »

---

[928] Le 10 décembre 1948, les 58 États Membres de l'Organisation des Nations unies qui constituaient alors l'Assemblée générale ont adopté la Déclaration universelle des droits de l'homme à Paris au Palais de Chaillot (résolution 217 A (III)).

[929] L'article 12 de la Déclaration universelle des droits de l'homme du 12 décembre 1948 précise : « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions* ».

[930] Nations unies, 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 2 200 A (XXI) du 16 décembre 1966 ; Entrée en vigueur : le 23 mars 1976, conformément aux dispositions de l'article 49.

[931] L'article 17 du pacte international relatif aux droits civils et politiques des Nations-Unies du 16 décembre 1966 : « *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 ».

[932] Convention européenne des droits de l'homme, Rome, novembre 1950, amendée par les Protocoles nos 11 et 14, complétée par le Protocole additionnel et les Protocoles nos 4, 6, 7, 12 et 13.

Au sein de l'Union européenne, le secret des communications fait l'objet de la directive 97/66[933]. La confidentialité des communications est garantie par son article 5[934]. Elle est reprise dans l'article 5 de la directive 2002/58/CE[935] : « *Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée […]* »

En France, le Code pénal protège le secret des correspondances. Ainsi, l'article 226-15 modifié par l'ordonnance n° 2000-916 du 19 septembre 2000[936] stipule : « *Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.*

« Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. »

La prise de connaissance du contenu d'une correspondance est ainsi définie comme un délit. Cet article englobe la correspondance classique et la correspondance transmise par voie électronique, donc les courriels et autres SMS. Le secret des correspondances émises par voie

[933] Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications* publiée au Journal officiel n° L 024 du 30/01/1998 p. 18.

[934] Directive 97/66/CE Art. 5. « *Les États membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessible au public. En particulier, ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées […] ».*

[935] 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)* publiée au Journal officiel des Communautés européennes du 31 juillet 2002 pp.37-47.

[936] Ordonnance n° 2000-916 du 19 septembre 2000 *portant adaptation de la valeur en euros de certains montants exprimés en francs dans les textes législatifs* parue au JORF n° 0220 du 22 septembre 2000 p. 14877.

électronique avait déjà été précisé par l'article 1 de la loi nº 91-646[937] : « *Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi.* »
La protection des correspondances et des communications électroniques est prévue dans le Code des postes et des communications électroniques. En particulier, l'article L.32-1 prévoit dans son I 6º « *Le respect par les opérateurs de communications électroniques de la protection des données à caractère personnel, du secret des correspondances et du principe de neutralité vis-à-vis du contenu des messages transmis ;* » et l'article L.32-3 « *Les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances* ».
Ce sont donc plusieurs textes, européens ou locaux qui protègent le secret des correspondances et des communications. Mais comme le précise l'article 5 de la directive 2002/58/CE, cette protection peut connaître des exceptions légales.

§ 2 - Les exceptions au secret des correspondances

L'article 66 du Code des douanes permet ainsi à La Poste de soumettre au contrôle douanier les envois frappés de prohibition à l'importation, passibles de droits ou soumis à des restrictions ou formalités à l'entrée. Ainsi, les courriers provenant d'un pays étranger peuvent être contrôlés par la Douane, mais l'agent des douanes ne peut en aucun cas, prendre connaissance de la teneur des correspondances ainsi contrôlées. Les lois sur la sécurité et la lutte antiterrorisme apportent également des exceptions à cette inviolabilité[938].
Mais ces restrictions doivent être prévues par la loi et justifiées par l'ordre public. Comme l'écrit Jean Pradel[939] : « *Pour traquer les malfaiteurs, il faut que la preuve se fasse. Mais elle ne saurait se faire au mépris des règles du code de procédure pénale, expression de la volonté du législateur. La procédure est un équilibre entre l'intérêt général qui implique la lutte contre le crime et l'intérêt des accusés qui appelle l'existence et le respect des garanties légales et judiciaires* ».
En 1990, la Cour européenne des droits de l'homme a ainsi sanctionné la France, considérant que les textes étaient trop vagues[940] : absence de délimitation précise et expresse des situations

[937] Loi nº 91-646 du 10 juillet 1991 *relative au secret des correspondances émises par la voie des télécommunications* publiée au JORF nº162 du 13 juillet 1991 p. 9167, abrogée le 1 mai 2012.
[938] Cf. Partie 1. Titre 2. Chapitre 2. Section 2. Sous-section 1. § 1 - La surveillance des individus à leur insu.
[939] Jean Pradel, « Investigations téléphoniques au cours de l'enquête », *Recueil Dalloz* 2006 p. 2836.
[940] Cour européenne des droits de l'homme, Arrêt du 24 avril 1990, Affaire *Kruslin c/ France*, Requête nº11801/85 et Affaire Huvig c/ France, Requête nº11105/84.

permettant l'interception de communications téléphoniques, absence de référence à la gravité des faits. La loi du 10 juillet 1991[941] met en place un organisme de contrôle pour les interceptions de sécurité : la Commission nationale de contrôle des interceptions de sécurité ou CNCIS qui sera remplacé par la Commission nationale de contrôle des techniques de renseignement par la loi relative au renseignement[942]. La plupart des États démocratiques européens ont institué de tels organismes de contrôle. Par exemple, en Allemagne, le contrôle est effectué par deux commissions, le PKG et la commission G10.

Les lois de lutte antiterrorisme[943] sont à l'origine de nouvelles dispositions concernant les technologies de l'information : vidéosurveillance, et interceptions de communications électroniques. Les interceptions de sécurité sont autorisées par des décisions administratives relevant du Premier ministre et non plus du pouvoir judiciaire[944].

Si l'interception des communications électroniques est protégée par la loi, les messages électroniques ne sont pas toujours considérés comme des courriers privés. La loi pour la confiance dans l'économie numérique[945] ne précise pas qu'un courrier électronique est un courrier privé et la décision du Conseil constitutionnel[946] laisse au juge l'appréciation du fait qu'un tel courriel est privé ou non[947]. De ce fait, un employeur peut consulter les courriers électroniques professionnels échangés par un employé sur la messagerie professionnelle en utilisant les ordinateurs mis à disposition par l'entreprise. La loi pour une république numérique[948] a précisé les modalités de confidentialité des correspondances électroniques privées[949].

---

941 Loi nº 91-646 du 10 juillet 1991 *relative au secret des correspondances émises par la voie des communications électroniques*, publiée au JORF nº162 du 13 juillet 1991 p. 9167.

942 Loi n° 2015-912 du 24 juillet 2015 *relative au renseignement* publiée au JORF n°0171 du 26 juillet 2015 page 12735.

943 Après 2006 et la loi nº 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.*

944 Cf. Partie 1. Titre 2. Chapitre 1. Section 1. Sous-section 2. § 1 - Les restrictions administratives à la protection de la vie privée.

945 Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique*, publiée au JORF nº0143 du 22 juin 2004 p. 11168.

946 Conseil constitutionnel, Décision nº 2004-496 DC du 10 juin 2004, *Loi pour la confiance dans l'économie numérique*.

947 « *En cas d'utilisation sur un PC professionnel, les messages échangés sur la messagerie professionnelle sont réputés professionnels et non privés, en cas d'utilisation d'une messagerie privée, non professionnelle, ces messages sont réputés privés et ne peuvent être ni lus ni utilisés par l'employeur* » (Cour de cassation, Chambre sociale, Arrêt nº 140 du 26 janvier 2016, Nº de pourvoi 14-15.360).

948 Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF nº0235 du 8 octobre 2016.

949 Article 68 : « *Le secret [des correspondances] couvre le contenu de la correspondance, l'identité des correspondants ainsi que, le cas échéant, l'intitulé du message et les documents joints à la correspondance* ».

Les messages électroniques sont stockés sur des serveurs et ils peuvent y être consultés. Google a ainsi scanné le contenu des messages échangés dans la messagerie gmail.com[950], un process technologique d'analyse des contenus qui permettait d'afficher de la publicité ciblée, en fonction des goûts et des centres d'intérêt des internautes. Google a annoncé qu'il abandonne cette technique[951]. Cette analyse est interdite par la loi pour une république numérique[952], sauf en cas de consentement exprès des utilisateurs[953]. Le consentement étant également présent dans le nouveau règlement général sur la protection des données [954]au niveau européen, Google a-t-il voulu éviter de nombreux procès potentiels en renonçant à cette pratique ?

[950] Gmail : l'analyse des emails par Google devant la justice américaine, ZDNet, 27 septembre 2013, en ligne à http://www.zdnet.fr/actualites/gmail-l-analyse-des-emails-par-google-devant-la-justice-americaine-39794372.htm consulté le 12 juillet 2017.
[951] Philippe Guerrier, « Publicité ciblée : Google arrête le scan des contenus sur Gmail, mais change de levier », *ITexpresso*, 26 juin 2017, en ligne à http://www.itespresso.fr/publicite-ciblee-google-arrete-scan-contenus-gmail-163336.html?inf_by=596643b1671db84e358b4855, consulté le 12 juillet 2017.
[952] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF n°0235 du 8 octobre 2016.
[953] Article 68 : « *Le traitement automatisé d'analyse, à des fins publicitaires, statistiques ou d'amélioration du service apporté à l'utilisateur, du contenu de la correspondance en ligne, de l'identité des correspondants ainsi que, le cas échéant, de l'intitulé ou des documents joints mentionnés auxdits I et II est interdit, sauf si le consentement exprès de l'utilisateur est recueilli à une périodicité fixée par voie réglementaire, qui ne peut être supérieure à un an. Le consentement est spécifique à chaque traitement* ».
[954] 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).*

Section 2. La légalisation de la numérisation

Avec la dématérialisation de nombreux actes de la vie privée, de nouveaux textes ont avalisé l'utilisation de documents dématérialisés. Dans la vie courante, la monnaie papier, numéraire ou scripturale, est remplacée par une monnaie virtuelle, en attendant les monnaies non régulées comme le *bitcoin*[955]. Pour des raisons de lutte contre la corruption ou la fraude fiscale, la monnaie scripturale remplace la monnaie fiduciaire dans les transactions à partir d'un certain montant[956]. Dans la vie courante, le chèque est aussi remplacé par la carte de crédit et la monnaie électronique, la monnaie fiduciaire ne conservant qu'un rôle d'appoint pour des transactions de faible valeur, le paiement sans contact pour des sommes inférieures à 30 euros se généralisant. Utiliser des techniques numériques pour payer ou réaliser une transaction en toute liberté nécessite de pouvoir identifier la personne effectuant cette opération et d'authentifier cette transaction. Afin de permettre à l'utilisateur de choisir librement le mode de réalisation d'une transaction, soit en tête-à-tête soit en ligne, l'authentification et la sécurité doivent présenter le même niveau de fiabilité qu'elle soit dématérialisée ou scripturale. Avec la technique d'échange des informations sous forme électronique, il est également nécessaire de sécuriser les échanges des données et des correspondances pour éviter ou limiter les fraudes, ainsi que les altérations de ces données[957].

Sous-section 1. Une Loi relative à la fraude informatique, dite « loi Godfrain »[958]

Le traitement des données personnelles s'il doit être déclaré à la Commission de l'informatique et des libertés, doit également être protégé des attaques et des vols. La protection des données nécessite la sécurité du transfert et de stockage de ces données et la non-captation par un tiers.

[955] Michel Aglietta, Laurence Scialom, « Les risques de la monnaie électronique », *L'Économie politique*, 2002/2 (nº 14), pp. 82-95. URL : https://www.cairn.info/revue-l-economie-politique-2002-2-page-82.htm consulté le 29 décembre 2017.
[956] Code monétaire et financier, art. L.122-6, L.112-6-1, D.112-3, R.112-5.
[957] Jacques Godfrain, « La loi du 5 janvier 1988 sur la fraude informatique (loi Godfrain) », Irène Bouhadana, William Gilles (sous la direction de), *Cybercriminalité cybermenaces et cyberfraudes,* Mars 2012, Les éditions IMODEV.
[958] Loi nº 88-19 du 5 janvier 1988*, relative à la fraude informatique* publiée au Journal officiel de la République française du 6 janvier 1988 p. 231.

Le responsable des traitements est responsable de la sécurité des données[959]. L'intrusion dans un système informatique reste cependant techniquement possible, la sécurité ne pouvant pas être assurée à 100 %[960].

Les fournisseurs de traitement informatique concernant les données à caractère personnel doivent assurer la protection de ces données en mettant en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé. Le vol de données peut avoir des conséquences pour les personnes dont les données ont ainsi été captées : divulgation d'informations, utilisation frauduleuse de données de paiement, etc. Personne ne souhaite retrouver sur un site Internet ou sur tout autre support, ses numéros de téléphone ou ses comptes bancaires, voir ses mots de passe ou des photos malveillantes détruisant une réputation. De grands groupes ont ainsi vu leurs fichiers piratés : Sony[961], Orange[962], etc.

Quels que soient les moyens mis en œuvre pour la sécurité des données et des traitements, les progrès des techniques de la cybercriminalité évoluent et des fournisseurs importants se sont vus piratés et ont subi le vol de leurs fichiers commerciaux ou non. Face à cette cybercriminalité, La France s'est dotée, dès 1988, d'une législation particulière relative à la pénalisation des intrusions dans un système informatique, quelle qu'en soit la raison. La loi Godfrain[963] sanctionne : les tentatives d'accès à un système informatique ; le maintien dans ce système ; la destruction de données ou l'entrave au bon fonctionnement d'un système informatique[964]. Cette loi a été intégrée dans le Code pénal dans un chapitre III « Des atteintes aux systèmes de traitement automatisé des données ». Cette loi est courte, un article unique qui créée ce chapitre III, chapitre qui définit en huit articles, les articles 462-2 à 462-9 (devenus les

[959] Loi n° 78-17, art.34 et Règlement général de protection des données, Art. 3-1-f), art. 32 et 35.

[960] Éric Léopold, Serge Lhoste, « La sécurité en question », dans *La sécurité informatique.* Paris, Presses Universitaires de France, « Que sais-je ? », 2007, pp. 30-59. URL : https://www.cairn.info/la-securite-informatique--9782130561675-page-30.htm consulté le 28 décembre 2017.

[961] « Sony Pictures reconnaît un "vaste vol de données confidentielles" », 4 décembre 2014, *20 minutes,* URL : http://www.20minutes.fr/web/1494339-20141204-sony-pictures-reconnait-vaste-vol-donnees-confidentielles consulté le 28 décembre 2017.

[962] Le Monde.fr avec AFP, « Nouveau vol massif de données personnelles chez Orange », 7 mai 2014, *Le Monde.fr,* URL : http://www.lemonde.fr/technologies/article/2014/05/06/vol-de-donnees-chez-orange-1-3-million-de-clients-et-de-prospects-touches_4412570_651865.html consulté le 28 décembre 2017.

[963] Loi nº 88-19 du 5 janvier 1988*, relative à la fraude informatique* publiée au Journal officiel de la République française du 6 janvier 1988 p. 231.

[964] Éric Léopold, Serge Lhoste, « Le cadre légal », dans *La sécurité informatique.* Paris, Presses Universitaires de France, « Que sais-je ? », 2007, pp. 92-102. URL : https://www.cairn.info/la-securite-informatique--9782130561675-page-92.htm consulté le 30 décembre 2017.

articles 323-1 à 323-7 dans le nouveau Code pénal de décembre 1992) les incriminations et les peines associées.

Cette loi, promulguée en 1988, concise, est toujours d'actualité, et reste souvent la seule loi pénale applicable en cas de cybercriminalité. Encore faut-il pour pouvoir la mettre en œuvre, être capable de détecter ces intrusions et leurs origines, tâches techniquement complexes qui se heurtent à l'omerta des sociétés ainsi agressées et à la difficile localisation des acteurs concernés, ces derniers agissant à partir de territoires situés hors de l'Union européenne : Fédération de Russie, Chine, voire États-Unis d'Amérique.

Le nouveau Règlement général sur la protection des données oblige les responsables de traitement à réaliser une étude d'impact des failles de sécurité sur les conséquences potentielles d'un vol de données[965].

Sous-section 2. Une sécurisation des transactions électroniques

La généralisation des échanges électroniques impose de connaître l'identité des intervenants dans une transaction. À cet effet, la signature électronique et les ventes sur Internet nécessitent des règles strictes à suivre et respecter.

§ 1 - L'équivalence du support papier et du support électronique

Dès 1999, l'Union européenne a défini le cadre communautaire d'une harmonisation de la signature électronique[966]. L'objectif de cette directive, défini dans son article 1, est de : « *faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur.* » Elle a été transposée en droit français dans le trimestre suivant sa publication[967] par modification du Code

[965] RGPD, Article 35.

[966] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, *sur un cadre communautaire pour les signatures électroniques* publiée au Journal officiel nº L 013 du 19/01/2000 pp. 12–20.

[967] Loi nº 2000-230 du 13 mars 2000 *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* publiée au JORF nº62 du 14 mars 2000 p. 3968.

civil qui rend équivalent l'écrit sur papier et sur support magnétique[968] et valide la signature électronique[969].

Dès mars 2000, le support électronique est juridiquement équivalent au support papier et admis comme preuve[970]. La dématérialisation des actes devient possible, mais elle nécessite de pouvoir identifier le signataire et garantir l'intégrité documentaire.

En mars 2001, un décret[971] va différencier la signature électronique de la signature électronique sécurisée qui doit répondre à des critères précis : « *être propre au signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectée* ». De fait, la sécurisation nécessite l'utilisation d'un certificat fourni par une autorité de confiance certifiée[972]. Si la signature électronique est une preuve quel que soit son niveau de sécurité, seule la signature électronique sécurisée est équivalente à la signature manuscrite en matière de preuve. Dans les échanges courants, lors d'une transaction effectuée sur Internet, l'utilisation d'un certificat n'est pas requise. Toutefois, des procédures sont mises en œuvre afin de permettre à l'utilisateur de pouvoir utiliser en toute confiance le commerce électronique et payer un achat en toute confiance.

En juillet 2014, le règlement eIDAS[973] vient redéfinir le cadre de l'identification électronique et des services de confiance. Le règlement eIDAS concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre le sujet de

---

968 Par insertion d'un article 1316-3 ainsi rédigé : « *Art. 1316-3. - L'écrit sur support électronique a la même force probante que l'écrit sur support papier* ».

969 Par insertion d'un article 136-4 ainsi rédigé : « *Art. 1316-4. — La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*
« Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État ».

970 Loi n° 2000-230 du 13 mars 2000 *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, publiée au JORF n°62 du 14 mars 2000 p. 3968.

971 Décret nº 2001-272 du 30 mars 2001 *pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique* publié au JORF nº0077 du 31 mars 2001 p. 5070.

972 Décret nº 2002-535 du 18 avril 2002 *relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information* publié au JORF nº92 du 19 avril 2002 p. 6944.

973 Règlement (UE) Nº 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.*

la signature électronique. En France, l'ANSSI et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) sont les organismes nationaux chargés de la mise en œuvre de ce règlement. Le règlement est applicable depuis le 1er juillet 2016. Il vise à instaurer un mécanisme de reconnaissance mutuelle des moyens d'identification électronique des États membres sur l'ensemble des services en ligne des autres États membres[974].

§ 2 - La sécurisation des échanges dématérialisés dans le commerce électronique

Internet a permis le développement du commerce électronique qui permet à tout individu d'accéder aux choix du commerçant et des produits proposés. Afin de garantir la liberté de choix du consommateur, le consommateur doit être protégé des entreprises malveillantes voire des usurpations d'identité.

En 2001, une ordonnance[975] transpose plusieurs directives européennes[976] concernant la protection des consommateurs et en particulier les contrats conclus à distance interagissant ainsi directement sur les transactions électroniques du « Business to Consumer » (B to C) ou en français « Professionnel à Consommateur ». Cette ordonnance modifie ou complète le code de la consommation pour « *toute vente d'un bien ou toute fourniture d'une prestation de service conclue, sans la présence physique simultanée des parties, entre un consommateur et un*

[974] Les exigences applicables aux trois niveaux de garantie prévus par le règlement, faible, substanciel et élevé, sont détaillées dans le règlement d'exécution n°2015/1502 du 8 septembre 2015. Ces niveaux sont accordés en fonction du respect de spécifications, normes et procédures minimales.

[975] Ordonnance nº 2001-741 du 23 août 2001 *portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation* publiée au JORF nº196 du 25 août 2001 p. 13645.

[976] Directive 89/397/CEE du Conseil du 14 juin 1989 *relative au contrôle officiel des denrées alimentaires* ; Directive 93/13/CEE du Conseil du 5 avril 1993 *concernant les clauses abusives dans les contrats conclus avec les consommateurs* ; Directive 95/53/CE du Conseil du 25 octobre 1995 *fixant les principes relatifs à l'organisation des contrôles officiels dans le domaine de l'alimentation animale*, modifiée par la directive 1999/20/CE du 22 mars 1999 du Conseil et par la directive 2000/77/CE du 14 décembre 2000 du Parlement européen et du Conseil ; Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 *concernant la protection des consommateurs en matière de contrats à distance* ; Directive 97/55/CE du Parlement européen et du Conseil du 6 octobre 1997 modifiant la directive 84/450/CEE *sur la publicité trompeuse afin d'y inclure la publicité comparative* ; Directive 98/27/CE du Parlement européen et du Conseil du 19 mai 1998 *relative aux actions en cessation en matière de protection des intérêts des consommateurs*, modifiée par la directive 1999/44/CE du Parlement et du Conseil et par la directive 2000/31/CE du Parlement européen et du Conseil ; Directive 1999/2/CE du Parlement européen et du Conseil du 22 février 1999 *relative au rapprochement des législations des États membres sur les denrées et ingrédients alimentaires traités par ionisation*.

professionnel qui, pour la conclusion de ce contrat, utilisent exclusivement une ou plusieurs techniques de communication à distance. »

Le consommateur doit disposer de certaines informations lors de la préparation de la commande et il dispose initialement d'un délai de rétractation de sept jours francs, devenu quatorze jours[977], sans avoir à justifier de motif ni à payer de pénalités. En cas d'exercice de ce droit de rétractation, le vendeur doit rembourser l'acheteur dans un délai maximum de trente jours. Ces clauses protectrices sont d'ordre public et ne peuvent donc être dérogées conventionnellement. De plus, afin d'éviter les abus, le fournisseur dispose d'un délai maximum de trente jours pour réaliser la prestation, si le bien est indisponible, le professionnel doit en aviser le consommateur et le rembourser dans les trente jours.

Cette ordonnance permet d'éviter certains abus constatés lors de vente en rupture de stock. Cette ordonnance est complétée en 2004 par la loi pour la confiance dans l'économie numérique[978] qui traite dans son titre II du commerce électronique. Le commerce électronique est défini comme « *l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services*. » Cette activité est « *soumise à la loi de l'État membre sur le territoire duquel la personne qui l'exerce est établie, sous réserve de la commune intention de cette personne et de celle à qui sont destinés les biens ou services* » sans déroger aux règles impératives prévues par la loi française et sans priver le consommateur résidant en France de la protection assurée par les dispositions impératives de la loi française relatives aux obligations contractuelles en particulier les dispositions définissant les droits du consommateur.

Cette loi complète le Code civil pour la validité des actes juridiques qui peuvent être établis et conservés sous forme électronique[979], à l'exclusion des actes sous seing privé relatifs au droit de la famille et des successions, ainsi qu'aux actes relatifs aux sûretés personnelles ou réelles.

Sur Internet, l'accord est formalisé par un clic de souris ou un appui sur une touche du clavier. La loi sur l'économie numérique de 2004 a ajouté au Code civil un article 1369-2[980] qui précise

---

[977] Ordonnance n° 2016-301 du 14 mars 2016 relative à la partie législative du code de la consommation.

[978] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* publiée au JORF nº0143 du 22 juin 2004 p. 11168.

[979] LCEN, Art. 1108-1. – « *Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317.*
« Lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même ».

[980] Devenu l'article nº1369-5 après l'ordonnance nº2005-674 du 16 juin 2005.

que pour qu'un contrat soit valablement conclu sur Internet, le consommateur a dû pouvoir vérifier le détail de sa commande, son prix total et avoir eu la possibilité de la corriger avant confirmation de l'accord exprimant son acceptation du contrat.

Le consommateur se trouve ainsi protégé par une législation spécifique prenant en compte les spécificités de la mise en relation via Internet d'un fournisseur d'offre, professionnel ou non, et d'un destinataire de l'offre, également professionnel ou non. La sécurité de la transaction est ainsi garantie au consommateur qui peut librement choisir de se procurer un bien ou un service dans une boutique en face à face ou à distance via un site marchand[981].

Si le processus de commande est ainsi encadré légalement, toute commande de service ou achat de biens nécessite un paiement. En général, sur Internet, ce paiement est effectué électroniquement par utilisation d'une carte bancaire. Certaines banques proposent à leur client un programme appelé e-carte bleue, ce petit programme permet d'obtenir pour une transaction unique dont le montant est précisé par le demandeur, un numéro de carte bancaire avec date de validité et cryptogramme. Les informations relatives à cette carte virtuelle sont fournies en lieu et place de la véritable carte bancaire, évitant ainsi de faire transiter sur le réseau des informations pouvant être captées et réutilisées pour produire de fausses cartes bancaires. Même en cas de captation, cette carte virtuelle ne pourra être utilisée qu'une seule fois pour un montant encadré. D'autres dispositifs de sécurité de paiement sont mis en place par les banques avec, par exemple, rappel sur un numéro de téléphone, défini à l'avance, pour confirmation de la transaction.

Toutefois, des fraudes restent possibles malgré les précautions prises, fraudes liées à des vols d'information dans les fichiers des entreprises permettant l'utilisation de moyens de paiement reconstitués. Le Code monétaire et financier protège le porteur d'un moyen de paiement électronique dans ses articles L.133-19 et L.133-20[982] lors de l'utilisation frauduleuse d'un

---

[981] Josef Drexl, « Le commerce électronique et la protection des consommateurs », *Revue internationale de droit économique*, 2002/2 (t. XVI), pp. 405-444. URL : https://www.cairn.info/revue-internationale-de-droit-economique-2002-2-page-405.htm consulté le 19 mars 2018.

[982] Code monétaire et financier, Article L.133-19 : « *I. - En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur supporte, avant l'information prévue à l'article L.133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 150 euros.*
« Toutefois, la responsabilité du payeur n'est pas engagée en cas d'opération de paiement non autorisée effectuée sans utilisation du dispositif de sécurité personnalisé.
« II. — La responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées.
« Elle n'est pas engagée non plus en cas de contrefaçon de l'instrument de paiement si, au moment de l'opération de paiement non autorisée, le payeur était en possession de son instrument.
« III. — Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant l'information aux fins de

moyen de paiement en obligeant l'établissement financier fournisseur du moyen de paiement à restituer au porteur de bonne foi les sommes détournées.
Le Code civil et le Code monétaire et financier se conjuguent pour développer les transactions électroniques, vecteurs de liberté et générateurs de richesse, mais devant les fraudes, les établissements bancaires ont imposé des montants maximums par transaction, ainsi que des limites au montant des achats réalisés par une personne physique dans une période donnée, au nom de la sécurité financière.

Ainsi, les libertés publiques et individuelles sont protégées par la loi dans une société de plus en plus numérisée et mondialisée. Des restrictions à ces libertés ont été imposées par la loi au nom de la défense de l'intérêt général et de la sécurité. Les libertés publiques restent protégées par la législation nationale, lois promulguées depuis la III^{e} République et modifiées pour tenir compte de l'évolution de la société, parfois complétées par des accords internationaux relatifs aux droits de l'homme adoptés après la seconde guerre mondiale. La protection des libertés individuelles liées à la protection de la vie privée est d'origine plus récente. Cette protection intègre les spécificités de la société numérique, spécificités apparues à partir de la seconde moitié du XX^{e} siècle. Elle tend à une harmonisation nécessaire au sein de l'Union européenne. Cette protection reste en perpétuelle amélioration face aux évolutions de la technique et aux conséquences de l'intrusion de ces techniques dans la vie personnelle des individus. Mais, malgré ces protections légales, la société numérique peut générer ou induire des atteintes à ces libertés, atteintes et restrictions peu anticipées par la législation. Certaines de ces atteintes aux libertés sont créées par une législation sécuritaire de lutte contre le terrorisme, pour une protection partielle et peu efficace contre une cybercriminalité mondialisée ou par protéger les données personnelles d'une marchandisation incontrôlée sur le WEB .

blocage de l'instrument de paiement prévue à l'article L.133-17.
« IV. — Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L.133-16 et L.133-17 ».
Article L.133-20 : « *Après avoir informé son prestataire ou l'entité désignée par celui-ci, conformément à l'article L.133-17 aux fins de blocage de l'instrument de paiement, le payeur ne supporte aucune conséquence financière résultant de l'utilisation de cet instrument de paiement ou de l'utilisation détournée des données qui lui sont liées, sauf agissement frauduleux de sa part ».*

Titre 2. La société numérique, un catalyseur des atteintes aux libertés

Les libertés fondamentales sont protégées par la Constitution, la législation et plusieurs instruments nationaux et internationaux, mais ces libertés sont encadrées par la loi pour garantir un équilibre entre les droits fondamentaux et le bien public[983]. La liberté d'expression s'arrête à la provocation à la haine raciale et à l'appel à la violence, par exemple. La protection de la vie privée et la liberté d'information[984] font l'objet d'un équilibre contrôlé par la Cour européenne des droits de l'homme[985] ou par le Conseil constitutionnel en France. La numérisation de la société n'a pas infléchi cette protection des libertés et certaines libertés connaissent un terrain favorable pour se développer dans cette société au travers des innovations techniques. Mais ces innovations techniques permettent aussi de mettre sous surveillance discrète les individus, et cette surveillance peut altérer peu ou prou ces libertés. Les révélations de Edward Snowden[986] ou de WikiLeaks[987] montrent que les États, même démocratiques, surveillent les informations transitant sur le réseau Internet et peuvent installer des logiciels espions[988] sur les objets connectés.

Dans notre société numérique, des situations décrites par des auteurs de science-fiction deviennent réalité. Dans 1984, George Orwell décrit des patrouilles qui surveillent en hélicoptère les individus au travers des fenêtres et invente la Police de la Pensée qui surveille sans pouvoir être détectée tout individu à travers le télécran[989]. Dans notre société numérisée, les patrouilles en hélicoptère sont remplacées par la vidéosurveillance, renommée vidéoprotection[990], et si le téléviseur ne surveille pas les individus, de nombreux dispositifs permettent de connaître leur activité : traces sur Internet, paiement électronique, géolocalisation

---

983 Jacques Mourgeon, « La surveillance des droits », dans *Les droits de l'homme.* Paris, Presses Universitaires de France, « Que sais-je ? », 2003, pp. 85-98. URL : https://www.cairn.info/les-droits-de-l-homme--9782130533849-page-85.htm consulté le 2 janvier 2018.

984 Grégoire Loiseau, « L'évolution de la jurisprudence française sur la vie privée des personnalités politiques », *LEGICOM*, 2015/1 (n° 54), pp. 119-123. URL : https://www.cairn.info/revue-legicom-2015-1-page-119.htm consulté le 2 janvier 2018.

985 Patrick Auvret, « L'équilibre entre la liberté et le respect de la vie privée selon la Cour européenne des droits de l'homme », *Gazette du Palais*, 12 avril 2005, p. 2.

986 Zygmunt Bauman, Didier Bigo, Paulo Esteves *et al.*, « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », *Cultures & Conflits*, 2015/2 (n° 98), pp. 133-166. URL : https://www.cairn.info/revue-cultures-et-conflits-2015-2-page-133.htm consulté le 2 janvier 2018.

987 Au travers de son site https://wikileaks.org/.

988 Lire sur le sujet Symantec Security Response, « Longhorn : Tools used by cyberespionage group linked to Vault 7 », *Symantec Official Blog,* 10 avril 2017, URL : https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7 consulté le 4 janvier 2018.

989 George Orwell, *1984*, édition Gallimard, 1950.

990 Le mot vidéosurveillance est remplacé par le mot vidéoprotection dans tous les textes législatifs et réglementaires par l'article 17 de la loi n° 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure*, dite LOPPSI 2.

des téléphones portables, courriers électroniques, messageries instantanées, etc. Une nouvelle de science-fiction, Minority Report de Philip K. Dick[991], portée à l'écran en 2002 par Stephen Spielberg, prédit une société où les futurs auteurs de crime sont arrêtés avant d'avoir commis leur crime. Aujourd'hui, des logiciels de prévision de délits ou de crimes sont utilisés par certaines unités de police dans le monde, et en France, les lois de lutte contre le terrorisme permettent sous le régime de l'État d'urgence de réduire la liberté d'aller et venir des personnes suspectées de préparer un acte de terrorisme. Cette surveillance est devenue possible en dehors de l'État d'urgence pour ces mêmes personnes suspectes sur simple décision administrative[992]. La société numérique nécessite le respect de l'État de droit pour éviter les atteintes aux libertés tant par les entreprises mercantiles que par une administration tentaculaire et sécuritaire. Encore faut-il que cet État de droit protège réellement et efficacement les individus, car les gouvernements, face à un risque sécuritaire édictent des législations d'exception utilisant les nouvelles technologies pour minimiser autant que faire se peut les risques d'attentats (chapitre 1) tandis que la mosaïque des législations internationales tend *de facto* à une insuffisance pratique des protections des libertés fondamentales (chapitre 2).

[991] Philip K. Dick, *Minority Report*, juin 2009, Folio bilingue Gallimard.
[992] Loi n° 2017-1510 du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme* publiée au JORF n°0255 du 31 octobre 2017.

Chapitre 1. Sécurité contre liberté, une lutte asymétrique

Dans l'Union européenne, les données à caractère personnel sont protégées par plusieurs textes, en particulier par la directive 95/46/CE[993], remplacée en 2018 par le nouveau règlement général sur la protection des données[994] ou RGPD, et leur traitement dans un pays hors du territoire européen est réglementé, le principe étant une interdiction de transfert de ces données à caractère personnel hors du territoire de l'Union européenne[995], interdiction sujette à des exceptions[996]. Depuis les attentats du 11 septembre 2001, sous la pression des États-Unis d'Amérique, les données personnelles de tous les voyageurs transitant ou se rendant aux États-Unis d'Amérique y sont transmises suite à un accord conclu entre la Commission européenne et le gouvernement américain[997], accord renégocié, mais toujours moins protecteur que les textes européens protégeant les données personnelles. L'Union européenne a également validé la transmission des données personnelles des voyageurs ou PNR entre les États membres[998], ainsi que la libre circulation des données à caractère personnel pour lutter contre la criminalité[999].

---

[993] 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* transposée dans la loi n°78-17 *relative à l'informatique et aux libertés*.

[994] 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).*

[995] Article 68 de la loi n°78-17 *relative à l'informatique et aux libertés*, transposant l'article 25 de la directive 95/46/CE.

[996] Article 69 de la loi n°78-17 *relative à l'informatique et aux libertés*, transposant l'article 26 de la directive 95/46/CE.

[997] Accord entre les États-Unis d'Amérique et l'Union européenne *pour l'utilisation des données des dossiers passagers (dossiers PNR) et leur transfert au ministère américain de la sécurité intérieure*, publié au Journal officiel de l'union européenne du 11 août 2012.

[998] 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.*

[999] 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.*

En France, comme dans d'autres États, pour des raisons de sécurité et de lutte contre le terrorisme, des textes législatifs ont été adoptés, réduisant les libertés individuelles au travers de restrictions de la liberté d'aller et venir, de captations autorisées des données personnelles ou d'interceptions des communications privées[1000]. Le juge judiciaire, garant constitutionnel des libertés[1001], voit son rôle de protecteur des libertés individuelles réduit[1002] et transféré partiellement au juge administratif par ces lois sécuritaires. Le contrôle de l'État concernant le traitement des données personnelles a été réduit par modification de la loi n° 78/17 du 6 janvier 1978, et le contrôle de la captation des conversations privées sur décision administrative ne relève en pratique que du juge administratif[1003], échappant au juge judiciaire dans les affaires de terrorisme. L'équilibre entre libertés individuelles et lutte pour la sécurité est menacé (section 1) les États privilégiant la sécurité au travers de nombreux textes sécuritaires (section 2).

[1000] Alex Türk, Pierre Piazza, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée. Entretien avec Alex TÜRK ; propos recueillis par Pierre PIAZZA », *Cultures & Conflits*, 2009/4 (n° 76), pp. 115-134. URL : https://www.cairn.info/revue-cultures-et-conflits-2009-4-page-115.htm consulté le 2 janvier 2018.

[1001] Article 66 de la Constitution du 4 octobre 1958 : « *Nul ne peut être arbitrairement détenu.*
« L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi ».

[1002] Lire à ce sujet les Discours de l'audience solennelle de rentrée de la Cour de cassation du 14 janvier 2016, accessible à l'URL : https://www.courdecassation.fr/venements_23/audiences_solennelles_59/debut_annee_60/annees_2010_3342/janvier_2016_33391.html, consulté le 14 juin 2017.

[1003] Conseil d'État, Avis du 12 mars 2015 sur le projet de loi relatif au renseignement.

Section 1. Une protection sécuritaire attentatoire aux libertés individuelles

La protection de l'individu face aux dangers de l'informatique fait l'objet de deux interprétations, compatibles, mais correspondant à deux philosophies différentes, la protection de l'individu est une fin en soi ou est la contrepartie du principe de libre circulation de l'information.

Dans l'Union européenne, les données à caractère personnel sont protégées par plusieurs textes, en particulier par la directive 95/46/CE[1004] remplacée le 25 mai 2018 par le Règlement général sur la protection des données[1005], et leur transfert et traitement dans un pays hors du territoire européen est réglementé[1006]. Tous les textes adoptés, tant au niveau de l'Union européenne qu'au niveau national des États membres, créent de fait de nouveaux droits pour les citoyens, ces droits doivent permettre de contrôler la collecte et l'utilisation des données à caractère personnel qui prolifèrent sur Internet. Le règlement général sur la protection des données[1007] confirme les droits existants et en crée de nouveaux en renforçant le principe du consentement et l'obligation de transportabilité des données.

En France, ces droits créés par la loi n° 78-17[1008] sont : le droit à l'information : toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée ; le droit d'opposition : toute personne a la possibilité de s'opposer, pour des raisons légitimes, à figurer dans un fichier ; le droit d'accès : toute personne a le droit d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle. Ce droit d'accès connaît un régime particulier, le droit d'accès indirect dans le cas des fichiers intéressant la sûreté de l'État, la défense et la sécurité publique. Dans ce cas, le droit d'accès est exercé par l'intermédiaire de la Commission de l'informatique et des libertés ; le droit de rectification : toute personne peut

[1004] Transposée en droit français par la 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.*

[1005] 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).*

[1006] Lire sur le site de la CNIL « Transférer des données hors de l'UE » à l'URL : https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue consultéle5 janvier2018.

[1007] 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).* Op. cit.

[1008] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* modifiée en 2004.

faire rectifier des informations qui la concernent. La loi n° 2016-1321[1009] a ajouté le droit à l'effacement, anticipant ainsi le Règlement général sur la protection des données[1010].

Après la transposition de la directive nº 95/46/CE, tous les États membres disposent d'une loi de protection des données à caractère personnel et d'une autorité de contrôle indépendante. En France, la transposition est réalisée le 6 août 2004 par une mise à jour de la loi nº 78-17[1011]. À l'exception du premier article, tous les articles sont réécrits pour s'adapter complètement au déploiement de l'Internet et intégrer les nouvelles technologies apparues depuis 1978. Mais de fait, certaines exemptions sont ajoutées concernant les obligations de l'administration. Certains traitements automatiques des données personnelles effectués par ou pour le compte d'une administration sont maintenant autorisés par décret et non plus par la Commission nationale de l'informatique et des libertés[1012]. La CNIL conserve l'obligation de fournir un avis motivé concernant ces traitements[1013], cet avis favorable ou défavorable est annexé au décret d'autorisation, et il ne peut empêcher la création du traitement. C'est ainsi que des fichiers de police ont été autorisés par décret, quelquefois plusieurs années après leur création[1014].

Ainsi, des textes législatifs existent et protègent la vie privée des individus, mais des exceptions légales permettent aux gouvernements de restreindre cette protection. Des contraintes existent au niveau européen, mais elles sont parfois contournées par des entreprises internationales qui se placent contractuellement sous le contrôle d'autres lois que la législation européenne, utilisant les écarts de législation qui peuvent exister entre la législation européenne et la législation américaine, voir même la législation de certains États d'Amérique du Nord[1015].

Depuis les attentats de New York du 11 septembre 2001, suivis des attentats du métro de Londres[1016] et des attentats de Madrid[1017], les États pour se protéger et prévenir les risques terroristes ont mis en place des législations d'exception attentatoires aux droits des personnes.

[1009] Loi du 7 octobre 2016 *pour une République numérique.*

[1010] Cf. Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 1. § 2 -C) Un nouveau règlement applicable en 2018 : le règlement général sur la protection des données ou RGPD

[1011] Loi nº 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

[1012] Articles 26 et 27 de la loi nº 78-17.

[1013] Article 28 de la loi nº 78-17.

[1014] Ce qui a été le cas des fichiers de la police STIC, et de la gendarmerie JUDEX.

[1015] Cf. Affaire Yahoo! citée par Jean-Jacques Lavenue, « Internet : efficacité des poursuites et ordre public international », Irène Bouhadana, William Gilles (Dir.), *Cybercriminalité, cybermenaces & cyberfraudes,* mars 2012, Éditions IMODEV, pp.84-91.

[1016] Trois attentats à la bombe dans le métro et un dans un autobus à Londres du 7 juillet 2005 suivis de quatre tentatives d'attentat à la bombe le 21 juillet 2005.

[1017] Plusieurs explosions dans des trains de banlieue à Madrid le 11 mars 2004.

Des restrictions légales et administratives à la protection de la vie privée ont été adoptées sous couvert de lutte contre l'insécurité et le terrorisme[1018]. En 2015, en réaction aux attentats de janvier contre le journal satirique Charlie Hebdo et contre un magasin HYPERCACHER, le gouvernement français a édicté une loi nouvelle[1019] légalisant des pratiques déjà mises en œuvre par les services de renseignements sans bases légales[1020].

Depuis les attentats du 11 septembre 2001, sous la pression des États-Unis d'Amérique, les données personnelles de tous les voyageurs transitant ou se rendant aux États-Unis d'Amérique y sont transmises suite à un accord conclu entre la Commission européenne et le gouvernement américain[1021], accord renégocié plusieurs fois, mais toujours moins protecteur que les textes européens protégeant les données personnelles[1022]. Une directive concernant les échanges de données des passagers a également été adoptée au niveau européen[1023]. De plus, depuis le 12 janvier 2009, tout voyageur européen désirant se rendre sur le territoire américain, même en transit, via un vol international, doit remplir un formulaire spécifique, l'ESTA ou « *Electronic System for Travel Authorization* », concernant les ressortissants des pays bénéficiant du Programme d'exemption de Visa (*Visa Waiver Program* ou VWP). De facto, cet ESTA est un visa valable deux ans, sans lequel l'entrée sur le territoire des États-Unis d'Amérique est impossible, même pour un simple transit. L'utilisation du formulaire, uniquement accessible via Internet[1024], nécessite la fourniture de données personnelles mises à disposition de l'administration américaine sans garanties ni droits pour une personne non nord-américaine, alors que la Cour de justice de l'Union européenne a annulé les accords « Safe Harbor » conclus entre la Commission et les États-Unis d'Amérique pour protection insuffisante des données sur le territoire américain[1025]. Les données fournies à l'administration américaine sont plus précises

[1018] Lyon David, « 6. Le 11 septembre, la "guerre au terrorisme" et la surveillance généralisée », dans *Au nom du 11 septembre...Les démocraties à l'épreuve de l'antiterrorisme.* Paris, La Découverte, « Cahiers libres », 2008, pp. 90-103. URL : https://www.cairn.info/au-nom-du--9782707153296-page-90.htm consulté le 2 janvier 2018.
[1019] Loi nº 2015-912 du 24 juillet 2015 *relative au renseignement* publiée au JORF nº0171 du 26 juillet 2015 p. 12735.
[1020] Jenny Raflik, « La France face au terrorisme d'hier à aujourd'hui », *Outre-Terre*, 2017/2 (n° 51), pp. 202-214. URL : https://www.cairn.info/revue-outre-terre-2017-2-page-202.htm consulté le 2 janvier 2018.
[1021] Accord signé en 2004 et renégocié en 2007 puis 2010. Il a été approuvé par le Parlement européen le 19 avril 2012.
[1022] Virginie Guiraudon, « La coopération transatlantique après le 11 septembre : », *Critique internationale*, 2005/3 (nº 28), pp. 21-35. URL : https://www.cairn.info/revue-critique-internationale-2005-3-page-21.htm consulté le 2 janvier 2018.
[1023] Directive (UE) 2016/681 du Parlement européen et du Conseil *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*.
[1024] Site officiel à l'URL : https://esta.cbp.dhs.gov/esta/ .
[1025] Cour de Justice de l'Union européenne (grande chambre) arrêt du 6 octobre 2015, affaire C-362/14 *Schrems.*

et complètes que celles demandées par l'administration française pour obtenir une carte d'identité nationale ou un passeport. Le Canada a instauré une autorisation de voyage électronique (AVE ou en anglais Electronic Travel Authorization eTA) à compter du 15 mars 2016[1026]. L'Australie avait mis en place un système similaire avant les États-Unis d'Amérique (ETA ou eVisitor)[1027].

En France, comme dans d'autres États, pour des raisons de sécurité et de lutte contre le terrorisme, des textes législatifs ont été promulgués, réduisant la sécurité des libertés individuelles au travers d'atteintes à la protection des données personnelles ou de captation des communications privées[1028]. Les textes réglementant la protection des données personnelles existent, mais pour des raisons de sécurité, les États imposent des compromis recherchant un difficile équilibre entre respect et protection des libertés et protection de l'ordre public (sous-section 1), et connaissent une tendance marquée vers une dérive sécuritaire (sous-section 2). L'équilibre entre sécurité et liberté est une problématique ancienne des pays démocratiques. Déjà en 1775, Benjamin Franklin disait : « *Ceux qui peuvent renoncer aux libertés essentielles pour obtenir un peu de sécurité temporaire ne méritent ni la liberté ni la sécurité* »[1029].

Sous-section 1. Les attaques contre la société et les États

La société numérique fragilise les États. En effet, un petit groupe de personnes déterminées disposant de moyens techniques suffisants, peut attaquer les ordinateurs d'un État et rendre indisponibles ces ordinateurs pendant une phase cruciale d'une attaque terroriste. Les États doivent se protéger contre de tels risques. Pour ce faire, de nouvelles lois de lutte contre le terrorisme ont été votées dans plusieurs États démocratiques au détriment des libertés individuelles.

Les cyberattaques peuvent viser les États, l'économie des États ou des personnes physiques ou morales. Elles peuvent aussi fragiliser certaines pratiques démocratiques comme les élections. Lors des élections présidentielles américaines de 2016, le gouvernement américain a mis en cause des cyberattaques semblant provenir de Russie et destinée à infléchir le résultat des

[1026] https://www.canada.ca/fr/immigration-refugies-citoyennete/services/visiter-canada/ave.html .
[1027] https://www.homeaffairs.gov.au/Trav/Visa-1/651- .
[1028] Floran Vadillo, « Du terrorisme en démocratie », *Sécurité et stratégie*, 2015/1 (20), pp. 5-13. URL : https://www.cairn.info/revue-securite-et-strategie-2015-1-page-5.htm consulté le 2 janvier 2018.
[1029] "*They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety".*

élections en faveur d'un des candidats[1030]. Un détournement et une captation intensive de données personnelles à partir du réseau social FACEBOOK a également été révélé[1031]. Ces données ont été utilisées pour déterminer le profil d'électeurs favorables à un des candidats et pout influencer ces électeurs par des messages ciblés.

§ 1 - Une nouvelle criminalité : la cybercriminalité

Les infractions liées à la cybercriminalité sont très diverses et il y a lieu de distinguer deux catégories de crimes ou délits liés à la cybercriminalité : les infractions traditionnelles, c'est-à-dire les crimes ou délits « ordinaires » facilités par l'utilisation de l'informatique, et les infractions spécifiques, c'est-à-dire les crimes ou délits qui ne doivent leur existence qu'au développement de l'informatique, des réseaux de télécommunications et de la numérisation de notre société[1032].

L'Institut National des Hautes Études de la Sécurité et de la Justice définit la cybercriminalité par « *l'ensemble des infractions commises via le réseau Internet, et consiste en l'utilisation frauduleuse des systèmes et réseaux informatiques* ». Dans son rapport annuel de 2011[1033], il cite comme infractions principales : les infractions au droit de la presse, la pédopornographie, le piratage, l'escroquerie et la contrefaçon, mais il précise que le terrorisme présente un risque dans le monde numérique. En annexe de ce rapport, Myriam Quémener[1034], magistrate, indique qu'il est possible d'identifier 164 « cyberinfractions » spécifiques dans l'arsenal répressif français.

[1030] *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* disponible à https://www.dni.gov/files/documents/ICA_2017_01.pdf et consulté le 16 juin 2017.

[1031] Brett Molina, "Facebook and Cambridge Analytica: What we know so far", *USA Today,* 19 march 2018, URL: https://www.usatoday.com/story/tech/news/2018/03/19/facebook-and-cambridge-analytica-what-we-know-so-far/437392002/ consulté le 9 avril 2018.

[1032] Susan W. Brenner, « Cybercrime, cyberterrorism and cyberwarfare », *Revue internationale de droit pénal*, 2006/3 (Vol. 77), pp. 453-471. URL : https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm consulté le 5 janvier 2018.

[1033] Observatoire national de la délinquance et des réponses pénales, La *criminalité en France*, *Rapport 2011*, Novembre 2011, CNRS éditions.

[1034] Myriam Quémener, « Justice et cybercriminalité : état des lieux et préconisations », Annexes *La criminalité en France*, Rapport de l'Observatoire national de la délinquance et des réponses pénales 2011, Novembre 2011, CNRS éditions

A) La criminalité augmentée par le numérique

Les nouvelles technologies de l'information et de la communication ou NTIC que nos voisins anglo-saxons dénomment *information and communication technologies* ou *ICT* sont utilisées par les délinquants pour perpétuer leurs délits. La technologie change, mais le délit demeure. Le délinquant peut être un escroc, un fraudeur, un espion, un harceleur ou un maître chanteur qui profite du cyberespace pour réaliser son infraction. Le crime ou le délit ne sont pas nouveaux et liés à la société numérique, seul le modus vivendi diffère. Les conséquences peuvent être augmentées par l'utilisation des techniques numériques. La menace de publication de photos ou de vidéo attentant à l'image d'une personne peut s'assimiler à un chantage. Cette même divulgation peut être aussi un acte de vengeance.

Comme le relève l'INHESJ[1035] dans son rapport 2013[1036], pour les infractions commises en utilisant les NTIC, l'utilisation des techniques numériques ne constitue pas l'infraction principale. Par exemple, dans le cas d'une atteinte sexuelle commise sur un mineur de moins de 15 ans par un majeur mis en contact par Internet, l'infraction retenue sera l'atteinte sexuelle. En effet, pour certaines infractions, le Code pénal prévoit que « *lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de télécommunications* », les peines peuvent être aggravées. En cas de viol, la peine encourue passe de 15 ans[1037] à 20 ans de réclusion criminelle[1038]. Mais, cette aggravation des peines est déjà prévue par le même article, en cas de viol d'un mineur de 15 ans. Donc, dans l'exemple de l'INHESJ, l'infraction principale retenue et sanctionnée reste le viol d'un mineur de 15 ans quel que soit le moyen utilisé pour la mise en contact, l'utilisation des NTIC comme moyen de réalisation du délit est neutre dans ce cas. Mais en cas d'agression sexuelle sans viol, ce moyen n'est plus neutre et la peine encourue passe de cinq ans d'emprisonnement[1039] à sept ans[1040].

L'incrimination reste due à la réalisation de l'infraction principale, quel que soit le moyen utilisé pour réaliser ou non le délit ou le crime. Certaines des peines encourues peuvent être

[1035] Institut National des Hautes Études de la Sécurité et de la Justice.
[1036] http://www.inhesj.fr/sites/default/files/ondrp_rapport_2013.pdf consulté le 4 juillet 2016.
[1037] Code pénal, article 222-23.
[1038] Code pénal, article 222-24.
[1039] Code pénal, article 222-27.
[1040] Code pénal, article 222-28.

aggravées si les techniques informatiques ont été utilisées pour faciliter le délit, mais cette utilisation peut être pénalement masquée par d'autres facteurs aggravants.

Les atteintes à la dignité et à la personnalité regroupent des infractions très diverses dans le Code pénal. Celles commises ou facilitées par l'usage d'Internet sont principalement des actes d'injures, de discrimination ou de diffamation. Elles relèvent de la loi du 29 juillet 1881 sur la liberté de la presse, loi plusieurs fois modifiée et complétée et dont l'adaptation aux NTIC a été réalisée dans le cadre de la loi pour la confiance dans l'économie numérique[1041]. En 2016, sur les 5 millions de victimes d'injures, 5% des injures ont été proférées par téléphone et 2% par courrier électronique ou autre. Concernant les menaces, sur les 1,8 millions estimés de personnes ayant subi des menaces, 10% des menaces sont accomplies par téléphones, 6% par courrier électronique ou via les réseaux sociaux[1042]. Mais seules 74 563 déclarations d'injures et menaces ont été enregistrées en 2016 dans le fichier de la main courante informatisée[1043]. Dans la pratique, peu de personnes injuriées ou menacées portent plainte.

B) La criminalité issue du numérique

Les atteintes aux droits de la personne, dus à des traitements informatiques sont liées à la loi informatique et libertés, et ne peuvent pas être commises par des moyens traditionnels, non numériques. Les infractions nouvelles liées aux systèmes informatiques et aux systèmes de traitement automatisé des données sont les accès frauduleux, l'altération d'un système[1044], l'attaque par déni de service ou les atteintes au droit de la personne par collecte ou usage frauduleux de données à caractère personnel.

Ces nouvelles infractions sont ce qu'il convient d'appeler des cyberattaques, nul ne peut les ignorer, le palais de l'Élysée a été la victime d'une de ces attaques en mai 2012 après que Bercy

[1041] Loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique* publiée au JORF n°0143 du 22 juin 2004 page 11168.

[1042] Source Observatoire national de la délinquance et des réponses pénales, « les atteintes aux personnes », Rapport annuel 2017, pp. 54-60. URL : https://inhesj.fr/sites/default/files/ondrp_files/publications/pdf/2017_RA_Partie%20atteintes%20aux%20personnes.pdf consulté le 27 février 2018.

[1043] Jean-Luc Besson, « Les signalements des usagers dans la main courante informatisée de la police nationale entre 2008 et 2016 », La note de l'ONDRP n° 23, février 2018, p. 3. URL : https://inhesj.fr/sites/default/files/ondrp_files/publications/pdf/note_23.pdf consulté le 28 février 2018.

[1044] Incriminations initialement créées par la loi Godfrain.

en a été une victime quelques mois auparavant. Les techniques utilisées peuvent être variées[1045]. Certaines techniques sont historiques et nées en quasi-simultanéité avec les innovations cibles, le phreaking[1046] et le hacking[1047], d'autres techniques sont plus modernes et ne sont apparues qu'avec Internet et la prolifération des messageries, le spamming[1048] et le phishing[1049]. D'autres attaques nécessitent des moyens techniques plus sophistiqués et une réelle préparation des attaques avec des moyens techniques plus ou moins complexes : l'attaque de l'homme du milieu[1050], les botnets[1051] et le déni de service[1052]. De nouvelles techniques appelées « ransonware » sont apparues en 2017[1053].

§ 2 - Des attaques facilitées par les techniques numériques : Cyberterrorisme et cyberguerre

Pour Richard Clarke, la cyberguerre a commencé, elle est globale[1054] et se joue des frontières. La cyberguerre est le fait des États constitués. Le cyberterrorisme est le fait de groupes non étatiques. Leur objectif est identique : s'introduire dans les systèmes d'information d'un pays ou d'une entreprise pour en prendre le contrôle et ainsi bloquer ou fausser les décisions. La spéculation financière s'exerçant sur l'Euro et les dettes des États montre quelle pression peut exercer une puissance extérieure sur les décisions des États, et donc des conséquences pour ses

[1045] Elisabeth Duval, « La cybercriminalité subie et combattue par un opérateur tel que SFR », Irène Bouhadana, William Gilles (Dir.), *Cybercriminalité, cybermenaces & cyberfraudes,* mars 2012, Éditions IMODEV, pp.196-201.
[1046] À l'origine, le phreaking consiste à pirater des systèmes de téléphonie filaire ou sans-fil.
[1047] Le hacking consiste en l'utilisation de techniques exploitant des failles et vulnérabilités d'un élément ou groupe d'éléments d'un système d'information pour le pénétrer et s'y maintenir dans un but malveillant ou non.
[1048] Le spamming consiste en l'envoi d'un même message électronique non sollicité à un destinataire ou à un grand nombre de destinataires au risque de les importuner.
[1049] Le but du phishing ou hameçonnage est d'obtenir d'une personne des informations confidentielles qui vont permettre de lui dérober de l'argent ou d'usurper son identité pour pénétrer un système sécurisé.
[1050] L'attaque de l'homme du milieu, en anglais *man in the middle attack*, consiste à intercepter des communications entre deux parties, sans qu'aucune des parties ne puisse détecter cette interception.
[1051] Le botnet est un réseau de robots informatiques qui peut être utilisé pour des raisons malveillantes, envoi en masse de spams ou attaques par déni de service.
[1052] L'objectif d'une attaque en déni de service est de saturer et donc de rendre indisponible un service à ses utilisateurs légitimes.
[1053] Cette technique consiste à s'introduire dans un ordinateur et à rendre indisponibles les fichiers en les cryptant. Une rançon est demandée pour décrypter ces fichiers et les rendre utilisables à nouveau. Deux attaques massives de ransonware ont eu lieu au niveau mondial en 2017.
[1054] Richard A. Clarke and Robert K. Knake, *Cyber war, the next threat to national security and what to do about it,* Harper Collins Publishers 2010, p. 20.

citoyens. Une rumeur a des conséquences immédiates en termes de confiance[1055] et peut donc provoquer une fluctuation immédiate des cours de bourse, des monnaies ou des taux d'emprunt. La liberté globale des États se trouve alors entravée par ces rumeurs, la liberté des citoyens s'en trouve par ricochet concernée et affaiblie.

L'altération d'un message peut avoir des conséquences dramatiques. Le 13 juillet 1870, l'altération de la dépêche d'Ems par Bismarck soulève une tempête dans l'opinion française comme dans l'opinion allemande. Le 19 juillet, la France déclare la guerre à l'Allemagne[1056] avec des conséquences historiques qui amèneront les deux guerres mondiales du vingtième siècle et la montée du nazisme en Allemagne.

Le contrôle de l'informatique par les États est indispensable et nécessaire pour leur sécurité. Qiao Liang écrit[1057] : « *Il ne fait aucun doute que l'apparition de l'informatique a été une innovation bénéfique pour la civilisation humaine. C'est à ce jour la seule chose qui puisse insuffler à la plaie technique qui s'est échappée de la boîte de Pandore une plus grande énergie, avec en même temps le pouvoir magique permettant de la contrôler. Il se trouve qu'à l'heure actuelle se pose la question de savoir qui disposera du pouvoir avec lequel contrôler l'informatique* ».

La notion de sécurité des États se retrouve au centre des préoccupations des gouvernements qui doivent faire face à un risque réel et mal perçu par les forces de sécurité traditionnelles, risque protéiforme et difficile à circonscrire. Internet, employé comme une arme, incarne le principe des conflits asymétriques. Les parties prenantes ne sont pas de même nature juridique : un État, une entreprise, un collectif de militants, un groupe terroriste ou même un individu isolé. La sécurité globale des États devient une des conditions de la jouissance des libertés, mais au nom de la protection des libertés, les États tendent à restreindre ces libertés pour contrôler les individus[1058].

[1055] Une fausse information concernant une société cotée en bourse peut avoir un impact sur son cours de bourse à la baisse ou à la hausse. Vinci a été ainsi victime de la publication d'un faux communiqué de presse le 22 novembre 2016 à 16 h 5. L'action a perdu 18,28 % à la suite de cette publication alors que son cours était en hausse de 0,28 % avant 16 h 5 (source Le Monde, 23 novembre 2016).

[1056] « 13 juillet 1870 La dépêche d'Ems », *Herodote.net,* URL : https://www.herodote.net/13_juillet_1870-evenement-18700713.php consulté le 5 janvier 2018.

[1057] Qiao Liang et Wiang Xiangsui, *La guerre hors limites*, Rivages poche/Petite bibliothèque édité en 1999 pour la version chinoise et 2003 pour la version française, p. 35.

[1058] Didier Peyrat, « Société, liberté, sécurité », *Le Débat*, 2003/5 (n° 127), pp. 94-103. URL : https://www.cairn.info/revue-le-debat-2003-5-page-94.htm consulté le 5 janvier 2018.

A) Les attaques visant les États

En 2007, l'Estonie (dont l'e-administration est l'une des plus développées d'Europe) a été le premier État à subir des attaques informatiques de grande ampleur. L'administration estonienne, des banques et des journaux ont été paralysés durant plusieurs semaines par l'envoi massif de requêtes informatiques saturant les ordinateurs, serveurs et réseaux. Ces attaques faisaient suite au déplacement d'une statue symbolique pour la minorité russe du pays[1059].

Dans son livre[1060], Richard Clarke relate plusieurs galops d'essai (*trial runs*) d'attaques entre États : 6 septembre 2007 en Syrie, défense aérienne aveuglée ; avril 2007 en Estonie, déni de service[1061] ; 7 août 2008 en Géorgie, prise de contrôle des accès Internet ; 4 juillet 2009 infection de 40 000 PC aux États-Unis d'Amérique et en Corée du Sud par un botnet. Plus récemment, en réponse à l'interruption du site MegaUpload, des attaques concertées émanant du collectif Anonymous[1062], ont ciblé plusieurs sites gouvernementaux : les sites de l'HADOPI, de l'Élysée, des ministères de la Justice et de la Défense en France, les sites du FBI, du département de la justice et de la maison blanche aux États-Unis. Ces attaques sont effectuées en représailles de décisions non acceptées par des groupes de pression qui tentent ainsi d'entraver la liberté de gouverner et décider des États.

L'OTAN s'est dotée dès 2008, d'une direction spéciale pour lutter contre ces risques après les attaques contre l'Estonie[1063]. Mais, la coordination au niveau des États ne semble pas à l'ordre du jour. La coopération et l'échange d'informations entre États ne peut être crédible tant que certains États utilisent leur avance technologique dans ce domaine pour attaquer d'autres États : Israël, Chine, Russie, États-Unis d'Amérique, mais aussi Corée du Nord.

[1059] Laurent Zecchini, « Les cyberattaques massives d'origine russe contre l'Estonie préoccupent l'Alliance atlantique », 19 mai 2007, *Le Monde.fr*, URL : http://www.lemonde.fr/europe/article/2007/05/19/les-cyberattaques-massives-d-origine-russe-contre-l-estonie-preoccupent-l-alliance-atlantique_912244_3214.html consulté le 5 janvier 2018.

[1060] Voir supra

[1061] Voir supra

[1062] « Fermeture de Megaupload: Les Anonymous contre-attaquent », 20 janvier 2012, 20 minutes, URL : http://www.20minutes.fr/high-tech/863304-20120120-fermeture-megaupload-anonymous-contre-attaquent consulté le 5 janvier 2018.

[1063] Nicolas Arpagian, « Les parties prenantes de la cybersécurité », dans *La cybersécurité.* Paris, Presses Universitaires de France, « Que sais-je ? », 2015, pp. 77-99. URL : https://www.cairn.info/la-cybersecurite--9782130652199-page-77.htm consulté le 5 janvier 2018.

Les États ont longtemps occulté les cyberrisques. En mars 2011, le ministère de l'Économie a dû reconnaître avoir été l'objet d'une cyberattaque[1064] lors de la préparation d'un G20, Groupe des chefs d'État ou de gouvernement des 20 principaux États mondiaux. Des informations importantes ont ainsi été obtenues par les pirates. Plusieurs ordinateurs ont été infectés avant que l'attaque ne soit constatée.

En 2011, l'infection par le virus Stuxnet des installations nucléaires de l'Iran met en cause Israël et les États-Unis d'Amérique[1065]. Ces attaques vers les États peuvent être des attaques criminelles, ourdies par des mafias ou des groupes terroristes, mais aussi par d'autres États comme le laissent supposer le virus STUXNET ou plus récemment les attaques semblant provenir de Russie pendant les élections américaines de 2016[1066] ou françaises de 2017, avec violation de messageries personnelles et intrusion dans des ordinateurs des partis politiques. Ces attaques, quand elles sont dévoilées, sont toujours minimisées pour des raisons de sécurité et de secret.

B) Les attaques visant l'économie et l'industrie

Ces mêmes techniques peuvent être utilisées au niveau des entreprises pour l'espionnage industriel en complément des techniques classiques. Ces attaques lorsqu'elles sont découvertes sont rarement divulguées, car elles nuisent à l'image de la société.

En mars 2008, une chaîne de magasins d'alimentation américaine a été victime d'une attaque informatique qui a permis de dérober les informations de plus de 4,2 millions de cartes bancaires. Un logiciel malveillant était installé dans tous les magasins de la chaîne en Nouvelle-Angleterre et dans l'État de New York, et dans la majorité de ceux de Floride. Il interceptait les données au moment où elles étaient transmises aux banques[1067].

[1064] Article « Le ministère de l'Economie et des Finances, victime d'une attaque informatique » du 7 mars 2011 dans *Libération.fr* à http://www.liberation.fr/economie/01012324121-le-ministere-de-l-economie-et-des-finances-victime-d-une-attaque-informatique consulté le 5 mai 2012

[1065] Philippe Rivière, Article « Cyber-attaque contre Téhéran », *Le Monde* in http://www.monde-diplomatique.fr/2011/03/RIVIERE/20197 mars 2001, consulté le 5 mai 2012

[1066] *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* disponible à https://www.dni.gov/files/documents/ICA_2017_01.pdf et consulté le 16 juin 2017.

[1067] In http://www.risques.gouv.fr/risques/autre-risque/Cyber-risques/ lu le 28 avril 2012, non disponible le 9 avril 2018.

En mai 2011, le piratage du site de SONY a permis aux pirates de s'emparer des coordonnées des abonnés aux jeux de SONY[1068]. SONY a dû interrompre durant plusieurs jours ses services en lignes Playstation Network et Qriocity. Certains services ont été fermés pendant plusieurs semaines, entraînant des pertes pécuniaires, mais aussi dégradant l'image de Sony.

Entre les 8 et 9 avril 2015, la chaîne de télévision francophone TV5 Monde[1069] a dû suspendre ses émissions après une cyberattaque revendiquée par un groupe se réclamant de l'organisation État islamique ou Daesh. Cette attaque vise l'infrastructure de diffusion de TV5 Monde. Les messageries disparaissent ensuite des serveurs puis le site Internet de la chaîne et ses comptes Twitter et Facebook sont piratés. Dans l'année 2015, l'ANSSI a enregistré 4 000 signalements et traité une vingtaine d'incidents majeurs de sécurité[1070].

En mai 2017, une attaque d'envergure mondiale a été révélée et met en jeu un nouveau type de ver : le RansonWare[1071]. Ce ver nommé WannaCry utilise une faille de sécurité de Windows pour se propager, il rend inaccessibles les fichiers en les codant et demande une rançon pour les décoder et les rendre de nouveau accessibles. Il aurait fait plus de 200 000 victimes dans 150 pays[1072]. En France, ce RansonWare a provoqué l'arrêt des chaînes de production chez Renault. La faille de sécurité semblait connue depuis plusieurs années de la NSA qui l'utilisait pour infiltrer certains ordinateurs[1073]. Cette révélation montre le rôle ambigu que peuvent jouer les agences de renseignement dans le domaine de la cybercriminalité.

D'autres attaques peuvent consister en la diffusion de fausses informations (*fake news* en anglais) afin d'agir sur les cours de bourse[1074] ou d'influencer des discussions liées à des fusions-acquisitions. Ces fausses nouvelles ont été largement utilisées durant les campagnes électorales présidentielles américaines de 2016 et françaises de 2017[1075].

[1068] « Piratage Sony – Tous les détails sur ce qui s'est vraiment passé », *Korben,* URL : https://korben.info/piratage-sony-psn.html consulté le 5 janvier 2018.

[1069] Sébastien Baer, *Que devient TV5 Monde après la cyberattaque ?* publié le 25 juillet 2015 at http://www.franceinfo.fr/emission/ils-ont-fait-l-actu/2015-ete/que-devient-tv5-monde-apres-la-cyberattaque-23-07-2015-07-25 lu le 7 décembre 2015.

[1070] Source ANSSI, *Rapport d'activité 2015,* disponible à l'URL : https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf consulté le 5 janvier 2018.

[1071] http://www.teachthought.com/current-events/global-cyber-attack-appeared-synchronized-ransonware-driven/ consulté le 17 juin 2017.

[1072] Source journalistique.

[1073] « *Cyberattaque WannaCry : Microsoft met en cause la NSA et veut une "convention de Genève numérique"* », HUFFPOST, 15 mai 2017, à http://www.huffingtonpost.fr/2017/05/15/cyberattaque-microsoft-met-en-cause-la-nsa-et-veut-une-convent_a_22086836/ consulté le 17 juin 2017.

[1074] Voir supra la manipulation de cours de Vinci.

[1075] Publication de faux messages au milieu de messages authentiques piratés dans les ordinateurs de EnMarche!

C) Les attaques visant les personnes physiques

Les attaques aux personnes physiques consistent à obtenir des informations personnelles permettant par usurpation d'identité partielle (identification et mot de passe) ou totale (vol de l'état civil) de capter des biens et valeurs de personnes physiques : achats avec paiement par cartes bancaires, transferts de fonds, etc.

Les moyens couramment utilisés sont : le phishing qui consiste en envoyant un message électronique imitant un message officiel d'une banque ou d'un organisme d'État, à récupérer les informations confidentielles permettant d'accéder à un compte bancaire ou d'utiliser une carte de crédit ; l'escroquerie basée sur l'envoi de messages jouant sur la naïveté ou la crédulité qui sollicitent des transferts de petites sommes récompensées après réalisation de l'opération objet du message initial, en général transfert d'une somme importante dont un certain pourcentage est réservé à la personne sollicitée, mais ce peut être aussi l'installation d'un logiciel malveillant qui efface les données de l'ordinateur et propose de les récupérer moyennant le paiement d'une rançon (RansonWare)[1076].

Toutes ces attaques aux personnes physiques relèvent de la cybercriminalité, mais elles restent souvent hors de portée des tribunaux pénaux faute d'en appréhender les auteurs, souvent localisés dans des pays où la législation anti-cybercriminalité est inexistante ou balbutiante[1077].

Cette cybercriminalité se double depuis plusieurs années du terrorisme. Internet est un vecteur de propagation du terrorisme. Depuis les attentats du 11 septembre 2001 à New York, de nombreux pays ont durci leur législation pénale après avoir fait le constat que les membres de groupes terroristes avaient largement recours aux nouvelles technologies. Souvent, ce sont des moyens d'investigation, comme les écoutes ou la captation de données, qui sont mis à la disposition des enquêteurs sous contrôle d'un magistrat, ou sur décision administrative.

[1076] Pour les personnes physiques, les sommes sont minimes en cas de paiement immédiat mai sont augmentées en cas de non-paiement. Ces RansonWare existaient avant l'attaque de WannaCry dirigée vers les entreprises.

[1077] Eugène Kaspersky, « Défis de la cybercriminalité », *Sécurité globale*, 2008/4 (N° 6), pp. 19-28. URL : https://www.cairn.info/revue-securite-globale-2008-4-page-19.htm consulté le 5 janvier 2018.

Sous-section 2. La riposte des États, un difficile équilibre entre sécurité et liberté

Nicolas Arpagian écrit : « *La cybersécurité devient la condition nécessaire du développement de nos sociétés modernes. Au détriment, souvent, du droit individuel à la vie privée* »[1078].

Depuis les attentats du 11 septembre 2001, les États ont pris conscience des risques d'attentats terroristes à grande échelle et de l'utilisation d'Internet pour leur préparation et le recrutement des terroristes. Afin de se protéger, des dispositions particulières ont été prises. Certaines de ces dispositions ont pour résultat de réduire les libertés individuelles[1079]. Aux États-Unis d'Amérique, le *USA Patriot Act* ou « *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* »[1080] est une loi antiterroriste qui a été votée par le Congrès des États-Unis et signée par George W. Bush le 26 octobre 2001, soit à peine plus d'un mois après ces attentats. L'un des axes centraux de ce long texte de 132 pages est d'effacer la distinction juridique entre les enquêtes effectuées par les services de renseignement extérieur (La Central Intelligence Agency ou CIA ou la National Service Agency ou NSA) et les agences fédérales responsables des enquêtes criminelles (Federal Bureau of Investigation ou FBI) dès lors qu'elles impliquent des terroristes étrangers. Elle crée aussi les statuts de combattant ennemi et combattant illégal, qui permettent au gouvernement des États-Unis de détenir sans limites et sans inculpation toute personne soupçonnée de projet terroriste[1081], renonçant ainsi au principe de sûreté et d'habeas corpus[1082] dont l'origine anglo-saxonne remonte à 1679 et qui garantit la liberté individuelle des citoyens en les préservant des arrestations et détentions arbitraires.

[1078] Nicolas Arpagian, *La Cybersécurité*, Presses universitaires de France, 2010, p. 7.

[1079] Virginie Gautron, David Monniaux, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », *Archives de politique criminelle*, 2016/1 (n° 38), pp. 123-135. URL : https://www.cairn.info/revue-archives-de-politique-criminelle-2016-1-page-123.htm consulté le 9 avril 2018.

[1080] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT) Act of 2001, Public law 107-56-Oct. 26, 2001.

[1081] Jean-Claude Paye, « L'état d'exception : forme de gouvernement de l'Empire ? », *Multitudes*, 2004/2 (nº 16), pp. 179-190. URL : https://www.cairn.info/revue-multitudes-2004-2-page-179.htm consulté le 9 avril 2018.

[1082] USA Patriot Act, Title IV, Subtitle B, Sec. 4012. *Mandatory detention of suspected terrorists, habeac corpus, judicial review.*

La France s'est dotée avec les lois LOPSI 1[1083] et LOPPSI 2[1084] puis les lois de lutte contre le terrorisme[1085] et la loi sur le renseignement[1086] de dispositions lui permettant de lutter contre le terrorisme et les atteintes à la sécurité. Une loi a introduit dans le droit commun les dispositions exceptionnelles prévues pour l'État d'urgence[1087]. Ces lois rendent légales certaines pratiques de surveillance des personnes pour lesquelles la France a été antérieurement condamnée par la Cour européenne des droits de l'homme[1088], faute d'autorisation légale à utiliser ces pratiques attentant aux libertés individuelles.

En 2012, avec l'affaire Mohamed Merah, le grand public a pu découvrir qu'un individu pouvait être surveillé par les services secrets lors de ses voyages dans un pays étranger, mais aussi lors des consultations sur Internet de sites particuliers, sa messagerie pouvant être également scrutée. Le Président de la République M. Sarkozy a, lors de cette affaire Merah, annoncé un projet de loi permettant de condamner pénalement ces agissements avant toute réalisation effective d'actes criminels, plaçant ainsi la France au niveau des États-Unis d'Amérique de M. Georges W. Bush et de l'*USA Patriot Act*. La fiction décrite dans *Minority Report*[1089] se rapproche de la vie quotidienne, la réalisation de l'acte n'est plus nécessaire pour la répression pénale. En 2016, le Conseil constitutionnel a considéré qu'il était non conforme à la Constitution de punir pénalement la simple consultation de sites djihadistes sur Internet[1090] faute de pouvoir déceler une intention terroriste dans cette seule consultation.

La loi sur le renseignement[1091] a légalisé certaines pratiques utilisées par les services de renseignement dans la prévention du terrorisme, la surveillance des communications

[1083] Loi nº 2002-1 094 du 29 août 2002 *d'orientation et de programmation pour la sécurité intérieure* publiée au JORF du 30 août 2002 p. 14398.
[1084] Loi nº 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure* publiée au JORF nº0062 du 15 mars 2011 p. 4582.
[1085] Loi nº 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* publiée au JORF nº0020 du 24 janvier 2006 p. 1129.
[1086] Loi nº 2015-912 du 24 juillet 2015 *relative au renseignement,* publiée au JORF nº0171 du 26 juillet 2015 p. 12735.
[1087] Loi n° 2017-1510 du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme* publiée au JORF n°0255 du 31 octobre 2017.
[1088] Cour européenne des droits de l'homme, 31 mai 2005, nº 59842/00, *Vetter c/ France.*
[1089] Minority Report (Rapport minoritaire au Québec) est un film de science-fiction américain réalisé par Steven Spielberg, sorti sur les écrans en 2002.
[1090] Conseil constitutionnel, Décision nº 2016-611 QPC du 10 février 2017, *M. David P. [Délit de consultation habituelle de sites Internet terroristes]*.
[1091] Loi nº 2015-912 du 24 juillet 2015 *relative au renseignement,* publiée au JORF nº0171 du 26 juillet 2015 p. 12 735 après la décision du Conseil constitutionnel nº 2015-713 DC du 23 juillet 2015.

internationales ayant quant à elle nécessité une loi complémentaire[1092] suite à la décision du Conseil constitutionnel déclarant non conforme à la Constitution cette disposition présente dans la loi relative au renseignement. Les moyens mis à disposition par la société numérique facilitent cette surveillance des individus. Sous couvert de sécurité et de prévention du terrorisme, les États cherchent à se doter de moyens de contrôle des individus en réduisant leurs libertés, en surveillant leurs déplacements et en contrôlant leur environnement, tous ces moyens sont facilités par les techniques numériques et des progrès dont ces techniques vont bénéficier dans les années à venir.

En Californie, un logiciel de prévision de l'exécution des délits est utilisé par la police de Santa Cruz et de Los Angeles[1093], logiciel de prédiction des délits mis au point par des scientifiques de l'UCLA[1094]. Ces logiciels sont aujourd'hui utilisés par plusieurs forces de police au niveau mondial. Des logiciels de rapprochement et d'analyse de différentes entrées d'une base de données permettent de mettre en relation des événements, des personnes ou des lieux au cours d'une enquête. Le logiciel ANACRIM est ainsi utilisé par les forces de police en France, l'utilisation d'un tel logiciel est autorisée par la loi,[1095] mais elle doit être déclarée à la CNIL comme tout traitement automatique de données à caractère personnel[1096].

[1092] Loi nº 2015-1 556 du 30 novembre 2015 *relative aux mesures de surveillance des communications électroniques internationales* publiée au JORF nº0278 du 1 décembre 2015 p. 22 185, après la décision du Conseil constitutionnel nº 2015-722 DC du 26 novembre 2015.

[1093] Elena Sender « Californie : la police connaît déjà l'heure du crime » dans *Sciences et Avenir* nº782 d'avril 2012, pp. 68-73

[1094] UCLA University of California, Los Angeles.

[1095] Loi nº 2003-239 du 18 mars 2003 *pour la sécurité intérieure*, Article 21 « *I. - Les services de la police nationale et de la gendarmerie nationale peuvent mettre en œuvre des applications automatisées d'informations nominatives recueillies au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'État, afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs* ».

[1096] ANACRIM a d'abord été utilisé sans déclaration légale à la CNIL par la Gendarmerie, avant d'être régularisé auprès de la CNIL, par la Loi relative au traitement de la récidive des infractions pénales, en date du 12 décembre 2005. La loi autorise l'enregistrement de personnes même sans indices, à l'appréciation des enquêteurs.

§ 1 - Les restrictions administratives à la protection de la vie privée

Outre les exceptions introduites dans les législations nationales et internationales pour protéger certains droits, des lois spécifiques ont été adoptées durant les dix premières années de ce siècle pour renforcer la sécurité et la sûreté en réduisant ou limitant la protection des individus ou celle de leur vie privée[1097]. Ces lois spécifiques sont souvent promulguées en réaction à un fait particulier, mobilisateur de l'opinion publique. Le délai entre le fait générateur, l'événement médiatisé, et la promulgation de la loi peut être très court, une procédure d'urgence étant alors mise en œuvre.

Le texte emblématique de la politique sécuritaire mise en place par les États-Unis est le USA Patriot Act ou « *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* »[1098]. Ce texte a été promulgué par George W. Bush le 26 octobre 2001, soit 45 jours après les attentats du 11 septembre 2001. Dans la pratique, cette loi autorise les services de sécurité à accéder aux données informatiques détenues par les particuliers et les entreprises, sans autorisation préalable d'un juge et sans en informer les utilisateurs[1099].

Au niveau français, il existe aussi des textes adoptés après les attentats, textes qui restreignent les droits des personnes relativement à la protection de leur vie privée. M. Sarkozy, ancien président de la République française, initiateur de nombreux textes répressifs soit comme ministre de l'Intérieur, soit comme Président de la République, a été mis sur écoutes téléphoniques pendant plusieurs mois par utilisation de ces lois, écoutes reconnues légales par la Cour d'appel de Paris le 7 mai 2015[1100], puis par la Cour de cassation le 22 mars 2016[1101].

L'une des premières lois promulguées en France est la loi d'orientation et de programmation pour la sécurité intérieure[1102]. Présentée en conseil des ministres le 10 juillet 2002, elle est défendue par Nicolas Sarkozy, ministre d'État, ministre de l'Intérieur. Examiné en urgence en

---

[1097] Marc-Olivier Padis, « Sécurité et terrorisme : un défi pour la démocratie », *Esprit*, 2006/8 (Août/septembre), pp. 67-69. URL : https://www.cairn.info/revue-esprit-2006-8-page-67.htm consulté le 2 janvier 2018.

[1098] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT) Act of 2001, Public law 107-56-Oct. 26, 2001.

[1099] Daniel Sabbagh, « Sécurité et libertés aux États-Unis dans l'après-11 septembre : un état des lieux », *Critique internationale*, 2003/2 (nº 19), pp. 17-23. URL : https://www.cairn.info/revue-critique-internationale-2003-2-page-17.htm consulté le 2 janvier 2018.

[1100] Chambre de l'instruction de la cour d'appel de Paris, arrêt nº5, 7 mai 2015.

[1101] Cour de cassation, Chambre criminelle, 22 mars 2016, pourvoi nº15-83.207, Publié au bulletin.

[1102] Loi nº 2002-1 094 du 29 août 2002 *d'orientation et de programmation pour la sécurité intérieure* (LOPSI).

juillet à l'Assemblée nationale, le projet de loi est adopté conforme par le Sénat, et déclaré conforme à la Constitution par le Conseil constitutionnel le 22 août 2002[1103]. Promulguer une loi en moins de 6 semaines reste un exploit en France où certaines lois demandent plusieurs années avant leur promulgation. Pour ne prendre qu'un exemple, la directive européenne 95/46/CE qui harmonisait les législations sur la protection des données personnelles au niveau européen et qui devait être transposée en droit français en octobre 1998 au plus tard, ne l'a été qu'en 2004, soit plus de cinq ans après, en dépit des pressions de la Commission européenne.

Outre des réorganisations des services de sécurité et de police français, cette loi d'orientation permet notamment aux officiers de police judiciaire, si un magistrat l'autorise, « *d'accéder directement à des fichiers informatiques et de saisir à distance par la voie télématique ou informatique les renseignements qui paraîtraient nécessaires à la manifestation de la vérité* ». Dans les faits, cette loi autorise la police française à utiliser des chevaux de Troie ou tout autre dispositif pour intercepter des données. Ceci est encore plus explicite dans une seconde loi adoptée quelques années plus tard. Cette première loi d'orientation sera entérinée par la loi sur la sécurité intérieure adoptée en 2003[1104] à l'initiative de M. Sarkozy, ministre de l'Intérieur. Le fichage est fortement facilité pour les forces de l'ordre dans la nouvelle loi. Le Conseil constitutionnel a déclaré conforme à la Constitution cette loi[1105], mais a rappelé que « *dans le cadre de certaines enquêtes administratives, l'article 2 de la loi du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, en vertu duquel une décision administrative "impliquant une appréciation sur un comportement humain" ne peut être exclusivement fondée sur un traitement automatisé "donnant une définition du profil ou de la personnalité de l'intéressé"* » ainsi que le fait que chacun a droit à une vie familiale normale. Ainsi, un traitement automatique doit être validé par une personne physique et ne peut seul, être à la base d'une décision produisant un effet de droit sur une personne physique. Cette restriction oblige par exemple à faire valider par un officier ou agent de police judiciaire la constatation

[1103] Conseil constitutionnel, Décision n° 2002-460 DC du 22 août 2002 *Loi d'orientation et de programmation sur la sécurité intérieure*.
[1104] Loi nº 2003-239 du 18 mars 2003 *pour la sécurité intérieure* publiée au JORF nº66 du 19 mars 2003 p. 4761.
[1105] Conseil constitutionnel, Décision nº 2003-467 DC du 13 mars 2003 *Loi pour la sécurité intérieure*.

d'un excès de vitesse relevé par un radar automatique ou un stationnement gênant ou interdit révélé par une caméra de vidéosurveillance[1106].

Dix ans plus tard, le 14 mars 2011, une nouvelle loi d'orientation dite LOPPSI 2[1107] a été promulguée. Le Conseil constitutionnel a déclaré non conformes à la Constitution 13 de ses articles[1108], certaines dispositions déclarées conformes à la Constitution ont été assorties de réserves d'interprétation. Cette loi dispose d'un volet de lutte contre la cybercriminalité[1109] : l'usurpation d'identité sur Internet devient un délit puni d'un an d'emprisonnement et 15 000 euros d'amende[1110], mais un policier peut usurper une identité ou utiliser une identité fictive durant une enquête[1111] sans encourir de sanction ; il devient possible d'imposer aux fournisseurs d'accès à Internet le blocage de sites WEB[1112] publiant du contenu pédopornographique par décision d'une autorité administrative[1113] ; une liste noire des sites, non rendue publique, peut-être établie par l'administration, les fournisseurs d'accès à Internet sont quant à eux tenus de bloquer l'accès à ces sites ; une obligation de filtrage des adresses IP désignées par arrêté du ministre de l'Intérieur est créée ; la police, sur autorisation du juge des libertés, pourra utiliser tout moyen (physiquement ou à distance) pour s'introduire dans des ordinateurs et en extraire des données[1114] dans diverses affaires, allant de crimes graves (pédophilie, meurtre, etc.) au trafic d'armes, de stupéfiants, au blanchiment d'argent, mais aussi au délit « d'aide à l'entrée, à la circulation et au séjour irrégulier d'un étranger en France commis en bande organisée », sans le consentement des propriétaires des ordinateurs. Cette possibilité a été utilisée pour retrouver un terroriste solitaire[1115], assassin de plusieurs personnes, mais aussi pour surveiller des personnes et prévenir leur départ vers la Syrie.

[1106] Cette obligation a été rappelée par la CNIL lors de la polémique soulevée lors de la rentrée universitaire de 2017 concernant la plateforme APB (CNIL, Décision n° MED-2017-053 du 30 août 2017 *mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation*).

[1107] Loi nº 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure.*

[1108] Conseil constitutionnel, Décision nº 2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*.

[1109] Loi n° 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure,* Chapitre II, art. 2 à 5.

[1110] Loi n° 2011-267 du 14 mars 2011, Art. 2.

[1111] Ibid. Art. 27 I.

[1112] Ibid. Art. 4.

[1113] Initialement, la commission des lois avait prévu le recours au juge pour ce blocage administratif (« *L'autorité administrative notifie, après accord de l'autorité judiciaire* », article 4). Cependant, ce contrôle du juge a été supprimé en seconde lecture par l'Assemblée nationale.

[1114] Loi n° 2011-267 du 14 mars 2011, Art. 36.

[1115] Lire sur le sujet Patricia Tourancheau, « Merah : des erreurs en série », 1 octobre 2012, *Libération.fr*, URL : http://www.liberation.fr/societe/2012/10/01/merah-des-erreurs-en-serie_850210 consulté le 2 janvier 2016.

La loi LOPPSI 2 augmente les moyens de vidéosurveillance dans les lieux publics[1116], mais étend aussi les possibilités d'écoutes téléphoniques : les préfets peuvent utiliser la vidéosurveillance, notamment en cas de grands événements publics, comme les rencontres sportives[1117] ; elle doit « favoriser la réalisation du plan de triplement des caméras installées sur le territoire »[1118] (environ 60 000 caméras prévues au niveau national) et « permettre aux services de police et de gendarmerie d'accéder aux images » ; dans les enquêtes sur la criminalité organisée, la police dispose de délais plus étendus pour les écoutes téléphoniques ; les enquêteurs peuvent placer des logiciels d'extraction de données sur les ordinateurs de suspects, sous le contrôle d'un juge d'instruction. Les données personnelles révélées par ces logiciels espions doivent être effacées à la clôture de l'enquête.

Ces deux lois, LOPSI et LOPPSI 2, montrent que sous couvert de lutte contre le terrorisme et la délinquance, les États tendent à réduire les droits des citoyens concernant la protection des données personnelles et la vie privée. Quelquefois, la lutte contre le terrorisme ne semble être qu'un alibi utilisé pour restreindre administrativement les libertés[1119]. La Constitution de la République française a confié[1120] à l'autorité judiciaire la garde des libertés individuelles, c'est-à-dire que seul le juge peut restreindre une liberté individuelle, raison pour laquelle de nombreuses mesures administratives attentatoires à cette liberté doivent préalablement recevoir l'assentiment d'un magistrat. Le Conseil constitutionnel a dans plusieurs de ses décisions précisé ce rôle : la réquisition administrative de données de trafic est autorisée pour prévenir le terrorisme, mais ne peut être utilisée pour la répression[1121] ; la transmission d'images de vidéosurveillance captées dans les espaces privés vers les forces de police et de gendarmerie a été censurée faute de garanties nécessaires à la protection de la vie privée des personnes[1122] ; l'interdiction d'accès à un site pédopornographique sur décision réglementaire n'a été acceptée

[1116] Loi n° 2011-267 du 14 mars 2011, Art. 18.
[1117] Ibid. Art. 21.
[1118] Extrait de l'exposé des motifs du projet de loi, pp. 11-12 disponible à l'URL : http://www.assemblee-nationale.fr/13/pdf/projets/pl1697.pdf consulté le 27 février 2018.
[1119] François Chobeaux, « La légalité n'excuse pas tout. Le projet de prévention de la délinquance », *VST - Vie sociale et traitements*, 2004/4 (n° 84), pp. 35-37. URL : https://www.cairn.info/revue-vie-sociale-et-traitements-2004-4-page-35.htm consulté le 2 janvier 2018.
[1120] Constitution, article 66.
[1121] Conseil constitutionnel, Décision 2005-532 DC du 19 janvier 2006 *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, sur l'article 6, considérants n^os^ 2-13.
[1122] Conseil constitutionnel, Décision n° 2010-604 DC du 25 février 2010 *Loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public*, sur l'article 5, considérants n^os^ 19-23.

que parce qu'une telle décision est susceptible de recours devant le juge compétent[1123] ; la surveillance de la voie publique par des personnes privées a été censurée[1124] ; la possibilité pour la police municipale de procéder à des vérifications d'identité a été censurée, car seule la police judiciaire est placée sous le contrôle et la direction de l'autorité judiciaire[1125] ; le traitement de données recueillies à l'occasion d'enquêtes a été autorisé, car placé sous le contrôle de l'autorité judiciaire pour son autorisation et parce que la durée de conservation de ces données est limitée dans le temps[1126] ; la mise en œuvre de la géolocalisation entourée de mesures de nature à garantir que, placées sous l'autorisation et le contrôle de l'autorité judiciaire, les restrictions aux garanties constitutionnelles ne sont pas disproportionnées au but recherché, est acceptée[1127] ; la délivrance d'autorisations de mesures de police administrative par le Premier ministre, après consultation d'une autorité administrative indépendante, ne porte pas d'atteinte à la liberté individuelle au sens de l'article 66 de la Constitution[1128]. Mais lors de la séance solennelle de rentrée de la Cour de cassation en janvier 2016, Bertrand Louvel, premier Président de la Cour de cassation, constatait que les nouvelles lois sécuritaires de lutte contre le terrorisme avaient ignoré le juge judiciaire au détriment du juge administratif[1129]. Comme le constatent Julien Bonnet et Agnès Roblot-Troizier, le Conseil constitutionnel s'en remet au contrôle du juge administratif dans le cadre de l'état d'urgence[1130].

Par ailleurs, lors de la transposition de la directive 95/46/CE pour la protection de la vie privée et des données à caractère personnel, la Commission de l'informatique et des libertés s'est vue privée d'une partie de ses prérogatives face au gouvernement alors que son pouvoir de sanction est renforcé vers les entreprises privées[1131]. Alors que pour toute entreprise, une autorisation préalable est nécessaire pour créer une application de traitement de données à caractère

[1123] Conseil constitutionnel, Décision n° 2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure, sur l'*article 4, considérants n^{os} 5-8.
[1124] Ibid. sur l'article 18, considérants n^{os} 14-19.
[1125] Ibid. sur l'article 92, considérants n^{os} 57-60.
[1126] Ibid. sur l'article 14, considérants n^{os} 67-73.
[1127] Conseil constitutionnel, Décision n° 2014-693 DC du 25 mars 2014 *Loi relative à la géolocalisation.*
[1128] Conseil constitutionnel, Décision n° 2015-713 DC du 23 juillet 2015 *Loi relative au renseignement*
[1129] Bernard Louvel, Audience solennelle de rentrée 2016 de la Cour de cassation, Discours disponible à l'URL : https://www.courdecassation.fr/publications_26/discours_tribunes_entretiens_2039/discours_2202/premier_president_7084/rentree_2016_33389.html, consulté le 15 juin 2017.
[1130] Julien Bonnet, Agnès Roblot-Troizier, « Droits fondamentaux et libertés publiques », *Les Nouveaux Cahiers du Conseil constitutionnel*, 2016/3 (N° 52), pp. 71-91. URL : https://www.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2016-3-page-71.htm consulté le 2 janvier 2018.
[1131] Florence Raynal, « De nouvelles dispositions pour protéger les données personnelles », *Documentaliste-Sciences de l'Information*, 2014/3 (Vol. 51), pp. 23-25. URL : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2014-3-page-23.htm consulté le 2 janvier 2018.

personnel, ces traitements sont autorisés par décret pour l'administration. Seul un avis de la Commission de l'informatique et des libertés est sollicité, le gouvernement peut passer outre à un avis défavorable, il doit seulement annexer l'avis motivé de la CNIL, favorable ou défavorable, à la publication du décret[1132]. Avec le Règlement général sur la protection des données, l'autorisation préalable est remplacée par le respect de certifications ou de règles éthiques prédéfinies[1133], mais les pouvoirs de sanction sont renforcés envers les sociétés privées. D'autres restrictions existent aussi au niveau international. Par exemple, l'Union européenne n'autorise pas le transfert des données à caractère personnel ni leur traitement hors du territoire de l'Union européenne, sauf par exception vers les États reconnus comme « adéquats » par la Commission européenne[1134], c'est-à-dire ceux ayant mis en place une législation similaire à celle existant dans l'Union. Toutefois, pour des raisons économiques, les principaux acteurs du WEB étant américains, ces transferts sont autorisés vers les acteurs apportant un niveau de protection suffisant via les « *Binding Corporate Rules* », les clauses contractuelles types ou l'adhésion aux règles du « Safe Harbor »[1135]. Ces dérogations n'apportent pas le niveau de protection garanti au sein de l'Union européenne. Une simple déclaration d'adhésion aux principes du Safe Harbor suffit pour les entreprises américaines. Cet accord de Safe Harbor a

[1132] Cf. Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 1. § 1 -B)1) L'assouplissement de la loi informatique et libertés.

[1133] 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)* Art. 40 et 42.

[1134] Article 9 du Règlement (EC) N° 45/2001

[1135] "*Safe Harbor Principles are a set of privacy and data protection principles that, together with a set of frequently asked questions (FAQs) providing guidance for the implementation of the principles, have been considered by the European Commission to provide an adequate level of protection.*
These principles were issued by the Government of the United States on 21 July 2000.
US organisations can claim that they comply with this framework. They should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) - under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce - or to the jurisdiction of another statutory body that will ensure compliance with the principles implemented in accordance with the FAQs".
Traduction en français par l'auteur : « Les principes de safe harbor reposent sur un ensemble de règles de protection de la vie privée et des données qui, associé à une série de questions fréquemment posées (FAQ) fournissant des conseils pour la mise en œuvre des principes, a été pris en compte par la Commission européenne pour fournir un niveau de protection adéquat.
« Ces principes ont été publiés par le Gouvernement des États-Unis le 21 juillet 2000.
« Les organisations américaines peuvent prétendre qu'elles sont conformes à ce cadre. Elles doivent divulguer publiquement leur politique de confidentialité et être soumises à la compétence de la Commission fédérale du commerce (FTC) - en vertu de l'article 5 de la Federal Trade Commission Act qui interdit les actes ou pratiques déloyaux ou trompeurs dans le commerce ou qui le concernent - ou à la juridiction d'un autre organe statutaire qui assurera le respect des principes mis en œuvre conformément aux FAQ ».

été invalidé par la Cour de justice de l'Union européenne[1136] pour protection insuffisante et remplacé par le « *Privacy Shield* »[1137].

De plus pour des raisons de sécurité et de lutte contre le terrorisme, des accords entre l'Union européenne et les États-Unis d'Amérique ont été conclus pour permettre le transfert vers les États-Unis des informations relatives aux passagers voyageant vers les États-Unis et contenues dans le Passenger Name Record ou PNR[1138], créé automatiquement par les compagnies aériennes, initialement pour des besoins de transfert d'information pour gérer les correspondances[1139]. Le PNR peut contenir indirectement des informations sensibles, par exemple la religion au travers des régimes, ou la santé. Au sein de l'Union européenne, cet accord négocié entre la Commission européenne et le gouvernement des États-Unis d'Amérique a fait l'objet de nombreuses critiques du G29[1140], entité qui regroupe les agences des États membres de protection des données personnelles. Le premier accord a été signé en mai 2004[1141], suite à son invalidation par la Cour de justice de l'Union européenne[1142], un nouvel accord a été renégocié en juillet 2007,[1143] mais ce nouvel accord reste controversé compte tenu du délai de rétention des informations par les agences américaines. En avril 2012, l'accord a été approuvé par le Parlement européen[1144] malgré des critiques concernant les recours insuffisants

[1136] Cour de justice de l'Union européenne (Grande Chambre), Arrêt du 6 octobre 2015, Affaire C-362/14, *Maximillian Schrems c/Data Protection Commisionner et Digital Rights Ireland Ltd*.

[1137] Marie-Andrée Weiss, « De la sphère au bouclier : qu'est-ce que le Privacy Shield ? », *I2D – Information, données & documents*, 2016/3 (Volume 53), pp. 20-22. URL : https://www.cairn.info/revue-i2d-information-donnees-et-documents-2016-3-page-20.htm consulté le 9 avril 2018.

[1138] Accord renégocié en 2011 et entré en vigueur le 1er juillet 2012.

[1139] Lorna Stefanick, « L'externalisation et la circulation transfrontalière des données : Défi de la protection des renseignements personnels dans le cadre du USA Patriot Act », *Revue Internationale des Sciences Administratives*, 2007/4 (Vol .73), pp. 583-603. URL : https://www.cairn.info/revue-internationale-des-sciences-administratives-2007-4-page-583.htm consulté le 9 avril 2018.

[1140] Groupe de travail « Article 29 », 01613/06/FR « *Avis 9/2006 sur la mise en œuvre de la directive 2004/82/CE du Conseil concernant l'obligation pour les transporteurs de communiquer au préalable les données relatives aux passagers (PNR) »*, adopté le 28 septembre 2006, accessible à http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp127_fr.pdf, consulté le 15 juin 2017.

[1141] Décision 2004/496/CE - Accord entre la Communauté européenne et les États-Unis d'Amérique - *Dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique.*

[1142] Cour de justice de l'Union européenne, Grande chambre, Arrêt du 30 mai 20016, Affaires C-317/04 et C-318/04 *Parlement européen c/ Conseil de l'Union européenne et Commission des Communautés européennes*.

[1143] Accord entre l'Union européenne et les États-Unis d'Amérique *sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007)* publié au Journal officiel n° L 204 du 04/08/2007 pp. 18-25.

[1144] Parlement européen, *Le Parlement européen donne son feu vert à l'accord PNR avec les États-Unis*, Communiqué de presse du 19 avril 2012, URL : http://www.europarl.europa.eu/news/fr/press-room/20120419IPR43404/le-parlement-europeen-donne-son-feu-vert-a-l-accord-pnr-avec-les-etats-unis consulté le 2 janvier 2012.

contre une utilisation inappropriée des données échangées[1145]. Ainsi un accord international, un traité, peut être négocié et conclu en dépit d'une inadéquation avec une législation nationale, et en droit international, un traité ratifié prévaut sur une législation nationale.

Face aux États qui maîtrisent les législations, le citoyen n'a que peu de moyens de lutter contre un usage abusif des données à caractère personnel et la violation légale de sa vie privée. Toutefois, un espoir est récemment venu de la Cour européenne des droits de l'homme qui a condamné la France pour avoir conservé dans ses fichiers de police des informations concernant un prévenu pour lequel un non-lieu avait été prononcé[1146], et de la Cour de justice de l'Union européenne qui a reconnu un certain droit à l'oubli pour les moteurs de recherche[1147] et a déclaré que l'accord PNR en cours de négociation entre le Canada et l'Union européenne ne pouvait pas être conclu sous sa forme actuelle[1148], mais sans remettre en cause le principe du transfert des données PNR dans le cadre de la lutte contre le terrorisme et la criminalité transnationale.

§ 2 - La dérive sécuritaire de la loi en matière de données personnelles

La législation concernant la protection des données à caractère personnel, tant au niveau européen avec la directive 95/46/CE que le Règlement général sur la protection des données, qu'en droit français avec la loi informatique et libertés, interdit ou limite les recoupements entre fichiers, les utilisations non conformes aux objectifs de la collecte pour lesquels il y a eu un consentement de la personne physique concernée, et le transfert de ces données vers un État qui n'a pas de législation équivalente à la législation européenne. Dans le cadre de la lutte contre le terrorisme ou le crime, ces protections sont atténuées, voire suspendues.

[1145] Valsamis Mitsilegas, « 8. Coopération antiterroriste États-Unis/Union européenne : l'entente cordiale », dans *Au nom du 11 septembre...Les démocraties à l'épreuve de l'antiterrorisme.* Paris, La Découverte, « Cahiers libres », 2008, pp. 118-130. URL : https://www.cairn.info/au-nom-du--9782707153296-page-118.htm consulté le 2 janvier 2018.

[1146] Cour Européenne des Droits de l'Homme, 18 septembre 2014, n° 21010/10, *Brunet c/ France*.

[1147] Cour de Justice de l'Union Européenne (grande chambre), arrêt du 13 mai 2014, affaire C-131/12 *Google Sapain SL c/ Agencia Española de Protección de Datos (AEPD)*.

[1148] Cour de justice de l'Union européenne, Grande chambre, Avis 1/15 du 26 juillet 2017.

A) Une collecte de masse

La loi LOPPSI 2[1149] met à disposition des forces de police et de gendarmerie le regroupement des données d'origine police (STIC) ou gendarmerie (JUDEX) afin de ne conserver qu'un traitement d'antécédents judiciaires et des fichiers d'analyse sérielle. Les personnes mises en cause dans une procédure judiciaire vont être ainsi fichées qu'elles soient victimes, comparses, accusées ou relaxées, et ce à partir de faits relevant d'une peine correctionnelle de cinquième catégorie[1150]. Les personnes recherchées seront également enregistrées dans ces fichiers de police[1151]. Pour des raisons de sécurité, il est ainsi permis à la police ou la gendarmerie de ficher progressivement toutes les personnes physiques présentes sur le territoire français, il suffira de porter plainte pour le vol d'un téléphone portable (il s'agit d'un délit) pour se retrouver enregistré pour quinze ans dans ce fichier centralisé[1152], accessible aux forces de police étrangères[1153].

Les attentats de 2015 ont fait découvrir au public le fichage des individus suspectés de radicalisation au travers de la fiche de signalement « S », fiche qui existait avant les attentats. Mais, le fichage à grande échelle de l'ensemble des citoyens français est en cours, en dehors des enquêtes administratives ou judiciaires, depuis octobre 2016 avec l'autorisation du traitement TES ou Titre électronique sécurisé. La création d'un tel traitement avait déjà été

[1149] Loi n° 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure,* art.11.

[1150] Loi nº 2005-1 549 du 12 décembre 2005 *relative au traitement de la récidive des infractions pénales* Article 30 : « *II. - Ces traitements peuvent contenir des données sur les personnes, sans limitation d'âge :*
« 1º A l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission d'une infraction mentionnée au premier alinéa du I ; l'enregistrement des données concernant ces personnes peut intervenir, le cas échéant, après leur condamnation ;
« 2º A l'encontre desquelles il existe des raisons sérieuses de soupçonner qu'elles ont commis ou tenté de commettre une infraction mentionnée au premier alinéa du I ;
« 3º Susceptibles de fournir des renseignements sur les faits au sens des articles 62, 78 et 101 du code de procédure pénale et dont l'identité est citée dans une procédure concernant une infraction mentionnée au premier alinéa du I ;
« 4º Victimes d'une infraction mentionnée au premier alinéa du I ;
« 5º Faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, prévue par l'article 74 du code de procédure pénale, ou d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte, prévue par les articles 74-1 et 80-4 du même code ».

[1151] Jean-Jacques Lavenue, « Anormalité, surveillance et fichiers de police », in Jean-Jacques Lavenue, Bruno Villabla, *Vidéo-surveillance et détection automatique des comportements anormaux*, Presses universitaires du Septentrion, pp. 235-260.

[1152] Lire à ce sujet la fiche éditée par la CNIL, « TAJ : Traitement d'Antécédents Judiciaires », *Les grands ficchiers en fiches,* 17 février 2015, disponible à l'URL : https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires consultée le 27 février 2018.

[1153] Dans le cadre de l'article 24 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

envisagée en 2012[1154], mais censurée par le Conseil constitutionnel[1155]. Cette création était prévue par l'article 5 de la loi 2012-410, son article 10 prévoyait l'accès à ces données pour les besoins de la prévention et de la répression des atteintes à l'indépendance de la Nation et à l'intégrité de son territoire. Ce traitement avait alors été dénoncé par la presse et les membres de l'opposition comme étant le « fichier des honnêtes gens »[1156]. Le gouvernement de 2012 avait alors renoncé à la création de ce fichier. En 2016, le gouvernement socialiste a autorisé la création dudit fichier[1157]. Ainsi, dans l'ambiance sécuritaire post 2015, un gouvernement socialiste autorise la création d'un fichier attentant à la liberté individuelle auquel s'était opposé l'opposition socialiste quelques années auparavant. Le fichier « des honnêtes gens » va permettre d'enregistrer, à terme, les données à caractère personnel, photo, empreintes digitales et état civil de l'ensemble des citoyens français puisque ces données sont collationnées lors de la demande d'une carte nationale d'identité ou d'un passeport, cette carte nationale d'identité n'est pas légalement obligatoire en France, mais tout citoyen doit pouvoir justifier de son identité et cette carte en est le moyen le plus usuel. Lors de la publication de cette ordonnance, le gouvernement a pris soin de publier l'avis sollicité du Conseil d'État[1158]. Dans cet avis, le Conseil d'État rappelle « *que la collecte et le traitement d'informations personnelles nominatives constituent une ingérence dans la vie privée des personnes, dont le droit au respect est garanti par l'article 2 de la Constitution et par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Une telle ingérence ne peut être autorisée que si elle poursuit un objectif d'intérêt général et si elle est mise en œuvre de manière adéquate et proportionnée à cet objectif* », reprenant ainsi sa propre jurisprudence[1159] ou celle du Conseil constitutionnel[1160]. Le Conseil d'État considère que la création d'un tel fichier répond à un objectif d'intérêt général, car il permet de faciliter la lutte contre l'usurpation d'identité et la recherche du demandeur au fichier des personnes recherchées.

[1154] Loi n° 2012-410 du 27 mars 2012 *relative à la protection de l'identité*, publiée au JORF n°0075 du 28 mars 2012 p. 5604.
[1155] Conseil constitutionnel, Décision n° 2012-652 DC du 22 mars 2012, *loi relative à la protection de l'identité*.
[1156] Jean-Jacques Urvoas, *Contre le « fichier des honnêtes gens »*, 6 mars 2012, disponible à http://www.urvoas.bzh/2012/03/06/contre-le-fichier-des-honnetes-gens/ consulté le 27 juin 2017.
[1157] Décret n° 2016-1 460 du 28 octobre 2016 *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*, publié au JORF n°0254 du 30 octobre 2016.
[1158] Conseil d'État, Section de l'intérieur, 23 février 2016, Avis relatif à la possibilité de créer un fichier regroupant les données relatives aux cartes nationales d'identité et aux passeports, n° 390180, disponible à http://www.conseil-etat.fr/content/download/75946/706640/version/1/file/avis_391080.pdf, consulté le 27 juin 2017.
[1159] Conseil d'État, assemblée, 26 octobre 2011, *Association pour la promotion de l'image et autres*, n^{os} 317827 et autres.
[1160] Conseil constitutionnel, Décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*.

L'existence d'un tel fichier, créé par un gouvernement démocratique et donc disponible à terme, peut s'avérer dangereuse en cas d'accession au pouvoir d'un régime autoritaire qui renierait les Droits de l'homme et autoriserait les recherches à partir des empreintes digitales ou génétiques, par exemple. La loi LOPPSI 2 prévoit également, là encore dans la droite ligne d'un mouvement amorcé il y a une dizaine d'années, l'extension des possibilités de recueil des empreintes génétiques à de nouvelles situations, en fait pour « *toute enquête ou instruction diligentées dans le cadre d'une procédure judiciaire* »[1161]. La Cour européenne des droits de l'homme a condamné la France pour non « *différenciation en fonction de la nature et de la gravité de l'infraction commise* »[1162], et ce sans prise en compte de la réserve du Conseil constitutionnel[1163].

Suite aux attentats de 2015, la loi pour le renseignement met en place une surveillance de masse[1164], surveillance accentuée par l'extension de la surveillance aux relations, famille et amis, des personnes suspectées de terrorisme. Cette extension, non remise en cause lors de l'examen de la loi par le Conseil constitutionnel a été censurée lors de la saisine d'une QPC[1165].

B) La mise en place d'une législation sécuritaire et antiterrorisme

Lors de la discussion à l'Assemblée nationale du projet de loi sur la sécurité (LOPPSI 2), la commission des lois constitutionnelles, de la législation et de l'administration générale de la république a été saisie du texte, mais la commission de la défense nationale et des forces armées s'en est saisie également pour avis, montrant ainsi la double portée de cette loi : loi de police intérieure et loi de sécurité contre les attaques extérieures. Dans son avis[1166], la commission relève que : « *La délinquance emprunte également de nouveaux canaux, plus complexes, en tirant tout le profit possible des progrès technologiques, comme le montre le développement de*

[1161] Code civil, Article 16-11 modifié par la loi nº 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure*, Article 6.
[1162] Cour européenne des droits de l'homme, *Affaire Aycaguer c/ France, Requête nº 8806/12*, Arrêt du 22 juin 2017.
[1163] Conseil constitutionnel, Décision nº 2010-25 QPC du 16 septembre 2010, *M. Jean-Victor C. [Fichier empreintes génétiques]*.
[1164] Félix Tréguer, « Feu vert à la surveillance de masse », *Le Monde diplomatique*, juin 2015, pp. 1, 4-5, disponible en ligne à https://www.monde-diplomatique.fr/2015/06/TREGUER/53056, consulté le 13 juillet 2017.
[1165] Conseil constitutionnel, Décision nº 2017-648 QPC du 04 août 2017 - *La Quadrature du Net et autres [Accès administratif en temps réel aux données de connexion]*, considérant nº 11.
[1166] Marc Joulaud, Avis nº1861 enregistré à la Présidence de l'Assemblée nationale le 22 juillet 2009 et présenté au nom de la commission de la défense nationale et des forces armées sur le projet de loi (nº 1697) *d'orientation et de programmation pour la performance de la sécurité intérieure.*

la cybercriminalité », montrant ainsi la nécessité de lutter contre cette nouvelle délinquance plus complexe à démontrer et à prévenir.

La commission prévoit que « *l'utilisation des nouvelles technologies permettra d'améliorer les missions de sécurité à plusieurs égards : le développement de l'informatique embarquée à bord des véhicules permettra notamment la consultation des fichiers à distance. […] ; les moyens de renseignement et de lutte contre le terrorisme seront renforcés. Parmi les équipements envisagés à cette fin figurent le traitement des données techniques liées à la téléphonie, l'interception, le brouillage des téléphones portables et satellitaires, et des scanners plus performants ; la vidéo sera plus largement utilisée que ce soit à terre ou embarquée. […] Avec la mise en place du projet ATHENA, le système de centralisation de l'information départemental de la gendarmerie offrira des fonctionnalités nouvelles dans la gestion des appels, du renseignement et des interventions par géolocalisation* ». Une utilisation de techniques numériques est envisagée pour accroître les performances des forces de l'ordre dans leurs investigations et permettre une meilleure interception des communications électroniques, une localisation des individus par traitement des métadonnées. La lutte contre le terrorisme nécessite, pour la commission parlementaire, une atteinte aux libertés individuelles par l'utilisation de la géolocalisation et l'interception des communications privées. Dans son rapport[1167], la commission des lois prévoit d'accroître les capacités d'élucidation de la police par l'utilisation des fichiers, de permettre le développement de logiciel de rapprochement judiciaire, d'adapter les moyens de la politique de sécurité aux évolutions technologiques et de lutter contre les utilisations illégales des nouvelles technologies. Elle envisage de mieux utiliser les nouvelles technologies pour lutter contre la criminalité organisée, et en particulier de recourir à la captation à distance de données informatiques.

Le projet de loi sur la sécurité prévoit l'utilisation intensive des moyens d'investigation numérique pour lutter contre le crime organisé et les utilisations frauduleuses des techniques numériques[1168]. La possibilité de rapprocher certains fichiers contenant des données

[1167] Éric Ciotti, Rapport n°2271 enregistré à la Présidence de l'Assemblée nationale le 27 janvier 2010 et 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 (n° 1697), *d'orientation et de programmation pour la performance de la sécurité intérieure*.

[1168] « Exposé des motifs du projet de loi », *Projet de loi d'orientation et de programmation pour la performance et la sécurité intérieure* enregistré à la Présidence de l'Assemblée nationale le 27 mai 2009, disponible à l'URL : http://www.assemblee-nationale.fr/13/pdf/projets/pl1697.pdf consulté le 27 février 2018.

personnelles juridiques est également envisagée[1169], ce rapprochement de fichiers est exclu par la loi « informatique et libertés » de janvier 1978. Ces mesures ont été votées par le Parlement dans le cadre de la loi LOPPSI 2 et déclarées conformes à la Constitution par le Conseil constitutionnel, même si de nombreux articles de cette loi ont été déclarés non conformes[1170].

§ 3 - La nécessité d'une riposte proportionnée

La quasi-totalité des lois adoptées pour lutter contre le terrorisme a été soumise au Conseil constitutionnel[1171] avant leur promulgation pour en vérifier la constitutionnalité. Le Conseil constitutionnel a ainsi vu son rôle de protecteur des droits fondamentaux confirmé[1172]. Comme le soulignait Pierre Mazeaud, président du Conseil constitutionnel de février 2004 à mars 2007, « *de même que la législation antiterroriste s'inscrit dans le cadre de la structure judiciaire classique, le Conseil [constitutionnel] fait application de sa jurisprudence classique pour en contrôler la constitutionnalité* »[1173].

En 1986[1174], le législateur n'a pas créé d'infraction spécifique pour les actes de terrorisme[1175]. L'acte terroriste a ainsi été défini par la combinaison entre un crime ou un délit de droit commun et son lien avec « *une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur* ». Le Conseil constitutionnel a considéré que cette définition par combinaison satisfaisait aux conditions de clarté et de précision exigées par la loi pénale[1176]. Lors de l'élaboration du nouveau Code pénal en 1994, l'incrimination a été ajoutée dans le Code pénal sans que ce système de combinaison ne soit revu ni que le Conseil

[1169] Jean-Jacques Lavenue, « L'interconnexion des fichiers de police : les ambiguïtés du rapport dialectique entre nécessité de la sécurité publique et protection des libertés » in Institut Maurice Hauriou, *Les fichiers de police,* Université de Toulouse, 15 septembre 2017.
[1170] Conseil constitutionnel, Décision n° 2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure.*
[1171] Seule la loi du 15 novembre 2001, relative à la sécurité quotidienne, n'a pas été déférée au Conseil constitutionnel.
[1172] Karine Roudier, « Prix de thèse du Conseil constitutionnel : Le contrôle de constitutionnalité de la législation antiterroriste. Étude comparée des expériences espagnole, française et italienne », *Les Nouveaux Cahiers du Conseil constitutionnel* 2012/4 (N° 37), pp. 147-154.
[1173] Pierre Mazeaud, *La lutte contre le terrorisme dans la jurisprudence du Conseil constitutionnel*, Visite à la cour suprême du Canada, 24 au 26 avril 2006.
[1174] Loi nº 86-1020 du 9 septembre 1986 *relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'Etat* publiée au Journal officiel nº0210 du 10 septembre 1986 p. 10956.
[1175] Gayraud Jean-François, Sénat David, « IV. Une définition impossible », « Le terrorisme », dans *Le terrorisme.* Paris, Presses Universitaires de France, « Que sais-je ? », 2006, pp. 12-47. URL : https://www.cairn.info/le-terrorisme--9782130558668-page-12.htm.
[1176] Décision nº 86-213 DC du 03 septembre 1986, *Loi relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État*.

constitutionnel ne soit consulté[1177], bien que la liste des incriminations de droit commun ait été élargie. Toutefois, en 1996 le Conseil constitutionnel a jugé non conforme l'élargissement des incriminations au délit d'aide à l'entrée ou au séjour irrégulier des étrangers en situation irrégulière[1178], estimant que le législateur avait « *entaché son appréciation d'une disproportion manifeste* ». En 2017[1179], le Conseil constitutionnel a également jugé non conforme le délit de consultation de sites terroristes institué par la loi du 3 juin 2016[1180] pour « *atteinte à la liberté de communication [non] nécessaire, adaptée et proportionnée* ». Un contrôle de proportionnalité est exercé par le Conseil constitutionnel.

Ce contrôle de proportionnalité a été aussi utilisé par le Conseil constitutionnel pour vérifier : que la durée de garde à vue ne porte pas une atteinte excessive à la liberté individuelle[1181] ; que de nouvelles modalités d'intervention de l'avocat en garde à vue ne portent pas une atteinte injustifiée ni à la liberté individuelle, ni aux droits de la défense, ni aux prérogatives de l'autorité judiciaire[1182] ; que les dispositifs de prise de vue des véhicules automobiles et de leurs occupants soient propres à assurer entre le respect de la vie privée et la sauvegarde de l'ordre public une conciliation non manifestement déséquilibrée[1183].

Mais, le Conseil constitutionnel a reconnu conforme à la Constitution la déchéance de nationalité pour actes de terrorisme prévue par la loi nº 2006-64[1184] eu égard à la gravité toute particulière que revêtent par nature les actes de terrorisme[1185]. Statuant sur l'article L.612-7 du code de la sécurité intérieure[1186], le Conseil constitutionnel a considéré que le législateur qui a entendu assurer un strict contrôle des dirigeants des entreprises exerçant des activités privées

[1177] Les lois n° 92-683 et no 92-684 du 22 juillet 1992 établissant le nouveau Code pénal n'ont pas été soumises au Conseil constitutionnel.

[1178] Décision nº 96-377 DC du 16 juillet 1996, *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire.*

[1179] Conseil constitutionnel, Décision nº 2016-611 QPC du 10 février 2017 *M. David P. [Délit de consultation habituelle de sites Internet terroristes]*.

[1180] Loi nº 2016-731 du 3 juin 2016 *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*, publiée au JORF nº0129 du 4 juin 2016.

[1181] Décision nº 2004-492 DC du 02 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*.

[1182] Idem.

[1183] Décision nº 2005-532 DC du 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*.

[1184] Loi nº 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* publiée au JORF nº0020 du 24 janvier 2006 p. 1129.

[1185] Conseil constitutionnel, Décision nº 2014-439 QPC du 23 janvier 2015, *M. Ahmed S. [Déchéance de nationalité]*.

[1186] Conseil constitutionnel, Décision nº 2015-463 QPC du 09 avril 2015, *M. Kamel B. et autre [Direction d'une entreprise exerçant des activités privées de sécurité - Condition de nationalité]*.

de sécurité et qui de ce fait sont associés aux missions de l'État en matière de sécurité publique, a pu fonder sa décision de différencier le traitement selon la nationalité desdits dirigeants sur un critère en rapport direct avec l'objectif de la loi.

Le Conseil constitutionnel va décider de la constitutionnalité de certaines restrictions à la liberté individuelle dans ses décisions relatives à la lutte contre le terrorisme par utilisation du contrôle de proportionnalité et de la nécessité des peines et des sanctions[1187]. Ainsi lors de la saisine concernant la loi LOPPSI 2[1188], le Conseil constitutionnel va censurer complètement ou partiellement huit des quinze articles critiqués par les députés et les sénateurs, et va soulever d'office et censurer complètement ou partiellement cinq autres articles. Dans le communiqué de presse annonçant sa décision[1189], le Conseil constitutionnel précise : « *Le Conseil constitutionnel a rejeté les griefs des requérants dirigés contre les articles 1er, 4, 11, 37-I, 38, 58, 60 et 61 (I). Il a fait droit à leurs griefs dirigés contre des dispositions des articles 18, 37 II, 41, 43, 53, 90, 92 et 101 qu'il a censurées. Enfin, il a examiné d'office pour les censurer des dispositions des articles 10, 14, 32, 91 et 123-II* ». S'il a rejeté sept griefs des requérants, il en a accepté huit en censurant les articles concernés, et il s'est autosaisi de cinq articles pour les censurer. Ce sont donc treize articles que le Conseil de loi a censurés pour ce projet de loi[1190]. Certains de ces articles sont censurés pour inadéquation des moyens : la revente de billets de spectacles ou de matchs pour éviter la présence de certains supporters ; pour méconnaissances d'exigences constitutionnelles en matière de justice pénale des mineurs ; pour reconnaissance d'une responsabilité correctionnelle des parents pour la faute d'autrui, serait-ce un enfant mineur ; mais aussi pour non-respect des prérogatives de la force publique et de la protection du juge. Les considérants retenus par le Conseil pour la censure des articles seront : méconnaissance de l'article 66 de la Constitution, non-respect du principe de légalité des délits, durée de rétention de données personnelles collectées trop longue, mais il accepte le renforcement des pouvoirs de police administrative en cas de grands rassemblements de personnes, sous le contrôle du juge comme étant une conciliation entre le respect de la liberté d'aller et venir et la sauvegarde de l'ordre public, qui n'est pas manifestement déséquilibrée.

[1187] Laurence Baghestani, « Principe de nécessité des peines et des sanctions » [Chronique de jurisprudence constitutionnelle (2e partie)], *Les Petites Affiches*, 31 juillet 2012, n° 152, pp. 28-29.

[1188] Conseil constitutionnel, Décision n° 2011-625 DC du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*.

[1189] Ïbid.

[1190] François Marcel, « Que reste-t-il de la Loppsi après la décision du Conseil constitutionnel ? », *Les Cahiers de la fonction publique et de l'administration*, mars 2011, n° 309, pp. 21-26.

Le Conseil constitutionnel a considéré comme conformes à la Constitution[1191], la géolocalisation réalisée sous contrôle de l'autorité judiciaire, ainsi qu'en cas d'enquête préalable sous le contrôle du procureur dans la limite de quinze jours avant saisine du juge des libertés, ces mesures n'ayant pas un caractère disproportionné eu égard à la complexité des infractions commises, et sont nécessaires à la manifestation de la vérité. Mais, le Conseil a estimé qu'une condamnation ne pouvait intervenir sur le « seul » fondement des données ainsi recueillies alors que la personne mise en cause n'a pas eu la possibilité de contester les conditions dans lesquelles ces données ont été recueillies, respectant ainsi le principe de contradiction.

Suite à la triple saisine du Conseil constitutionnel par le Président de la République, par le Président du Sénat et par plus de soixante députés, concernant la loi sur le renseignement[1192], loi dans laquelle la surveillance administrative est renforcée pour la prévention des attentats, le Conseil constitutionnel, dans sa décision publiée le 23 juillet 2015[1193], a déclaré non conformes à la Constitution certaines dispositions prévues dans cette loi : la procédure dite d'urgence opérationnelle, autorisant les services de renseignement à procéder à la mise en œuvre de certaines techniques sans avis préalable du Premier ministre pour atteinte disproportionnée au droit du respect de la vie privée, à l'inviolabilité du domicile et au secret des correspondances (article 2 modifiant l'article L.821-6 du code de la sécurité); les mesures de surveillance internationale pour méconnaissance de l'étendue de la compétence du législateur (article 6 modifiant l'article L.854-1 du code de la sécurité intérieure) ; une disposition relative aux crédits de la commission nationale de contrôle des techniques de renseignement pour méconnaissance d'une règle de procédure (article 2 modifiant l'article L.832-4 du code de la sécurité intérieure)[1194].

Ainsi, dans la prolongation de sa jurisprudence antérieure, le Conseil constitutionnel n'a déclaré non conformes à la Constitution que peu d'articles de la loi sur le renseignement pour atteinte disproportionnée aux libertés fondamentales[1195], alors que de nombreuses critiques sont formulées et que des requêtes devant la Cour européenne des droits de l'homme ont été

[1191] Conseil constitutionnel, Décision no 2014-693 DC du 25 mars 2014, *Loi relative à la géolocalisation*.
[1192] Loi votée par le Sénat le 23 juin 2015 et par l'Assemblée nationale le 24 juin 2015.
[1193] Conseil constitutionnel, décision n° 2015-713 DC du 23 juillet 2015, *Loi relative au renseignement*.
[1194] Michel Verpeaux, « La loi sur le renseignement, entre sécurité et libertés. À propos de la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015 », *La Semaine juridique*. Édition générale, 14 septembre 2015, n° 38, pp. 1639-1646.
[1195] Agnès Roblot-Troizier, « Un contrôle de constitutionnalité restreint sur les mesures de la police administrative du renseignement », *Revue française de droit administratif,* novembre-décembre 2015, n° 6, pp. 1195-1200.

déposées dès le 3 octobre 2015 par le barreau de Paris et cent quatre-vingts journalistes de la presse judiciaire, requêtes ayant fait l'objet d'une décision de communication le 26 avril 2017[1196]. Les requérants soulèvent trois griefs principaux : base légale insuffisante compte tenu du flou entourant les documents ou informations pouvant être saisis par les services de renseignements ; les conditions permettant d'opérer le tri entre les activités relevant du mandat d'avocat ou de conseil ; disproportion des techniques de captation, boîtes noires algorithmique ou IMSI-catchers[1197], capables de capturer toutes les conversations dans un périmètre donné.
La Cour européenne des droits de l'homme utilise également la notion de proportionnalité en cas de violation des articles de la convention européenne de sauvegarde des droits de l'homme. De fait, la Cour utilise deux concepts modérateurs pour forger des concepts permettant de concilier la liberté individuelle et l'intérêt de la collectivité : la marge nationale d'appréciation qui accorde aux États une liberté d'appréciation dans l'application de la Convention et dans le choix des mesures à prendre en fonction de leurs spécificités, et le principe de proportionnalité qui permet de vérifier si les moyens employés sont bien proportionnés à l'objectif suivi[1198].

A) Les prérogatives de la force publique et la protection du juge

La délégation à des personnes privées du visionnage et de l'exploitation de la vidéosurveillance est déclarée non conforme à la Constitution[1199]. Elle permet de confier à des personnes privées la surveillance de la voie publique et à leur déléguer des tâches de police administrative générales inhérentes à l'exercice de la force publique. Elle entre en contradiction avec l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789[1200]. Le Conseil constitutionnel a également déclaré non conforme dans cette décision, la possibilité pour des agents de police municipale de procéder à des contrôles d'identité, alors qu'ils ne sont pas

[1196] Franck Johannès, « *La Cour européenne des droits de l'homme rendra une décision sur la loi renseignement – Le dossier en droit* », Le Monde, 16 mai 2017, article disponible à http://libertes.blog.lemonde.fr/2017/05/16/la-cour-europeenne-des-droits-de-lhomme-rendra-une-decision-sur-la-loi-renseignement-le-dossier-en-droit/, consulté le 21 juin 2017.
[1197] *International Mobile Subscriber Identity-catcher* ou IMSI-catcher est un dispositif permettant d'intercepter le trafic des téléphones mobiles et de suivre la localisation de ces téléphones.
[1198] Extrait de « *La jurisprudence de la Cour européenne des droits de l'homme* », Le forum des étudiants de Sciences Po en ligne à http://www.forum-scpo.com/union-europeenne/jurisprudence-convention-europeenne-des-droits-de-l-homme-cedh.htm, consulté le 13 juillet 2017.
[1199] Conseil constitutionnel, Décision nº 2011-625 DC du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure.*
[1200] DDHC, Art. 12. La garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée.

placés sous l'autorité d'un officier de police judiciaire, lui-même placé sous l'autorité et le contrôle de l'autorité judiciaire, cette disposition contrevenait à l'article 66 de la Constitution.
Alors que la Constitution donne au juge judiciaire le rôle de protection des libertés individuelles et de la propriété privée[1201], et que l'article 136 du Code de procédure pénale prévoit que, dans les cas d'atteinte à la liberté individuelle, le juge judiciaire est exclusivement compétent, cette compétence n'est pas générale et absolue, elle ne s'exerce que dans deux cas, définis par la jurisprudence : la voie de fait[1202] et l'emprise[1203]. En France, la protection des libertés fondamentales est d'origine prétorienne et le juge administratif en a été le premier garant. En 1971, le Conseil constitutionnel a donné à cette protection un statut constitutionnel[1204] en incluant le préambule de ladite Constitution, la Déclaration des droits de l'homme et du citoyen de 1789 et le préambule de la Constitution de 1946, dans le droit positif.
Mais, les décisions successives du Conseil constitutionnel en matière des lois de lutte contre le terrorisme et le crime organisé ont réduit la protection des libertés individuelles par le juge judiciaire[1205]. Dès l'origine de la V^e^ République, Michel Debré, comparant la garantie judiciaire apportée par l'article 66 à la procédure anglo-saxonne de l'habeas corpus, annonçait devant le Conseil d'État, en 1958 : « *Nous pourrons, à cet égard, faire mieux encore que le droit anglo-saxon* »[1206]. En 1977, le Conseil constitutionnel consacre la liberté individuelle en tant que « principe fondamental reconnu par les lois de la République »[1207] et proclamé par le préambule de la Constitution de 1946, sans référence à l'article 66 de la Constitution ni à la Déclaration des droits de l'homme et du citoyen de 1789[1208]. Mais le Conseil constitutionnel va progressivement briser le lien entre liberté individuelle et garantie judiciaire en démultipliant

[1201] Constitution Article 66 « *Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi.* »
[1202] Il y a voie de fait lorsque l'administration a porté une atteinte grave à une liberté fondamentale ou au droit de propriété, soit par une décision manifestement insusceptible de se rattacher à un pouvoir appartenant à l'administration, soit par l'exécution irrégulière d'un acte.
[1203] L'emprise concerne l'atteinte à la propriété individuelle par l'administration.
[1204] Conseil constitutionnel, Décision n° 71-44 DC du 16 juillet 1971, *Loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association*.
[1205] Dany Cohen, « Le juge, gardien des libertés ? », *Pouvoirs* 2009/3 (n° 130), pp. 113-125.
[1206] Michel Debré, Allocution devant le Conseil d'État, in *Travaux préparatoires des institutions de la V^e^ République,* volume III, La Documentation française, 1991, pp. 268-269.
[1207] Conseil constitutionnel, Décision n° 76-75 DC du 12 janvier 1977 *Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales*.
[1208] Louis Favoreu, Patrick Gaïa, Richard Ghevontian et autres, *Droit des libertés fondamentales*, Précis Dalloz, 5^e^ édition, pp. 188-189.

les composantes de la liberté individuelle[1209] : liberté d'aller et venir[1210], liberté du mariage[1211], droit au respect de la vie privée[1212] et le droit à l'anonymat[1213]. Ces « libertés-démembrements », comme les appellent Louis Favoreu[1214], vont pouvoir s'émanciper de la protection de l'article 66 de la Constitution. Ainsi, la protection de la vie privée, de l'inviolabilité du domicile et du secret des correspondances ou de la liberté d'aller et venir relève désormais des articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen[1215] et non plus de l'article 66 de la Constitution. L'autonomie formelle des libertés dérivées de la liberté individuelle est consacrée dans un considérant de principe[1216] : « *[…] il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties ; qu'au nombre de celles-ci figurent la liberté d'aller et venir, l'inviolabilité du domicile privé, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789, ainsi que la liberté individuelle, que l'article 66 de la Constitution place sous la surveillance de l'autorité judiciaire* ». Il découle de cette décision que du point de vue des sources, les libertés mentionnées doivent être considérées comme échappant au rayonnement de l'article 66 de la Constitution.

La protection des données personnelles informatisées s'est totalement émancipée du joug de la liberté individuelle pour ne dépendre que du droit au respect de la vie privée[1217]. Depuis 1993, en matière de protection des données personnelles, la compétence de la juridiction

[1209] Gilles Armand, « Que reste-t-il de la protection constitutionnelle de la liberté individuelle ? », *Revue française de droit constitutionnel* 2006/1 (nº 65), pp. 37-72.
[1210] Conseil constitutionnel, Décision nº 93-325 DC du 13 août 1993, *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France*, considérant nº 3.
[1211] Ibid.
[1212] Conseil constitutionnel, Décision nº 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, considérant nº 2.
[1213] Ibid.
[1214] Louis Favoreu, Patrick Gaïa, Richard Ghevontian et autres, *Droit des libertés fondamentales*, Précis Dalloz, 5e édition, pp. 193-210.
[1215] Conseil constitutionnel, Décision nº 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, considérant nº 7.
[1216] Conseil constitutionnel, Décision nº 2004-492 DC du 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, considérant nº4.
[1217] Conseil constitutionnel, Décision nº 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*.

administrative est retenue[1218]. La protection du juge judiciaire en matière de liberté individuelle se trouve restreinte à une liberté individuelle qui peut être assimilée à la sûreté.

1) L'accès aux données personnelles des personnes physiques par les fichiers de police

En France, la Commission nationale de l'informatique et des libertés, ou CNIL, créée par la loi nº 78-17 du 6 janvier 1978, a en charge de veiller au respect des dispositions de ladite loi, c'est-à-dire informer les individus de leurs droits et obligations en matière de traitement automatisé des données à caractère personnel et elle dispose d'un pouvoir réglementaire pour contrôler les traitements automatiques de ces données personnelles[1219].

Dans le cadre de leurs missions de police judiciaire, la police et la gendarmerie ont été amenées à enregistrer les données collectées lors des enquêtes dans des fichiers de police, STIC et JUDEX, fusionnés dans TAJ, traitement des antécédents judiciaires. Début 2005, la gendarmerie et la police nationale, confrontées à la nécessité de moderniser leurs systèmes respectifs JUDEX et STIC, se sont associées pour réaliser un nouveau fichier commun de recherches et de rapprochements criminels : ARIANE (Application de rapprochements, d'identification et d'analyse pour les enquêteurs). Les informations contenues dans ARIANE respectent les mêmes règles que les applications STIC et JUDEX actuelles. En revanche, l'origine des informations (police ou gendarmerie) ne sera plus distinguée. ARIANE a tracé une voie qui est reprise dans le cadre d'autres projets que constituent la refonte mutualisée des fichiers des objets et véhicules volés (projet FOVeS) et du fichier des personnes recherchées (projet FPS)[1220].

De nombreux autres fichiers sont utilisés pour des objectifs ciblés, le fichier des personnes recherchées avec ses fiches S est aujourd'hui au centre des débats concernant la sécurité du territoire, les personnes soupçonnées de radicalisation djihadiste faisant l'objet de certaines de

[1218] Conseil constitutionnel, Décision nº 93-325 DC du 13 août 1993, *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France*, considérant nº 121.
Conseil constitutionnel, Décision nº 98-405 DC du 29 décembre 1998, *Loi de finances pour 1999*, considérant nº 62.

[1219] Chapitre II, Articles 6 et suivants de la loi nº78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés.*

[1220] Ce fichier regroupe les fiches « S » signalant entre autres les personnes radicalisées susceptibles d'attenter à la sécurité de l'État.

ces fiches S. Ces différents fichiers relevant de la sécurité de l'État font partie de ces traitements dont l'accès par les individus est indirect, c'est-à-dire qu'il doit être demandé par la Commission de l'informatique et des libertés aux autorités compétentes.

Alors que la Commission nationale de l'informatique et des libertés a régulièrement émis des réserves concernant le contenu et la conservation des données enregistrées lors des enquêtes dans les fichiers de police[1221], l'article 14 de la Loi dite LOPPSI 2[1222] autorise les logiciels de rapprochement judiciaire. Ces logiciels permettent la mise en œuvre de traitements de données à caractère personnel recueillies à l'occasion d'enquêtes judiciaires. Ces traitements ne sont pas réservés à des infractions graves. Le Conseil constitutionnel a contrôlé que le législateur avait

---

[1221] Relaté dans la question écrite n° 07002 de M. Yves Détraigne au Sénat : « *Malgré un premier signalement en 2009, l'autorité administrative indépendante déplore que rien n'ait été réellement mis en œuvre pour améliorer la situation et que de sérieux dysfonctionnements persistent malgré la modernisation actuellement en cours des applications informatiques des ministères de l'intérieur et de la justice.*
« Entre la fin de 2012 et le début de 2013, la CNIL, grâce à vingt-trois contrôles sur place et à soixante-et-un contrôles sur pièces, a radioscopé aussi bien le contenu et l'utilisation des fichiers STIC et JUDEX que le projet de traitement des antécédents judiciaires (TAJ), qui doit fusionner ces deux fichiers pour constituer une base de données géante commune à la police et à la gendarmerie dès 2014.
« Or, selon la CNIL, il n'a pas été prévu de mettre à jour les millions de fiches issues de STIC et de JUDEX, qui comportent de nombreuses données inexactes, avant leur versement dans TAJ. Ainsi, des personnes continueront à se voir refuser l'accès à certains emplois, à un titre de séjour ou à la nationalité française sur le fondement de données d'antécédents erronées.
« L'autorité indépendante émet plusieurs recommandations, notamment celle de « nettoyer » les fiches avant qu'elles soient reprises dans le TAJ afin de corriger les erreurs et de mettre à jour les fiches les plus sensibles (fiches relatives aux mineurs, aux infractions récentes ou de nature criminelle).
Elle suggère également que soient renforcées les règles de confidentialité, les mesures de sécurité et de confidentialité instaurées au sein des services de police et de gendarmerie restant encore insuffisantes selon elle, et surtout que soit limité dans le temps l'accès aux données dans le cadre administratif et envisagée la diminution de certaines durées de conservation. », Malgré un premier signalement en 2009, l'autorité administrative indépendante déplore que rien n'ait été réellement mis en œuvre pour améliorer la situation et que de sérieux dysfonctionnements persistent malgré la modernisation actuellement en cours des applications informatiques des ministères de l'intérieur et de la justice.
« Entre la fin de 2012 et le début de 2013, la CNIL, grâce à vingt-trois contrôles sur place et à soixante-et-un contrôles sur pièces, a radioscopé aussi bien le contenu et l'utilisation des fichiers STIC et JUDEX que le projet de traitement des antécédents judiciaires (TAJ), qui doit fusionner ces deux fichiers pour constituer une base de données géante commune à la police et à la gendarmerie dès 2014.
« Or, selon la CNIL, il n'a pas été prévu de mettre à jour les millions de fiches issues de STIC et de JUDEX, qui comportent de nombreuses données inexactes, avant leur versement dans TAJ. Ainsi, des personnes continueront à se voir refuser l'accès à certains emplois, à un titre de séjour ou à la nationalité française sur le fondement de données d'antécédents erronées.
« L'autorité indépendante émet plusieurs recommandations, notamment celle de « nettoyer » les fiches avant qu'elles soient reprises dans le TAJ afin de corriger les erreurs et de mettre à jour les fiches les plus sensibles (fiches relatives aux mineurs, aux infractions récentes ou de nature criminelle).
Elle suggère également que soient renforcées les règles de confidentialité, les mesures de sécurité et de confidentialité instaurées au sein des services de police et de gendarmerie restant encore insuffisantes selon elle, et surtout que soit limité dans le temps l'accès aux données dans le cadre administratif et envisagée la diminution de certaines durées de conservation. » disponible à l'URL : https://www.senat.fr/questions/base/2013/qSEQ130607002.html, consultée le 24 juin 2017.

[1222] Loi n° 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure*.

apporté des garanties pour assurer la conciliation entre la sauvegarde de l'ordre public et le respect de la vie privée[1223]. D'une part, il ressort de l'article 14 que celui-ci n'a pas « *pour objet d'autoriser la mise en œuvre d'un traitement général de données recueillies à l'occasion de diverses enquêtes* »[1224]. Ces traitements de données sont autorisés, au cas par cas, par l'autorité judiciaire dans le cadre d'une enquête déterminée. D'autre part, les données enregistrées ne doivent pas être conservées plus de trois ans après leur enregistrement[1225]. À cet effet, le Conseil a censuré partiellement les dispositions de l'article 230-23 du code de procédure pénale. Compte tenu de ces conditions restrictives portant sur la durée de conservation des données, l'article 14 est, pour le surplus, déclaré par le Conseil constitutionnel conforme à la Constitution[1226] sans considération des remarques et critiques formulées par la Commission de l'informatique et des libertés.

2) Des fichiers objet de contrôles inadaptés ou inefficaces face à une législation sécuritaire

Le traitement des données personnelles, qu'il soit d'ordre privé ou public, est encadré par la loi n° 78-17 dite « informatique et liberté ». Tout traitement automatique de données personnelles doit être déclaré à la Commission de l'informatique et des libertés préalablement à sa création. L'administration a créé des fichiers contenant des informations personnelles répertoriant toute personne objet d'une procédure judiciaire. Ces fichiers ont été créés sans déclaration préalable à la CNIL ni demande d'avis, et régularisés par décret plusieurs années après leur création. Le rôle de la CNIL a été précisé et modifié au cours des différentes modifications de cette loi[1227].

La loi LOPPSI 2 a prévu un regroupement des fichiers de police et de gendarmerie existant, en un seul fichier dit traitement de données à caractère personnel relatif aux « antécédents judiciaires » ainsi que des logiciels de rapprochement judiciaire à des fins d'analyse criminelle et des fichiers d'analyse sérielle.

[1223] Conseil constitutionnel, Décision n° 2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure,* considérants n^{os} 67 et suivants.
[1224] Ibid., considérant n° 71.
[1225] Ibid., considérant n° 72.
[1226] Ibid., considérant n° 73.
[1227] Son rôle est aujourd'hui défini par l'article 11 du chapitre III suite aux dernières modifications apportées par la loi n° 2017-56 du 20 janvier 2017 *portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes.*

Le STIC (Système de Traitement des Infractions constatées) est une méga-base de données interconnectant les fichiers policiers et répertoriant toute personne ayant été concernée par une procédure judiciaire (crimes, délits et contraventions diverses et variées), qu'elle soit mise en cause ou bien... victime, et quand bien même le mis en examen est blanchi[1228]. Créé par la loi nº 95-73 du 21 janvier 1995[1229], le STIC entre en activité officielle sans ses décrets d'application. Au 1er janvier 1997, il comportait les noms de 2,5 millions de prévenus, 2,7 millions de victimes, portant sur 5 millions de procédures et 6,3 millions infractions. Certaines données remontent à 1965[1230]. Créé officiellement par le décret du 5 juillet 2001[1231], le STIC a donc fonctionné, en toute illégalité, pendant 6 ans, avant d'être légalisé en toute confidentialité en début d'été. À la suite de l'entrée en vigueur de la loi nº 2003-239[1232], le décret nº 2006-1258[1233], apporte des modifications à l'utilisation de ce fichier qui peut être exploité pour faciliter la constatation des infractions pénales, le rassemblement des preuves et la recherche des auteurs[1234]. Ce décret précise que, en cas de classement sans suite pour insuffisance de preuves, toute personne mise en cause peut demander l'effacement des données le concernant au procureur de la République, responsable du traitement[1235]. Les dispositions relatives à ce fichier ont été codifiées par la loi no 2011-267[1236] et le décret no 2012-652[1237] du 4 mai 2012 aux articles 230-6 et suivants et R. 40-23 et suivants du code de procédure pénale. Les données du fichier STIC sont introduites dans le Fichier des Antécédents Judiciaires qui incorpore également les données du fichier JUDEX.

Début mai 2012, plusieurs décrets ont été édictés et concernent le traitement d'antécédents judiciaires[1238], la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse

---

[1228] La France a été condamnée par la Cour européenne des droits de l'homme pour la gestion de ce fichier STIC (CEDH, arrêt de 18 septembre 2014, Requête nº 21010/10, *Affaire Brunet c/ France*).

[1229] Loi nº 95-73 du 21 janvier 1995 *d'orientation et de programmation relative à la sécurité*, publiée au JORF nº20 du 24 janvier 1 995 p. 1249.

[1230] Source : SGP, syndicat majoritaire des gardiens de la paix

[1231] Décret nº2001-583 du 5 juillet 2001 *pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées*, paru au JORF nº155 du 6 juillet 2001 p. 10779.

[1232] Loi nº 2003-239 du 18 mars 2003 *pour la sécurité intérieure* publiée au JORF nº66 du 19 mars 2003 p. 4761.

[1233] Décret nº2006-1 258 du 14 octobre 2006 *modifiant le décret nº 2001-583 du 5 juillet 2001 portant création du système de traitement des infractions constatées dénommé " STIC ",* publié au JORF nº240 du 15 octobre 2006 p. 15319.

[1234] Ibid., article 2.

[1235] Ibid., article 4.

[1236] Loi nº 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure*, dite Loi LOPPSI 2 déjà citée.

[1237] Décret nº 2012-652 du 4 mai 2012 *relatif au traitement d'antécédents judiciaires* publié au JORF nº0107 du 6 mai 2012 p. 8047.

[1238] Ibid.

criminelle[1239] et de mise en œuvre des fichiers d'analyse sérielle[1240]. Dans le traitement d'antécédents judiciaires, le décret prévoit l'enregistrement de « *photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale* » pour les personnes mises en cause. Les données à caractère personnel des personnes mises en cause sont conservées vingt ans pour les majeurs et cinq ans pour les mineurs. Par dérogation, elles peuvent être conservées quarante ans. En cas de plusieurs mises en cause, la durée le plus longue à partir de la dernière mise en cause est retenue pour la conservation des données. Les données ainsi collectées sont accessibles aux services de police étrangers. L'utilisation du fichier STIC sera prolongée de quelques années malgré la création du traitement des antécédents judiciaires[1241] pour tenir compte des difficultés de mise en œuvre du TAJ.

Même en cas de non-lieu, le nom du prévenu n'est pas sûr de disparaître des fiches, et ce même si un droit d'accès et de rectification est prévu dans les textes[1242]. La Commission de l'informatique et des libertés a constaté des irrégularités dans la gestion de ce fichier[1243] et émis des propositions pour une gestion de ce fichier plus respectueuse du droit des personnes[1244] : harmonisation des procédures, sécurisation des accès, respecter les profils d'utilisation et vérifier les décisions d'effacement ou de rectification. Dans sa conclusion, la Commission de l'informatique et des libertés écrit : « *Dans la pratique quotidienne, on constate un manque de rigueur dans la gestion du STIC ainsi qu'une absence de prise en compte des conséquences graves qui en découlent pour les personnes.* » La France a été condamnée par la Cour européenne des droits de l'homme au titre de l'article 8 pour rétention injustifiée et longue des données dans le fichier STIC[1245].

Le fichier STIC était utilisé par les forces de police, la gendarmerie utilisait, quant à elle, le fichier JUDEX. Il n'existe que très peu d'informations concernant le système judiciaire de Documentation et d'EXploitation (JUDEX) de la gendarmerie. Mis en place en 1985/86 pour

---

[1239] Décret n° 2012-687 du 7 mai 2012 *relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle* publié au JORF n°0108 du 8 mai 2012 p. 8268.

[1240] Décret n° 2012-689 du 7 mai 2012 *relatif aux conditions de mise en œuvre des fichiers d'analyse sérielle et des logiciels de rapprochement judiciaire* publié au JORF n°0108 du 8 mai 2012 p. 8270.

[1241] Le TAJ est opérationnel au 1er janvier 2014, comme indiqué par la circulaire du 18 août 2014 *relative aux fichiers d'antécédents judiciaires* (NOR : JUSD1419980C).

[1242] Source : Syndicat de la magistrature.

[1243] Article *STIC : Histoires vécues* sur le site de la CNIL, à http://www.cnil.fr/la-cnil/actu-cnil/article/article/stic-histoires-vecues/ consulté le 13 mai 2012.

[1244] Dans l'article *Contrôle du STIC : Les propositions de la CNIL pour une utilisation du fichier plus respectueuse du droit des personnes* du 20 janvier 2009 à http://www.cnil.fr/la-cnil/actu-cnil/article/article/controle-du-stic-les-propositions-de-la-cnil-pour-une-utilisation-du-fichier-plus-respectueuse-du/ consulté le 13 mai 2012.

[1245] Cour européenne des droits de l'homme, arrêt du 18 septembre 2014, affaire *Brunet c/ France*.

remplacer le système PROSAM qui datait de 1967, ce fichier, qui est l'équivalent pour la gendarmerie française du fichier STIC pour la Police nationale, a fonctionné sur l'ensemble du territoire, de manière clandestine, pendant plus de 20 années, sans aucun moyen pour les personnes concernées d'exercer leur droit d'accès et de rectification, avant qu'il n'acquière d'existence légale le 20 novembre 2006[1246].

En avril 2005, la Commission de l'informatique et des libertés a critiqué dans son rapport 2004 l'utilisation de ces fichiers de police, pas toujours à jour, notamment pour recruter du personnel de sécurité[1247]. En 2009, un rapport parlementaire[1248] constatait de nombreuses erreurs dans les données présentes dans le STIC et les délais trop longs pour l'accès indirect aux données par la CNIL. Dans un rapport de 2013[1249], la Commission de l'informatique et des libertés constatait des difficultés dans la mise en œuvre du TAJ. En 2015, la CNIL constate que les délais d'accès prévus ne sont pas respectés privant ainsi les personnes physiques du droit d'accès indirect[1250].

Si les fichiers STIC, JUDEX et TAJ posent problème quant aux conséquences pour les personnes physiques présentes dans ces fichiers en termes d'embauches éventuelles, il existe d'autres fichiers gérés par l'administration et traitant des données à caractères personnels. En 2006, le rapport Bauer[1251] commence par une liste des fichiers non recensés dans ledit rapport : les fichiers de la Défense nationale ; le Fichier national des immatriculations (FNI) ; le Fichier national des cartes d'identité ; le Fichier national des passeports ; le Fichier réseau mondial visas 2 (RMV 2) ; l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF) ; le fichier ELOI ; le Fichier national des personnes incarcérées ; le Casier judiciaire national ; le Fichier des naturalisations ; les fichiers de l'Office français de protection des réfugiés et apatrides ; le Répertoire national d'identification des personnes physiques ; le Fichier du recensement ; les fichiers d'état civil ; le Fichier national des comptes bancaires (FICOBA) ; le Fichier national des chèques irréguliers (FNCI) ; le Fichier central des chèques (FCC) ; le Fichier national des incidents de remboursement des crédits aux particuliers.

[1246] Décret n°2006-1411 du 20 novembre 2006 *portant création du système judiciaire de documentation et d'exploitation dénommé « JUDEX », paru* au JORF n°270 du 22 novembre 2006.

[1247] CNIL, *25e rapport d'activité 2004*, p. 103

[1248] Delphine Batho et Jacques Bénisti, *Rapport d'information* N° 1548 enregistré à la Présidence de l'Assemblée nationale le 24 mars 2009.

[1249] CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur*, Rapport adopté par la CNIL réunie en séance plénière le 13 juin 2013, disponible à https://www.cnil.fr/sites/default/files/typo/document/Rapport_controle_des_fichiers_antecedents_judiciaires_juin_2013.pdf, consulté le 27 juin 2017.

[1250] CNIL, Décision n° 2015-005 du 2 février 2015, *avertissement*.

[1251] Alain Bauer, *Fichiers de police et de gendarmerie : comment améliorer leur contrôle et leur gestion ?,* décembre 2006, La documentation française.

Le recensement des fichiers de la police nationale sont alors : « *Le Système de circulation hiérarchisée des enregistrements opérationnels de la police sécurisés (CHEOPS) fédère et permet de donner accès, sous une même configuration, à différentes applications de police : le Système de traitement des infractions constatées (STIC) ; le Fichier des véhicules volés (FVV) ; le Fichier des personnes recherchées (FPR) ; le Fichier des renseignements généraux (FRG) ; le Fichier national transfrontières (FNT) ; le Fichier des brigades spécialisées (FBS) ; le Fichier informatisé du terrorisme (FIT) ; le Fichier national du faux monnayage (FNFM) ; le Fichier national automatisé des empreintes génétiques (FNAEG)* ». Cette liste est complétée par d'autres fichiers : le fichier d'information Schengen (SIS) ; le fichier de la Direction de la surveillance du territoire (DST) ; le Système d'analyse et de liens de la violence associée au crime (SALVAC) ; le fichier de travail de la police judiciaire (FTPJ) ; le Fichier automatisé des empreintes digitales (FAED) ; les fichiers de la gendarmerie nationale : JUDEX ; le Fichier des objets signalés (FOS) ; le fichier de traitement des images des véhicules volés (FTIVV) ; ANACRIM ; le Service central de préservation des prélèvements biologiques (SCPPB) ; le Fichier des avis de condamnations pénales (FAC) ; PULS@R ; la Bureautique brigade 2000 (BB2000) ; COG-RENS ; le Fichier alphabétique de renseignements (FAR) ; le Fichier des personnes nées à l'étranger (FPNE) ; le fichier ARAMIS ; le Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (SDRF) ; le Fichier de suivi des personnes faisant l'objet d'une rétention administrative ; le Fichier de la batellerie ; le Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) ; le Fichier national des permis de conduire (FNPC).

Un nouveau rapport a été publié en 2008[1252]. Il constate un accroissement du nombre de fichiers qui de 36 en 2006 est passé à 45 fichiers. Dans un rapport publié le 27 décembre 2011[1253], la mission d'information parlementaire sur les fichiers de police recense 80 fichiers de police dont 28 n'ont fait ni l'objet d'une déclaration à la CNIL, ni l'objet d'un texte législatif ou réglementaire les autorisant. Le rapport constate que 38 millions de victimes d'infractions sont recensées dans le STIC. Comme le constate Jean-Jacques Lavenue, toute une série de fichiers

[1252] Alain Bauer, *Mieux contrôler les fichiers de police pour protéger les libertés*, décembre 2008, La documentation française

[1253] Delphine Batho et Jacques Alain Bénisti, *Rapport d'information déposé en application de l'article 145-8 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la république*, enregistré à la Présidence de l'Assemblée nationale le 21 décembre 2011.

est apparue sans que ceux qui y sont inscrits aient directement commis le moindre acte illégal[1254].

B) Des dysfonctionnements régulièrement constatés

Après l'énumération des fichiers recensés, le rapport Bauer de 2006, constate des « problèmes et dysfonctionnements »[1255] dans l'alimentation et l'utilisation de ces fichiers ou traitements automatisés : erreurs matérielles de saisie ; fichiers locaux non déclarés.

Le groupe de travail a constaté que ce sont les fichiers STIC et JUDEX qui posent le plus de difficultés, ils sont alimentés durant l'enquête par les officiers de police judiciaire qui y introduisent leurs conclusions. Celles-ci peuvent être modifiées par le procureur de la République, le juge d'instruction ou la juridiction de jugement. L'article 25 de la loi no 2003-239 du 18 mars 2003 relative à la sécurité intérieure a modifié cet article en élargissant les cas dans lesquels il peut être procédé à la consultation de ces fichiers de police judiciaire à des fins d'enquêtes administratives. L'absence de mise à jour des fichiers STIC ou JUDEX a donc des conséquences importantes pour les personnes intéressées. Cette constatation rejoint celles formulées par la Commission de l'informatique et des libertés dans son rapport d'activité de 2004. Le rapport constate également que « *la mise en œuvre du droit d'accès à ces deux fichiers par l'intermédiaire de la CNIL fait apparaître un certain nombre de dysfonctionnements* ».

Dans ses conclusions, le groupe de travail écrit : « *Pour l'essentiel, les travaux du groupe de travail ont permis de constater que l'utilisation de certains des fichiers de police judiciaire dans le cadre de procédures administratives, malgré les contrôles de la Commission nationale de l'informatique et des libertés (CNIL) et les opérations d'apurement importantes réalisées par les services de police et les unités de gendarmerie, révélait des dysfonctionnements et pouvaient attenter aux libertés individuelles ou nuire à l'efficacité de l'action publique.*[1256] », et il constate que : « *C'est donc l'usage à des fins autres que judiciaires de ces fichiers de police et de gendarmerie qui continue de poser problème.* »

[1254] Jean-Jacques Lavenue, « Anormalité, surveillance et fichiers de police », Jean-Jacques Lavenue, Bruno Villabla, *Vidéo-surveillance et détection automatique des comportements anormaux,* Presses universitaires du Septentrion, pp. 235-260.

[1255] Alain Bauer, *Fichiers de police et de gendarmerie : comment améliorer leur contrôle et leur gestion ?* décembre 2006, La Documentation française, pages 87 et suivantes

[1256] Ibid., p.129.

Il préconise une amélioration des droits d'accès indirect, une meilleure coordination procureur, gendarmerie et police pour le contrôle des informations et leur mise à jour. Ces mêmes recommandations se retrouvent dans le rapport parlementaire[1257], ainsi que dans les décisions de la CNIL. Le rapport Bauer de 2008, préconise la désignation d'un expert « informatique et libertés » au sein des services de police et de gendarmerie[1258] et de mieux contrôler l'utilisation de ces fichiers et d'améliorer la gestion des habilitations[1259], ainsi que de désigner un magistrat chargé du contrôle des fichiers d'antécédents judiciaires[1260].

En principe, tous ces fichiers de police sont créés pour améliorer la lutte contre la criminalité et le terrorisme, même si leur usage est parfois dévoyé par l'administration. Mais outre cette myriade de traitements automatiques, la lutte contre le terrorisme et la criminalité fait l'objet d'une législation internationale complexe faute de définition précise[1261].

[1257] Delphine Batho et Jacques Bénisti, *Rapport d'information N° 1548* enregistré à la Présidence de l'Assemblée nationale le 24 mars 2009.
[1258] Alain Bauer, *Fichiers de police et de gendarmerie : comment améliorer leur contrôle et leur gestion ?* décembre 2006, La Documentation française, p.128.
[1259] Ibid. p.131.
[1260] Ibid. p.134.
[1261] Ghislaine Doucet, « Terrorisme : définition, juridiction pénale internationale et victimes », *Revue internationale de droit pénal*, 2005/3 (Vol. 76), pp. 251-273. URL : https://www.cairn.info/revue-internationale-de-droit-penal-2005-3-page-251.htm consulté le 6 janvier 2018.

Section 2. Une lutte contre le terrorisme et la cybercriminalité, mosaïque de droits complexe

La cybercriminalité est internationale, les infractions peuvent être commises simultanément dans plusieurs pays comme ce fut le cas avec WannaCry en mai 2017[1262]. À l'origine conçue comme une succession de défis à la sécurité des réseaux, elle est devenue une activité mafieuse, donnant naissance à de véritables « marchés noirs » d'informations piratées, allant des atteintes à l'identité et à la propriété intellectuelle, aux fraudes à la carte bancaire et à la demande de rançon comme pour un kidnapping[1263]. Elle peut s'attaquer aux individus, aux entreprises et aux États. Elle est utilisée aussi par des réseaux terroristes[1264]. Pour être efficace, la lutte contre la cybercriminalité doit être internationale, les auteurs des attaques étant localisés dans des territoires autres que ceux des États attaqués. Mais comme l'écrit dans son rapport 2001, l'observatoire national de la délinquance et des réponses pénales, « *de la même façon qu'il existe des paradis fiscaux, il existe encore de gros progrès à faire sur l'harmonisation des législations et leur implémentation effective. Certains pays sont parfois considérés comme de véritables paradis numériques pour la cybercriminalité* »[1265].

Peu d'États reconnaissent avoir fait l'objet de cyberattaques, aussi les quelques cas reconnus sont-ils exemplaires. Ces attaques rendues publiques concernent : des dénis de service, provoqués par un envoi massif et ciblé sur un serveur ou groupe de serveurs de requêtes de connexion, provoquant la saturation du serveur et son indisponibilité ; la contagion par des chevaux de Troie d'ordinateurs personnels pour intercepter des fichiers stratégiques. Lors de l'attaque des ordinateurs du ministère des Finances françaises avant un G20[1266], ce type

[1262] « Rançongiciel WannaCry : les Etats-Unis incriminent la Corée du Nord », *LeMonde.fr,* 19 décembre 2017, URL : http://www.lemonde.fr/logiciel-de-racket-wannacry/article/2017/12/19/rancongiciel-wannacry-les-etats-unis-incriminent-la-coree-du-nord_5231600_5128888.html consulté le 9 avril 2018.

[1263] Thomas Cassuto, « Vie privée, vie publique et cybercriminalité », *Sécurité globale*, 2008/4 (n° 6), pp. 45-66. URL : https://www.cairn.info/revue-securite-globale-2008-4-page-45.htm consulté le 9 avril 2018.

[1264] Mounir Laldji, « Les menaces des entités criminelles transnationales sur la sécurité intérieure des États », *Sécurité globale*, 2016/2 (n° 6), pp. 43-62. URL : https://www.cairn.info/revue-securite-globale-2016-2-page-43.htm consulté le 9 avril 2018.

[1265] Eric Freyssinet, « L'Europe en lutte contre la cybercriminalité » in *La criminalité en France, Rapport de l'Observatoire national de la délinquance et des réponses pénales* 2011, Novembre 2011, CNRS éditions, p. 887.

[1266] David Le Bailly, « Gigantesque affaire d'espionnage à Bercy », *Paris Match*, 7 mars 2011, à http://www.parismatch.com/Actu/Societe/Affaire-d-espionnage-au-ministere-par-de-l-Economie-et-des-Finances-Paris-Match-146419, consulté le 17 juin 2017.

d'attaque a été utilisé. Le gouvernement français qui a reconnu cette attaque[1267], en a minimisé les conséquences et proclamé qu'elle avait été détectée avant que les fichiers n'aient pu être interceptés et transmis à l'extérieur du ministère. Une cyberattaque a également bloqué une chaîne de télévision pendant plusieurs heures en s'infiltrant dans les ordinateurs de la chaîne[1268]. Suite à cette attaque, le ministre de l'Intérieur a annoncé la création de 500 emplois supplémentaires aux 452 ayant été créés en deux ans, dont 100 dédiés à la plateforme de signalement PHAROS (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), plateforme intégrée à l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication[1269].

Compte tenu du secret entourant les cyberattaques vers les États, il est difficile de connaître l'importance et le nombre des attaques. Seules les attaques visibles sont connues. Cependant, les États mettent en place un arsenal de moyens permettant de lutter contre de telles attaques ou de les prévenir en tentant de neutraliser les groupes préparant des attaques ou des attentats. Ces moyens consistent à doter les forces de l'ordre de moyens légaux et techniques leur permettant de surveiller les réseaux et de prévenir les attaques.

En France, comme le précise la loi du 18 décembre 2013[1270], le Premier ministre *« définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information »*, l'ANSSI, rattachée au secrétaire général de la défense et de la sécurité nationale[1271]. La stratégie française est définie par quatre objectifs : « *être une puissance mondiale de cyberdéfense et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie ; garantir la liberté de décision de la France par la protection de l'information de souveraineté ; renforcer la cybersécurité des infrastructures vitales nationales ; et assurer la sécurité dans le cyberespace.[1272]* » Ainsi, dans cette stratégie,

[1267] « Bercy : la cyber-attaque visait le G20. Plus de 150 ordinateurs ont été piratés depuis décembre, selon Paris-Match. Baroin confirme. », *Europe 1*, 7 mars 2011, à http://www.europe1.fr/france/bercy-la-cyber-attaque-visait-le-g20-442555, consulté le 17 juin 2017.

[1268] Cyberattaque contre la chaîne francophone TV5 Monde du 8 avril 2015 (Frantz Vaillant, « TV5Monde : une cyberattaque inquiétante », 10 avril 2015, *TV5 Monde*, URL : https://information.tv5monde.com/info/tv5monde-une-cyberattaque-inquietante-27502 consulté le 10 avril 2018).

[1269] Les signalements se font par le portail dédié à l'URL : https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action .

[1270] Loi nº 2013-1 168 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* publiée au JORF nº0294 du 19 décembre 2013 p. 20570.

[1271] Extrait de http://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/ lu le 7 décembre 2015.

[1272] Ibid.

il est reconnu que la protection des données permet de garantir la liberté de décision. Cette protection des données a fait l'objet de la loi Godfrain[1273] en 1988, modifiée par la loi pour la confiance dans l'économie numérique[1274].

Au niveau international, l'Organisation des Nations Unies (ONU) a initié des travaux afin d'aboutir à une Convention universelle de la cybercriminalité[1275]. Le projet de déclaration de Salvador faisant suite au douzième congrès des Nations Unies pour la prévention du crime et la justice sociale[1276] constate « que *le développement des technologies de l'information et des communications et l'utilisation croissante d'Internet ouvrent de nouvelles possibilités aux délinquants et favorisent la progression de la criminalité* » et préconise une amélioration de *« la législation nationale et de renforcer la capacité des autorités nationales, pour lutter contre la cybercriminalité, sous toutes les formes* ». Il invite « *la Commission pour la prévention du crime et la justice pénale à convoquer un groupe intergouvernemental d'experts à composition non limitée en vue de réaliser une étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États membres, la communauté internationale et le secteur privé* ». Certains des pays présents ne souhaitaient pas aller au-delà de la Convention de Budapest qui est l'instrument juridique international en matière de lutte contre la cybercriminalité[1277]. La convention définit les infractions d'accès illégal, d'interception illégale, d'atteinte à l'intégrité des données, d'atteinte à l'intégrité du système, des infractions informatiques, falsifications ou fraudes informatiques[1278], et des infractions liées à la pornographie enfantine ou aux atteintes à la propriété intellectuelle. La tentative et la complicité sont également retenues comme infractions[1279].

[1273] Loi nº 88-19 du 8 janvier 1988 *relative à la fraude informatique* publiée au Journal officiel du 6 janvier 1988 p. 231.

[1274] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique*, Chapitre II : Lutte contre la cybercriminalité, Article 41 à 46, publiée au JORF nº0143 du 22 juin 2004 p. 11168.

[1275] Guérric Poncet, « Cybercriminalité : vers une convention de l'ONU ? », 24 novembre 2011, *Le Point Tech & Net,* URL : http://www.lepoint.fr/high-tech-internet/cybercriminalite-vers-une-convention-de-l-onu-23-11-2011-1399291_47.php consulté le 6 janvier 2018.

[1276] Nations Unies, *Projet de déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux : les systèmes de prévention du crim et de justice pénale et leur évolution dans un monde en mutation,* Douzième Congrès des Nations unies pour la prévention du crime et de la justice pénale, Salvador (Brésil), 12-19 avril 2010, URL : http://www.un.org/fr/documents/view_doc.asp?symbol=A/CONF.213/L.6/Rev.2 consulté le 13 novembre 2015.

[1277] Brigitte Pereira, « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », *Revue internationale de droit économique*, 2016/3 (t. XXX), pp. 387-409. URL : https://www.cairn.info/revue-internationale-de-droit-economique-2016-3-page-387.htm consulté le 9 avril 2018.

[1278] Reprenant ainsi les incriminations pénales définies par la loi Godfrain dès 1988 (Loi nº 88-19 du 5 janvier 1988 *relative à la fraude informatique*).

[1279] Cf. ci-après Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 3. § 1 -A) La convention de Budapest.

Au niveau européen, l'Europe de la lutte contre la cybercriminalité prend un nouveau virage avec la création d'un véritable outil commun, un Centre européen de lutte contre la Cybercriminalité officiellement inauguré le 11 janvier 2013 dans les locaux d'Europol à La Haye aux Pays-Bas, dont la création avait été officiellement annoncée le 28 mars 2012[1280]. Sa mission est de centrer son action sur les activités illicites suivantes : la fraude en ligne, notamment financière, perpétrée par des organisations criminelles ; l'exploitation sexuelle des enfants sur Internet ; les attaques des infrastructures critiques et des systèmes d'information de l'Union européenne. Le Centre doit également faciliter les travaux de recherche et développement (R et D) dans le domaine, contribuer au renforcement des capacités dont disposent les services européens de police, les juges et les procureurs en la matière, élaborer des rapports et publier des alertes précoces. Un an après sa création, son premier rapport[1281] était publié[1282] et insistait sur l'apparition de nouveaux *malware* et de cybercriminalité transfrontière ciblant des individus fragiles.

Au niveau de l'Union européenne, un règlement régissant l'identification électronique et les services de confiance[1283] est entré en vigueur en France en juillet 2016, une directive Network and Information Security (NIS) établit des mesures harmonisées pour assurer un niveau élevé et commun de sécurité des réseaux et des systèmes d'information[1284]. Cette directive doit être transposée par les États membres au plus tard le 9 mai 2018 pour une application au 10 mai 2018. La sécurité des réseaux devient une préoccupation de l'Union européenne.

[1280] Commission européenne, Communiqué de Presse du 9 janvier 2013 : « *Le Centre européen de lutte contre la cybercriminalité (EC3) sera inauguré le 11 janvier* » disponible à http://europa.eu/rapid/press-release_IP-13-13_fr.htm, consulté le 17 juin 2017.

[1281] EC3 EUROPOL, *First Year Report*, disponible en ligne à l'URL : https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf consulté le 17 juin 2017.

[1282] A l'occasion de la publication de ce rapport, le chef du centre déclarait : « *Dans les 12 mois qui ont suivi la création de l'EC3, nous nous sommes investis à fond avec les autorités répressives de toute l'Union européenne dans la lutte contre la cybercriminalité transfrontière, y compris au niveau des enquêtes. Je suis fier et satisfait de nos résultats, mais nous ne pouvons nous reposer sur nos lauriers. Je suis particulièrement préoccupé par l'émergence de logiciels malveillants de plus en plus complexes et de formes technologiquement avancées de cyberescroquerie, ainsi que du cyberharcèlement à l'égard des mineurs. Nous n'avons encore vu que la partie émergée de l'iceberg. Néanmoins, l'EC3, avec l'appui très apprécié de ses parties prenantes et de ses partenaires, se consacrera tout entier au soutien des opérations que les États membres engageront pour combattre frontalement la cybercriminalité* ».

[1283] Règlement (UE) nº 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* publié au Journal Officiel de l'Union européenne du 28 août 2014.

[1284] Directive (UE) 2016/1 148 du Parlement européen et du Conseil du 6 juillet 2016 *concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, publiée au Journal officiel de l'Union européenne du 19 juillet 2016.

L'OTAN s'est dotée en 2008 d'une cellule spécialisée dans la cybermenace[1285]. Dans le rapport de 2012, il est fait état du coût économique de l'insécurité[1286] face au surcoût engendré par les mesures de protection. Plusieurs autres pays ont créé de telles cellules. Mais en parallèle, les États se sont dotés d'un arsenal législatif permettant de lutter contre le terrorisme et d'accroître la sécurité.

En matière d'Internet, toute législation nationale se heurte au fait que le réseau est mondial et dominé par les États-Unis d'Amérique, tant par la nationalité des sociétés présentes sur le réseau Internet, les GAFA, que par une législation américaine hégémonique et extraterritoriale. Au niveau européen, de nombreuses directives concernent la société numérique obligeant chaque État membre à transcrire dans sa législation ces ordonnances, produisant des différences liées à cette adaptation, différences qui vont se réduire du fait de la mise en application du nouveau règlement dès 2018.

Sous-section 1. Une législation nationale fragilisée par des accords internationaux

La législation protégeant les libertés existe dans tous les États démocratiques de l'Union européenne, mais cette législation peut être empêchée par des traités internationaux ou par des directives ou règlements de la Commission européenne, voire limitée par la loi dans l'intérêt général. En France, État moniste, les traités auxquels la Nation a adhéré prévalent sur sa législation propre[1287]. Pour cette raison, alors que le Président de la République négocie et ratifie les traités[1288], le Parlement doit approuver la signature des traités internationaux qui modifient des dispositions de nature législative ou relatifs à l'état des personnes[1289].

[1285] Lire à ce sujet le « *Rapport annuel 2012 du secrétaire général* » de l'OTAN, en particulier le paragraphe « *La cyberdéfense* », disponible à http://www.nato.int/cps/fr/natohq/opinions_94220.htm, consulté le 21 juin 2017.

[1286] OTAN, Rapport 2012, « *S'il est vrai qu'il y a un prix à payer pour la sécurité, il faut aussi savoir que l'insécurité peut coûter beaucoup plus cher.* »

[1287] Règle *Pacta sunt servanda (les accords doivent être conservés).*

[1288] Constitution de la République, 4 octobre 1958, article 52 : « *Le Président de la République négocie et ratifie les traités.* »

[1289] Ibid, article 53 : « *Les traités de paix, les traités de commerce, les traités ou accords relatifs à l'organisation internationale, ceux qui engagent les finances de l'État, ceux qui modifient les dispositions de nature législative, ceux qui sont relatifs à l'état des personnes, ceux qui comportent cession, échange ou adjonction de territoire, ne peuvent être ratifiés ou approuvés qu'en vertu d'une loi.* »

Au niveau européen, le traité de Lisbonne[1290] permet aux parlements des États membres de s'opposer à des propositions législatives qui ne respecteraient pas le principe de subsidiarité[1291]. Mais l'Union dispose d'une compétence exclusive dans certains domaines[1292], en particulier pour la conclusion d'un accord international prévue dans un acte législatif de l'Union ou nécessaire à l'exercice de sa compétence interne ou susceptible d'altérer les règles communes ou d'en altérer la portée. Ainsi l'Union européenne peut-elle négocier des accords internationaux concernant l'adéquation des pays concernant la protection des données personnelles sans que les parlements nationaux ne puissent s'y opposer alors que de tels accords peuvent restreindre certaines protections individuelles garanties par les législations nationales, voire communautaires[1293].

Si la défense des libertés reste une règle respectée globalement par les états démocratiques, la surveillance des individus a de tout temps était présente dans les préoccupations des États, surveillance pouvant devenir obsessionnelle et occultant les principes généraux de droit. Dans les petites sociétés, la surveillance de tous, sous le regard de tous reste prédominante[1294]. Dans un État démocratique, la surveillance concerne le comportement des individus au regard du droit qui légitime la capacité à surveiller les individus, il s'agit alors d'une surveillance basée sur leur comportement ou sur leurs opinions publiques ou religieuses. La France au cours de son histoire a connu de véritables régimes de surveillance : la Convention, le Premier et le Second Empire, l'époque de Vichy et l'Occupation[1295]. Pour la surveillance des individus, l'État dispose de moyens techniques : des fichiers, des moyens d'identification comme la photographie, les fiches anthropométriques mises en place par Alphonse Bertillon dès 1879[1296],

[1290] Traité signé à Lisbonne le 13 décembre 2007 entre les vingt-sept États membres de l'Union européenne, qui transforme l'architecture institutionnelle de l'Union. Les modifications apportées aux traités existants avant sa signature, le traité instituant la Communauté européenne (Rome, 1 957) rebaptisé « traité sur le fonctionnement de l'Union européenne » et le traité sur l'Union européenne (Maastricht, 1 992), sont entrées en vigueur le 1er janvier 2009.

[1291] Traité sur le fonctionnement de l'Union européenne, article 69.

[1292] Ibid. article 3.

[1293] Négociations en cours pour un accord de libre-échange entre les États-Unis d'Amérique et l'Union européenne ou accord PNR Union européenne-Canada.

[1294] Sébastien Laurent, « Faire l'histoire de la surveillance » in Christian Aghroum, et al. *Identification et surveillance des individus : Quels enjeux pour nos démocraties ?* Nouvelle édition [en ligne]. Paris : Éditions de la Bibliothèque publique d'information, 2010, p. 26. Disponible sur Internet : http://books.openedition.org/bibpompidou/1192, consulté le 15 juillet 2017.

[1295] Ibid.

[1296] Jean-Lucien Sanchez, « Alphonse Bertillon et la méthode anthropométrique », *Sens-Dessous*, 2012/1 (n° 10), pp. 64-74. URL : https://www.cairn.info/revue-sens-dessous-2012-1-page-64.htm consulté le 9 avril 2018.

les empreintes digitales et aujourd'hui l'ADN. L'administration a, de tout temps, investi les techniques pour améliorer sa capacité de surveillance : télégraphe, téléphone, radio, etc.
Les possibilités fournies par la technique numérique et l'accroissement des puissances de calcul des ordinateurs ont permis l'émergence d'une surveillance de masse réelle et effective au détriment du respect des libertés. Si en période « normale », cette surveillance reste discrète, elle peut devenir plus invasive en période de troubles ou de risques d'attentats. Une législation spéciale de lutte contre les attentats a ainsi vu le jour au titre de la sécurité, cette législation particulièrement liberticide était cantonnée à la proclamation de l'état d'urgence. À partir de novembre 2017, une loi renforçant la sécurité intérieure et la lutte contre le terrorisme introduit dans le droit « commun » les possibilités administratives d'assignation à résidence, de fermeture de lieus de culte, de visites domiciliaires et de surveillances individuelles dès qu'un comportement « constitue une menace d'une particulière gravité pour la sécurité et l'ordre public »[1297].

§ 1 - Une législation sécuritaire et asymétrique

Outre les exceptions liées à l'intérêt général, introduites dans les législations nationales et internationales, des lois spécifiques ont été adoptées durant les dix premières années de ce siècle pour renforcer la sécurité et la sûreté en réduisant ou limitant la protection des individus ou celle de leur vie privée[1298]. Le texte emblématique de la politique sécuritaire mise en place par les États est le USA Patriot Act[1299]. Dans la pratique, cette loi autorise les services de sécurité à accéder aux données informatiques détenues par les particuliers et les entreprises, sans autorisation préalable et sans en informer les utilisateurs. Elle permet de maintenir en détention, des individus non-citoyens américains suspectés d'être des ennemis de l'extérieur.
Au niveau français, il existe aussi des textes adoptés après ces attentats, textes qui restreignent les droits des personnes relativement à la protection de leur vie privée. M. Sarkozy, ancien Président de la République française, initiateur de nombreux textes répressifs soit comme

[1297] Loi n° 2017-1510 du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme* publiée au JORF n°0255 du 31 octobre 2017.
[1298] Didier Bigo, « Chapitre 16. Un espace de liberté, de sécurité et de justice? », dans *Politiques européennes.* Paris, Presses de Sciences Po (P.F.N.S.P.), « Les Manuels de Sciences Po », 2009, pp. 331-352. URL : https://www.cairn.info/politiques-europeennes--9782724611328-page-331.htm consulté le 9 avril 2018.
[1299] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Public Law 107–56, October 26, 2001.

ministre de l'Intérieur, soit comme Président, a été mis sur écoutes téléphoniques pendant plusieurs mois par application de ces textes. À côté de ces lois sécuritaires, il existe des accords internationaux de coopération ne respectant pas les protections individuelles légales[1300].

L'une des premières lois promulguées en France est la loi d'orientation et de programmation pour la sécurité intérieure[1301]. Le fichage est fortement facilité par les forces de l'ordre dans la nouvelle loi. La Commission de l'informatique et des libertés s'est inquiétée des dangers de l'utilisation des fichiers prévue par le projet de loi sur la sécurité[1302].

Dix ans plus tard, le 14 mars 2011, une nouvelle loi d'orientation, dite LOPPSI 2[1303], est promulguée. Dès le mois de juillet 2009, la CNIL avait rendu public son avis sur plusieurs articles de la loi dont l'installation des « mouchards »[1304]. Cette loi dispose d'un volet de lutte contre la cybercriminalité et augmente les moyens de vidéosurveillance dans les lieux publics, étend les possibilités d'écoutes téléphoniques. Ces deux lois LOPSI et LOPPSI 2, montrent que sous couvert de lutte contre le terrorisme et la délinquance, les États réduisent les droits des citoyens concernant la protection des données personnelles et de la vie privée.

Par ailleurs, lors de la transposition de la directive 95/46/CE pour la protection de la vie privée et des données à caractère personnel, la Commission de l'informatique et des libertés s'est vue privée d'une partie de ses prérogatives face au gouvernement qui, en cas d'un avis défavorable de la CNIL, peut passer outre, et doit seulement annexer l'avis défavorable de la CNIL à la publication du décret d'autorisation du traitement[1305].

Après les attentats de 2015, cette législation sécuritaire s'est étoffée et la France vit sous un régime d'exception : l'état d'urgence créé et mis en place durant la guerre d'Algérie. En

---

[1300] Elisabeth Autbier, « La CJUE déclare incompatible l'accord des données PNR signé avec le Canada », 28 juillet 2017, *Dalloz actualité*, URL : https://www.dalloz-actualite.fr/flash/cjue-declare-incompatible-l-accord-des-donnees-pnr-signe-avec-canada, consulté le 9 avril 2018.

[1301] Loi nº 2002-1 094 du 29 août 2002 *d'orientation et de programmation pour la sécurité intérieure (LOPSI).*

[1302] Claude Lienhard, « La loi d'orientation et de programmation pour la sécurité intérieure », *La Semaine juridique*, édition générale nº 37, 11 septembre 2002.

[1303] Loi nº 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

[1304] Malgré des recherches sur Internet et sur le site de la CNIL, l'auteur n'a pas réussi à retrouver cet avis. Seuls sont disponibles les commentaires des journaux relatant cette publication intitulée « Délibération n°2009-200 du 16 avril 2009 *portant avis sur sept articles du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure* ». Par contre, l'avis de la Commission nationale consultative des droits de l'homme est facilement accessible (Commission nationale consultative des droits de l'homme, « Avis sur le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (Adopté par l'assemblée plénière du 15 avril 2010) », URL : http://www.cncdh.fr/sites/default/files/10.04.15_avis_loppsi.pdf consulté le 9 avril 2018).

[1305] Cf. Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 1. § 1 -B)1) L'assouplissement de la loi informatique et libertés.

novembre 2017, certaines dispositions de l'état d'urgence sont transposées dans le « droit commun »[1306]. Ainsi, d'un état d'exception temporaire permettant de faire face à un risque sécuritaire important, la législation française banalise cet état d'exception, et permet à l'administration d'utiliser les possibilités exceptionnelles offertes sans que le Parlement puisse décider de cette exception qui devient permanente.

Des restrictions aux libertés proviennent d'accords internationaux[1307]. Pour des raisons de lutte contre le terrorisme, des accords entre l'Union européenne et les États-Unis ont été conclus pour permettre le transfert des informations relatives aux passagers voyageant vers les États-Unis et contenues dans le Passenger Name Record ou PNR. En Europe, cet accord négocié entre la Commission européenne et le gouvernement des États-Unis d'Amérique a fait l'objet de nombreuses critiques du groupe de travail dit G29, entité qui regroupe les agences nationales de protection des données personnelles. Le premier accord a été signé en mai 2004, un nouvel accord a été renégocié en juillet 2007, mais ce nouvel accord reste controversé compte tenu du délai de rétention des informations par les agences américaines. En avril 2012, l'accord a été approuvé par le Parlement européen malgré des critiques concernant les recours insuffisants contre une utilisation inappropriée des données échangées. Ainsi un accord international, un traité, peut être négocié et conclu en dépit d'une inadéquation avec une législation nationale, et en droit international, un traité ratifié prévaut sur une législation nationale.

§ 2 - Une législation spécifique de lutte contre le terrorisme

Après les attentats contre l'hebdomadaire satirique « Charlie Hebdo » et le magasin Hypercacher en janvier 2015, la France a renforcé son arsenal légal de lutte contre le terrorisme. Après les attentats du 13 novembre 2015, l'état d'urgence a été appliqué, et maintenu jusqu'en novembre 2017, date à laquelle il a été remplacé par une loi antiterrorisme renforcée. Ce régime qui a été mis en place pendant deux ans, permet sans accord préalable d'un juge, des assignations à résidence, des perquisitions, des interdictions de cortèges, des contrôles d'identité et des fouilles de bagages et de véhicules, des fermetures de lieux de réunion, sur simple décision administrative.

[1306] Loi n° 2017-1510 du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme* publiée au JORF n°0255 du 31 octobre 2017.
[1307] Cf. Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 1. § 1 - Une législation sécuritaire et asymétrique.

La législation de lutte contre le terrorisme n'arrête pas les attaques terroristes comme a pu le constater la France avec les attentats de la nuit du vendredi 13 novembre 2015 et ses 120 morts et quelques 200 blessés ou l'attentat de Nice du 14 juillet 2016 sur la promenade des Anglais, ayant fait 84 morts et 200 blessés. L'état d'urgence a été prononcé sur tout le territoire français depuis le 13 novembre 2015 et maintenu pendant plus de deux ans. En France, l'état d'urgence est une situation spéciale qui restreint les libertés. Il « *confère aux autorités civiles, dans l'aire géographique à laquelle il s'applique, des pouvoirs de police exceptionnels portant sur la réglementation de la circulation et du séjour des personnes, sur la fermeture des lieux ouverts au public et sur la réquisition des armes* ». Cet état d'urgence a été créé par la loi[1308] pendant la guerre d'indépendance de l'Algérie pour faire face à la situation de l'époque, les autres régimes d'exception possibles en France sont l'état de siège[1309] encadré par l'article 36 de la Constitution[1310] en cas de guerre et les pouvoirs exceptionnels octroyés au Président de la République par l'article 16 de cette même Constitution. Une loi antiterrorisme renforcée permet de sortir de l'état d'urgence au 1er novembre 2017[1311], en transposant certaines possibilités administratives autorisées par l'état d'urgence dans le « droit commun » dès qu'une forte présomption de trouble à l'ordre public et à la sécurité existe ou qu'une présomption de préparation d'un attentat terroriste est détectée par les forces de renseignement. Ainsi, face au risque terroriste, des mesures d'exception sont introduites dans la législation courante, sans intervention du Parlement. Parmi ces mesures, figure l'interception des communications et les visites domiciliaires avec saisie des terminaux de télécommunication numérique (ordinateur, tablette ou smartphone).

[1308] Loi n° 55-385 du 3 avril 1955 *instituant un état d'urgence et en déclarant l'application en Algérie* publiée au JORF du 7 avril 1955 p. 3479.
[1309] L'état de siège est créé sous sa forme actuelle par la loi du 3 avril 1878. Elle a été abrogée par le 19° du I de l'article 5 de l'ordonnance n° 2004-1 374 du 20 décembre 2004, relative à la partie législative du code de la défense. Ce code de la défense précise : « *L.2121-1 L'état de siège ne peut être déclaré, par décret en conseil des ministres, qu'en cas de péril imminent résultant d'une guerre étrangère ou d'une insurrection armée.*
« Le décret désigne le territoire auquel il s'applique et détermine sa durée d'application.
« L.2121-2 Aussitôt l'état de siège décrété, les pouvoirs dont l'autorité civile était investie pour le maintien de l'ordre et la police sont transférés à l'autorité militaire.
« L'autorité civile continue à exercer ses autres attributions ».
[1310] Constitution du 4 octobre 1958, Article 36 « *L'État de siège est décrété en Conseil des ministres. Sa prorogation au-delà de douze jours ne peut être autorisée que par le Parlement* ».
[1311] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme publiée au JORF n°0255 du 31 octobre 2017.

En 1798, le terme « terrorisme » apparaît pour la première fois dans le supplément du dictionnaire de l'Académie française. Il désigne alors un mode de gouvernement[1312]. En décembre 1800, Napoléon Bonaparte échappe à l'un des premiers actes de terrorisme moderne : un attentat à la bombe perpétré par des royalistes chouans[1313]. Sans évoquer le terrorisme d'État mis en place en 1792 durant « La Terreur » par les révolutionnaires ni dans une période plus récente, les méthodes nazies d'extermination d'otages civils pour opposer la population aux Résistants, la France a connu une première période de terrorisme avec les anarchistes à la fin du XIXe siècle, et, après 1954, des actions terroristes liées au conflit interne avec l'indépendance de l'Algérie, mais aussi des actions terroristes liées à des revendications territoriales (Corse, Bretagne, Pays basque) ou idéologiques (groupes d'extrême gauche), puis les conflits dans le Moyen-Orient. Aujourd'hui, il semble que le risque terroriste soit la prolongation des attentats du 11 septembre 2001 à New York.

La législation contre le terrorisme a toujours été votée en réaction à des attentats, par des gouvernements qui ont réagi à chaud aux événements. Cette législation peut être considérée comme une législation de crise, les lois ainsi votées sont assorties d'une clause temporaire avec analyse de leur efficacité. Devant la difficulté d'anticiper les actes de terrorisme, les gouvernements vont édicter des lois de surveillance qui vont limiter les libertés fondamentales et même la sûreté des individus puisque les individus suspectés de préparer ou d'aider à la préparation d'un acte de terrorisme peuvent être arrêtés et privés de liberté avant d'avoir perpétré leur acte. Ces lois rappellent le film « minority report »[1314]. Dans ce film, grâce aux visions du futur fournies par trois individus exceptionnels doués de précognition, les agents de Précrime peuvent arrêter les criminels avant qu'ils n'aient commis leur méfait.

La première législation française antiterroriste regroupe les lois votées le 12 décembre 1893, le 18 décembre 1893 et le 28 juillet 1894. Ces lois sont abolies depuis le 23 décembre 1992. Elles seront restées applicables durant un siècle et auront connu trois républiques : la III[e] République

[1312] Jean-Pierre Gross, « Michel Vovelle (dir.), *Le tournant de l'an III : Réaction et Terreur blanche dans la France révolutionnaire,* Paris, Éditions du CTHS, 1997, 616 p., 300 F », *Revue d'histoire moderne et contemporaine*, 2001/4 (nº48-4), pp. 243-245. URL : https://www.cairn.info/revue-d-histoire-moderne-et-contemporaine-2001-4-page-243.htm consulté le 9 avril 2018.

[1313] Gilles Ferragu, « La France et ses "siècles de plomb" », *Confluences Méditerranée*, 2017/3 (n° 102), pp. 13-28. URL : https://www.cairn.info/revue-confluences-mediterranee-2017-3-page-13.htm consulté le 9 avril 2018.

[1314] Stéphane Spielberg, *Minority report*, sorti en 2002, d'après la nouvelle de Philip K. Dick.

qui les aura votées, la IV^e^ puis la V^e^ République[1315] qui les abrogera avec la publication du nouveau Code pénal au journal officiel[1316].

Ces lois ont été votées pour répondre à l'inquiétude de l'opinion et répondre à une série d'attentats anarchistes[1317]. La loi du 12 décembre 1893 suit l'attentat d'Auguste Vaillant visant les députés, et a pour objet de modifier la loi du 29 juillet 1881 sur la presse pour réprimer l'apologie, ou provocation indirecte, et permettre à un juge d'ordonner une saisie et une arrestation préventive. La loi du 18 décembre 1893 modifie la loi de 18 décembre 1853 sur les associations de malfaiteurs et vise les groupes anarchistes en permettant l'arrestation de tout membre ou sympathisant. Enfin, la loi du 28 juillet 1894 qui suit l'assassinat du président de la République Sadi Carnot par un jeune anarchiste à Lyon, a pour objet de réprimer directement les menaces anarchiques, elle permet une véritable chasse aux sorcières et aboutira au procès des trente[1318].

Le 30 avril 1894, Jean Jaurès, dans un discours à la chambre des députés, dénonce la politique répressive du gouvernement et l'usage d'agents provocateurs : « *C'est ainsi que vous êtes obligés de recruter dans le crime de quoi surveiller le crime, dans la misère de quoi surveiller la misère et dans l'anarchie de quoi surveiller l'anarchie.* »

Comme l'écrit Léon Blum[1319], ces lois scélérates « *abrogent les garanties conférées à la presse en ce qu'elles permettent la saisie et l'arrestation préventive ; elles violent une des règles de notre droit public en ce qu'elles défèrent des délits d'opinion à la justice correctionnelle ; elles violent les principes du droit pénal en ce qu'elles permettent de déclarer complices et associés d'un crime des individus qui n'y ont pas directement et matériellement participé ; elles blessent l'humanité en ce qu'elles peuvent punir des travaux forcés une amitié ou une confidence, et de la relégation un article de journal* ».

[1315] Bibia Pavard, Florence Rochefort, Michelle Zancarini-Fournel, « Chapitre 1 - Longévité des lois répressives », dans *Les lois Veil. Contraception 1974, IVG 1975.* Paris, Armand Colin, « U », 2012, pp. 15-30. URL : https://www.cairn.info/les-lois-veil--9782200249489-page-15.htm consulté le 9 avril 2018.

[1316] Loi n° 92-1336 du 16 décembre 1992 *relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur*, publiée au JORF n° 0298 du 23 décembre 1992 p. 17568.

[1317] Gilles Ferragu, « 3 - Le moment anarchiste en France et en Europe », dans *Histoire du terrorisme.* Paris, Éditions Perrin, « Synthèses historiques », 2014, pp. 96-126. URL : https://www.cairn.info/histoire-du-terrorisme--9782262047511-page-96.htm consulté le 8 janvier 2018.

[1318] Procès ouvert le 6 août 1894 devant la cour d'assises de la Seine durant lequel 30 inculpés furent jugés, allant de théoriciens de l'anarchie à de simples cambrioleurs, tous rassemblés dans une même accusation d'association de malfaiteurs.

[1319] Léon Blum alias « un juriste », « Comment ont été faites les lois scélérates » in *La Revue Blanche*, 1 juillet 1898.

Le risque anarchiste a pratiquement disparu aujourd'hui, mais le risque terroriste reste présent dans la vie contemporaine des Français depuis les « événements d'Algérie » et les attentats du FLN du 1er novembre 1954 à 1 957, et de l'OAS dans les années 1961 et 1962, contre les populations civiles tant des départements d'Algérie que de la métropole[1320]. Dans cette période, l'état d'urgence a été créé par la loi. Depuis ces attentats, des mesures de vigilance en cas de menaces d'agressions terroristes ont été mises en œuvre par une instruction interministérielle datant de 1978, prolongée en 1981 par le plan Pirate. En 1995, ce plan devient le plan Vigipirate[1321]. Il sera actualisé à plusieurs reprises depuis 2000. Il sera activé une première fois en 1991 durant la guerre du Golfe, mais surtout, il sera permanent à partir des premiers attentats du RER Saint Michel le 25 juillet 1995, et atteindra le niveau rouge en juillet 2005 suite aux attentats du métro de Londres. Le 20 février 2014, le code à plusieurs couleurs est abandonné au profit de deux niveaux d'alerte : le niveau Vigilance et le niveau Alerte attentat qui est mis en œuvre en région parisienne après les attentats de Charlie Hebdo du 7 janvier 2015.

Disposer des forces de police ou de l'armée pour prévenir des attentats sur certains sites n'est pas une mesure suffisante pour lutter contre le terrorisme. Il est nécessaire de donner aux services de sécurité des moyens d'investigation pour rechercher les individus qui pourraient préparer un attentat et les empêcher de passer à l'acte. La France dispose d'un arsenal législatif important pour mener ce type de missions. Mais, comme l'écrivaient les sénateurs dans la saisine du 23 décembre 2005 contre la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles des frontières « *L'indispensable volonté de prévenir et punir les actes de terrorismes ne saurait, en revanche, légitimer le glissement insidieux vers un état d'urgence permanent* »[1322]. Dans un État de droit, le droit à la sécurité doit toujours être concilié avec le droit à la sûreté, c'est-à-dire le droit de n'être ni surveillé, ni poursuivi, ni arrêté, ni détenu, ni condamné arbitrairement. Les sénateurs précisent que « *la plus grande victoire des terroristes serait que nous renoncions à l'État de droit* ».

[1320] Jenny Raflik, « La France face au terrorisme d'hier à aujourd'hui », *Outre-Terre*, 2017/2 (N° 51), pp. 202-214. URL : https://www.cairn.info/revue-outre-terre-2017-2-page-202.htm consulté le 8 janvier 2018.

[1321] Mathieu Rigouste, « 7. La guerre à l'intérieur : la militarisation du contrôle des quartiers populaires », dans *La frénésie sécuritaire. Retour à l'ordre et nouveau contrôle social.* Paris, La Découverte, « Sur le vif », 2008, pp. 88-98. URL : https://www.cairn.info/la-frenesie-securitaire--9782707154323-page-88.htm consulté le 9 avril 2018.

[1322] Conseil constitutionnel, Décision n° 2005-532 DC du 19 janvier 2006 *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, Saisine par 60 sénateurs du 23 décembre 2005, en ligne à l'URL : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2006/2005-532-dc/saisine-par-60-senateurs.101434.html consultée le 10 avril 2018.

Ainsi au XXI^e^ siècle, comme au XIX^e^ siècle, l'équilibre entre lutte contre le terrorisme et préservation des libertés individuelles reste difficile à conserver[1323]. La France s'est dotée d'une législation répressive et préventive face au terrorisme moderne. Mais, les terroristes se déjouant des frontières, une coordination internationale est nécessaire pour une lutte efficace.

A) La lutte contre le terrorisme dans la législation française

Les actes de terrorisme sont définis par l'article 421-1 du Code pénal : « *Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes : Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne, l'enlèvement et la séquestration ainsi que le détournement d'aéronef, de navire ou de tout autre moyen de transport, définis par le livre II du présent code ; les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définies par le livre III du présent code ; les infractions en matière de groupes de combat* » c'est-à-dire *« les groupements de personnes détenant ou ayant accès à des armes, dotés d'une organisation hiérarchisée, et susceptibles de troubler l'ordre public »*[1324] et les infractions liées à la fourniture d'un logement ou de subsides à l'auteur ou au complice d'un acte de terrorisme [1325]; ainsi que les infractions de blanchiment[1326] et les délits d'initié[1327] prévus au code monétaire et financier. Mais ces infractions ne sont considérées comme des actes de terrorisme que si elles sont perpétrées dans le but de troubler l'ordre public[1328]. Actes et volonté de troubles sont nécessaires, cette dualité a été acceptée par le Conseil constitutionnel. La protection de l'ordre public peut donc justifier la restriction des libertés prévue par les lois de lutte contre le terrorisme.

[1323] Samy Cohen, « Pourquoi les démocraties en guerre contre le terrorisme violent-elles les droits de l'homme ? », *Critique internationale*, 2008/4 (n° 41), pp. 9-20. URL : https://www.cairn.info/revue-critique-internationale-2008-4-page-9.htm consulté le 9 avril 2018.
[1324] Code pénal, articles 431-13 à 431-17.
[1325] Code pénal, article 434-6.
[1326] Code pénal, chapitre IV du titre II du livre III.
[1327] Code monétaire et financier, article L.465-1.
[1328] Thierry S. Renoux, « Juger le terrorisme ? » in *Dossier : La justice dans la constitution*, Cahiers du Conseil constitutionnel n° 14, mai 2003.

Ainsi, les actes proprement dits de terrorisme sont réprimés, mais aussi les actes liés à leur préparation et leur mise en place. Prévention et répression sont les deux axes de lutte contre le terrorisme, au travers d'une législation ancienne et continuellement mise à jour.

1) L'arsenal juridique français

La législation de lutte contre le terrorisme est ancienne et connaît des aménagements nombreux. Elle permet la mise en place d'un dispositif de lutte répressif et préventif. Le code de procédure pénale crée un régime spécial pour les affaires de terrorisme. Les règles concernant l'enquête et l'instruction sont plus souples que dans le régime général. « *Les bases de la législation antiterroriste en France ont été posées par la loi nº 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État. Elle repose, d'une part, sur la définition d'infractions à caractère terroriste, d'autre part, sur la mise en place de règles procédurales spécifiques. Ces dispositions s'inscrivent dans le cadre de notre droit pénal et ne dérogent pas aux grands principes qui le gouvernent* »[1329].

a) Les premières lois de lutte contre la cybercriminalité

La première loi spécifique au développement de l'informatique et à sa capacité de stockage est la loi nº 78-17du 6 janvier 1978 dite « loi informatique et libertés »[1330]. Elle définit de nouveaux droits au citoyen en termes de contrôle et de préservation des libertés. Cette loi qui a institué la CNIL lui a donné un pouvoir de sanction administrative et pénale en cas de non-respect des obligations de déclaration et d'autorisation préalable à tout traitement automatique de données à caractère personnel. Les sanctions pénales ne sont que des amendes plafonnées à 150 000 € ou 300 000 € en cas de récidive, ces sanctions pénales ne sont pas dissuasives pour les grandes entreprises internationales comme Google ou Facebook, pour ne citer que celles-ci. Google a été condamné à une amende de 150 000 € par la CNIL alors qu'en 2012 son bénéfice était de plus d'un milliard de dollars. Le Règlement général sur la protection des données porte le montant maximum de ces amendes administratives « *à 20 000 000 EUR ou, dans le cas d'une*

[1329] Extrait du rapport de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale du Sénat du 10 octobre 2012 concernant le projet de loi nº6 relatif à la sécurité et à la lutte contre le terrorisme.
[1330] Cf. Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 1. § 1 -A) Une loi française innovante protégeant les données personnelles

entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu »[1331].

Les sanctions administratives sont souvent plus persuasives, car publiques. Ce sont la fermeture de l'application ou la nécessité de modification de l'application, ou un simple avertissement public qui peut être plus dissuasif pour une grande entreprise que l'amende. Le groupe ORANGE a été condamné par la CNIL (avertissement au public) pour insuffisance de sécurité suite au vol de données à caractère personnel relatives aux abonnés d'ORANGE[1332].

La seconde loi importante en matière de cybercriminalité est la loi n° 88-19 du 5 janvier 1988, dite loi Godfrain du nom du sénateur qui en est à l'origine, adoptée dix ans après la loi informatique et libertés[1333]. Cette loi sanctionne les tentatives d'accès à un système informatique, le maintien dans ce système, la destruction de données ou l'entrave au bon fonctionnement d'un système informatique. Cette loi a été intégrée dans le Code pénal dans un chapitre III « Des atteintes aux systèmes de traitement automatisé des données ». Cette loi vise les campagnes de SPAM, la propagation des virus et les attaques de déni de service. La tentative est punie des mêmes peines que la réalisation de l'infraction. La difficulté d'application de cette loi tient au fait que nombre de ces attaques sont perpétuées à partir d'un territoire extérieur au territoire français et même européen. Si les juges français sont compétents pour juger de tels faits dont les effets sont produits sur le territoire français, il est difficile de faire appliquer la sanction dans ces États où de telles législations n'existent pas.

Une troisième loi importante a complété la loi Godfrain, il s'agit de la loi du 21 juin 2004 dite loi pour la confiance dans l'économie numérique. En particulier, cette loi a incriminé le fait d'aspirer un site ou de le défigurer. Elle a également réprimé le fait de diffuser des informations concernant les failles de sécurité. Cette loi a créé un droit de l'Internet.

D'autres textes ont complété la loi Godfrain, la directive 2009/136/CE, transposée via un nouvel article dans la loi informatique et libertés, qui prévoit que lorsqu'une faille de sécurité est constatée sur un service de communication électronique, l'autorité nationale compétente doit en être informée, les personnes dont les données à caractère personnel auraient pu faire l'objet d'une violation doivent en être informées et le service de communication électronique

[1331] Règlement général de protection des données, Art. 83.

[1332] « La Cnil sanctionne Orange après une importante faille de sécurité », 26 aout 2014, *Le Figaro.fr*, URL : http://www.lefigaro.fr/secteur/high-tech/2014/08/26/01007-20140826ARTFIG00117-la-cnil-sanctionne-orange-apres-une-importante-faille-de-securite.php consulté le 10 avril 2018.

[1333] Cf. Partie 1. Titre 1. Chapitre 2. Section 2. Sous-section 1. Une Loi relative à la fraude informatique, dite « loi Godfrain »

doit leur fournir des recommandations appropriées. Lors du vol de données perpétré chez ORANGE, ce dernier a contacté tous ses abonnés concernés. Le non-respect de cette directive expose l'opérateur à des sanctions pénales.

De nouvelles lois visent à améliorer la sécurité et à lutter contre la criminalité et le terrorisme[1334]. La loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers a pris en compte l'importance d'Internet comme vecteur de propagation et d'échange d'informations à visée terroriste. Elle assimile les cybercafés et les bornes Wi-Fi à des opérateurs de téléphonie qui doivent assurer la conservation des données.

La loi d'orientation de programmation et de performance sur la sécurité intérieure du 14 mars 2011, appelée LOPPSI 2 crée une infraction nouvelle d'usurpation d'identité en ligne et permet la captation de données informatiques en installant un cheval de Troie à l'insu de la personne soupçonnée de certaines infractions graves, sous contrôle strict d'un magistrat. Mais, c'est depuis 1986 que la France a élaboré progressivement un ensemble de lois de lutte contre le terrorisme, chacune de ces lois attentant aux libertés individuelles pour permettre la recherche et la prévention des attentats.

b) La litanie législative de lutte contre le terrorisme

La loi du 9 septembre 1986[1335] est la première loi française spécialement dédiée à la lutte contre le terrorisme. Elle a été adoptée en réaction aux attentats de 1985 et 1986[1336]. La loi du 9 septembre 1986 a créé dans le livre IV du Code de procédure pénal un titre intitulé : « *Titre XIV*

[1334] Cf. Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 1. § 2 -A) La lutte contre le terrorisme dans la législation française.

[1335] Loi n° 86-1020 du 9 septembre 1986 *relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État*, publiée au JORF n°0210 du 10 septembre 1986 page 10956.

[1336] Attentats du 23 février 1985 (magasin Marks & Spencer : 1 mort, 14 blessés), du 4 et du 9 mars (cinéma Rivoli Beaubourg : 18 blessés), le double attentat des magasins « Galeries Lafayette » et « Printemps Haussmann », le 7 décembre (43 blessés), l'attentat à la galerie marchande de l'Hôtel Claridge situé sur les Champs-Élysées (8 blessés) et la tentative au 3e étage de la tour Eiffel du 3 février 1986, suivis de l'attentat à la librairie Gibert jeune (5 blessés) et à la FNAC du Forum des Halles (22 blessés) les 4 et 5 février, puis le 20 mars dans la galerie Point Show des Champs-Élysées (2 morts et 29 blessés). Après une pause et la promulgation de la loi, les attentats reprendront : 4 septembre tentative dans le RER à gare de Lyon, 8 septembre bureau de poste de l'Hôtel de Ville (1 mort et 21 blessés), 12 septembre cafeteria Casino au centre commercial de la Défense (54 blessés), 14 septembre pub Renault sur les Champs Élysées (2 policiers et un serveur tués), 15 septembre locaux du permis de conduire à la préfecture de Police à Paris (1 mort, 56 blessés) et le 17 septembre magasin Tati rue de Rennes (7 morts et 55 blessés).

– Des infractions en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur »[1337] et donne compétence au procureur de la République, au juge d'instruction, au tribunal correctionnel et à la cour d'assises de Paris pour les actes de terrorisme sur l'ensemble du territoire national. Le délai de garde à vue de quarante-huit heures peut être renouvelé une fois, portant le délai maximal de garde à vue à quatre-vingt-seize heures. Ce délai a été porté en 2006 à six jours[1338], l'entretien avec un avocat n'étant possible qu'à la quatre-vingt-seizième heure ou à la cent vingtième[1339]. Le nouveau Code pénal de 1992[1340] transfère la définition des actes de terrorisme de l'article 706-16 de code de procédure pénale à l'article 421-1 du Code pénal donnant ainsi officiellement naissance aux infractions de terrorisme[1341].

Après les attentats de 1995[1342], la répression est renforcée par la loi du 22 juillet 1996[1343]. Après la promulgation de cette loi, un nouvel attentat sera perpétré sur le RER[1344]. L'incrimination de terrorisme est étendue à la participation à un groupement tendant à préparer un des faits matériels caractérisés comme un acte de terrorisme[1345]. Mais, le Conseil constitutionnel a censuré dans cet article 1er, l'incrimination de « l'aide à l'entrée, à la circulation ou au séjour irréguliers d'un étranger »[1346].

Alors que la France ne connaît plus de vague d'attentats, de nouvelles lois sécuritaires vont être promulguées pour contenir le sentiment d'insécurité qui se développe après les attentats du 11 septembre 2001 à New York. Ces nouvelles lois vont prendre en compte l'évolution des techniques, et en particulier l'utilisation du réseau Internet et des techniques numériques.

[1337] Article 1er, loi no 86-1020 du 9 septembre 1986.

[1338] Loi no 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* publiée au JORF no 20 du 24 janvier 2006 p. 1129.

[1339] Code de procédure pénale, article 706-88.

[1340] Cf. supra.

[1341] Julie Alix, « Fascicule 20 : Terrorisme », *Jurisclasseur* 15 mars 2011, mis à jour 30 juin 2014.

[1342] Attentats dans les stations parisiennes de métro ou de RER Saint-Michel (25 juillet 1995, 8morts et 117 blessés), Maison-Blanche (6 octobre 1995, 12 blessés légers), et plusieurs autres endroits (place de l'Etoile le 17 août, 11 blessés, marché Richard Lenoir à Paris le 3 septembre, 4 blessés, Villeurbanne le 7 septembre, 14 blessés, gare du Musée d'Orsay à Paris le 17 octobre, 26 blessés).

[1343] Loi no 96-647 du 22 juillet 1996 *tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire* publiée au JORF no170 du 23 juillet 1996 p. 11104.

[1344] Attentat sur le RER à la station Port-Royal (3 décembre 1996, 4 morts et 91 blessés).

[1345] Article 3 de la loi no 96-647.

[1346] Conseil constitutionnel, Décision no 96-377 DC du 16 juillet 1996 *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire.*

La loi du 15 novembre 2001[1347] contraint plus fermement la vente et la détention d'armes de guerre. Cette même loi comporte un Chapitre V « *Dispositions renforçant la lutte contre le terrorisme* ». Conscient de l'évolution permanente des moyens utilisés par les terroristes, les dispositions de ce chapitre sont adoptées pour une période courte (jusqu'au 31 décembre 2003 soit deux ans environ), et soumises à un rapport d'évaluation avant la fin de cette période. La visite d'un véhicule sur réquisition du procureur de la République est autorisée. Dans le cas d'une enquête concernant des armes de guerre, la visite de locaux autres que des locaux à usage d'habitation peuvent avoir lieu à toute heure après une décision du juge des libertés et de la détention. Les opérateurs de télécommunications doivent pouvoir conserver pour des besoins d'enquêtes criminelles les données techniques durant une année. Les fournisseurs de prestations de cryptologie doivent fournir sur demande les conventions permettant le déchiffrement des données cryptées. Le fait de financer une entreprise terroriste devient également un acte de terrorisme.

Une nouvelle loi est promulguée le 9 septembre 2002[1348] pour alléger le code de procédure pénale et le rendre plus efficace ainsi qu'une loi pour la sécurité intérieure le 18 mars 2003[1349]. Les dispositions de la loi du 15 novembre 2001 concernant la lutte contre le terrorisme y sont prorogées jusqu'au 31 décembre 2005. Cette dernière loi officialise les traitements automatiques des données personnelles recueillies lors des enquêtes par la police et la gendarmerie, de plus, ces données peuvent être transmises « *à des organismes de coopération internationale en matière de police judiciaire ou à des services de police étrangers* ».

Le 9 mars 2004, une loi[1350] pour adapter la justice aux évolutions de la criminalité est promulguée. Son article 17 crée dans le livre IV du code de procédure pénale, un nouveau titre « *Titre X — De l'entraide judiciaire internationale* ». Le mandat d'arrêt européen y est reconnu et traité, les faits de terrorisme sont concernés, car passibles de plus d'un an d'emprisonnement. L'article 24 de cette loi crée un nouveau titre dans le code de l'organisation judiciaire « *Titre V – Les juridictions spécialisées prévues par les articles 704, 706-2 et 706-75 du code de procédure civile* » qui concerne donc les infractions monétaires et les actes de terrorisme.

[1347] Loi nº 2001-1 062 du 15 novembre 2001 *relative à la sécurité quotidienne* publiée au JORF nº266 du 16 novembre 2001 p. 18215.
[1348] Loi nº 2002-1 138 du 9 septembre 2002 *d'orientation et de programmation pour la justice* publiée au JORF du 10 septembre 2002 p. 14934.
[1349] Loi nº 2003-239 du 18 mars 2003 *pour la sécurité intérieure* parue au JORF nº66 du 19 mars 2003 p. 4761.
[1350] Loi nº 2004-204 du 9 mars 2004 *portant adaptation de la justice aux évolutions de la criminalité* publiée au JORF nº59 du 10 mars 2004 p. 4567.

Après les attentats de Madrid et de Londres[1351], la lutte législative contre le terrorisme reprend. Le 24 janvier 2006, une nouvelle loi de lutte contre le terrorisme[1352] est promulguée. Les services de police et de gendarmerie peuvent être autorisés à obtenir les images et enregistrements des installations de vidéosurveillance prises sur la voie publique. Le traitement automatisé des données à caractère personnel recueillies à l'occasion de déplacements internationaux hors de l'Union européenne est autorisé. Dans le cadre de la lutte et de la prévention des actes de terrorisme, les forces de police et de gendarmerie ont accès au fichier national des immatriculations, au système national de gestion des permis de conduire, au système de gestion des cartes d'identité, au système de gestion des passeports, au système de gestion des dossiers des ressortissants étrangers en France. Les articles 3, 6 et 9 de cette loi étaient initialement applicables jusqu'au 31 décembre 2008, la loi du 1er décembre 2008[1353] les a prorogés au 31 décembre 2012. L'article 6, prévoyant une réquisition administrative des données techniques de connexion, avait fait l'objet d'un recours auprès du Conseil constitutionnel[1354].

En 2011, une nouvelle loi sécuritaire est promulguée, la loi dite LOPPSI 2[1355]. Cette loi a été fortement critiquée et le Conseil constitutionnel a déclaré non conformes en totalité ou partiellement 13 des 142 dispositions du texte adopté par le Parlement[1356]. Cette loi prévoit dans le cadre de la lutte contre la cybercriminalité l'incrimination pénale d'usurpation d'identité. Le blocage de sites WEB peut être imposé par une autorité administrative. Une liste noire des sites à bloquer est établie par l'administration et les fournisseurs d'accès Internet ou FAI sont tenus de les bloquer. La police sur autorisation du juge peut s'introduire dans des ordinateurs et en extraire des données[1357].

[1351] Attentats de Madrid du 11 mars 2004 (200 morts et 1 400 blessés) et ceux dans le métro de Londres du 7 juillet 2005 (56 morts et 700 blessés) et du 21 juillet (ne faisant aucune victime).

[1352] Loi nº 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* publiée au JORF nº0020 du 24 janvier 2006 p. 1129.

[1353] Loi nº 2008-1 245 du 1er décembre 2008 *visant à prolonger l'application des articles 3, 6 et 9 de la loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* publiée au JORF nº0280 du 2 décembre 2008 p. 18361.

[1354] Conseil constitutionnel, Décision nº 2005-532 DC du 19 janvier 2006 *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*.

[1355] Loi nº 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure publiée* au JORF nº0062 du 15 mars 2011 p. 4582.

[1356] Conseil constitutionnel, Décision nº 2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*.

[1357] Disposition critiquée par la Commission nationale de l'informatique et des libertés dans son avis rendu public (Délibération n°2009-200 du 16 avril 2009 *portant avis sur sept articles du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure*).

Le 12 mars 2012, le code de la sécurité intérieure est créé par ordonnance[1358]. Cette ordonnance a été ratifiée par l'article 24 de la loi nº 2014-1 353 du 13 novembre 2014[1359]. Ce code possède, dans son Livre II « *Ordre et sécurité publics* », un Titre II intitulé « *Lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la Nation* ». Ce code dispose de l'accès de la police et de la gendarmerie nationales à des traitements administratifs automatisés : Le fichier national des immatriculations ; le système national de gestion des permis de conduire ; le système de gestion des cartes nationales d'identité ; le système de gestion des passeports ; le système informatisé de gestion des dossiers des ressortissants étrangers en France ; les données à caractère personnel relatives aux ressortissants étrangers ; ainsi qu'à des données détenues par des opérateurs privés : les données conservées par les opérateurs de communications électroniques[1360] dans les conditions définies à l'article L.34-1-1 du code des postes et communications électroniques[1361] ; les données conservées par les prestataires de services de communication au public en ligne dans les conditions définies à l'article 6 de la loi nº 2004-575 du 21 juin 2004[1362] pour la confiance dans l'économie numérique et des communications

[1358] Ordonnance nº 2012-351 du 12 mars 2012 *relative à la partie législative du code de la sécurité intérieure* publiée au Journal officiel du 13 mars 2012 p. 4533.

[1359] Loi n° 2014-1353 du 13 novembre 2014 *renforçant les dispositions relatives à la lutte contre le terrorisme* publiée au JORF n°0263 du 14 novembre 2014 page 19162.

[1360] Code des postes et communications électroniques, Article L.34-1 « *VI - Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.*

« Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ».

[1361] Code des postes et communications électroniques, Article L.34-1-1 « *Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L.34-1 la communication des données conservées et traitées par ces derniers en application dudit article.*

« Les données pouvant faire l'objet de cette demande sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

« Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes mentionnés au premier alinéa pour répondre à ces demandes font l'objet d'une compensation financière.

« Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'intérieur qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Les demandes, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité ».

[1362] « *Les personnes [dont l'activité est d'offrir un accès à des services de communication au public en ligne et les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages*

électroniques. Pour les besoins de la prévention des actes de terrorisme, les agents des services de renseignement du ministère de la Défense individuellement désignés et dûment habilités sont également autorisés, dans les conditions fixées par la loi nº 78-17 du 6 janvier 1978, à accéder aux mêmes traitements administratifs automatisés.

Entre le 11 mars 2012 et 19 mars 2012, Mohammed Merah tue un militaire à Toulouse, deux militaires à Montauban, et 4 enfants et en blesse un autre devant un collège juif à Toulouse. Il sera identifié grâce aux données techniques laissées sur Internet lors d'une consultation d'une annonce passée par sa première victime pour vendre une motocyclette. La loi nº 2012-1432 du 21 décembre 2012[1363] a été présentée en Conseil des ministres le 3 octobre 2012 par M. Manuel Valls, ministre de l'Intérieur. Cette loi renforce la répression contre le terrorisme. Autorisée temporairement depuis 2005 jusqu'au 31 décembre 2012, la surveillance dans un but préventif des données de connexion (Internet, géolocalisation, factures détaillées du téléphone) est prolongée jusqu'au 31 décembre 2015[1364]. La limitation est supprimée par la loi relative au renseignement[1365]. Elle modifie le Code pénal permettant ainsi de poursuivre les actes de terrorisme commis par des ressortissants français à l'étranger ainsi que les personnes ayant participé à des camps terroristes à l'étranger[1366].

La loi nº 2014-1 353 du 13 novembre 2014[1367] renforce les dispositions relatives à la lutte contre le terrorisme en mettant en place une interdiction administrative de sortie du territoire[1368] avec invalidation possible du passeport et de la carte d'identité de la personne concernée par cette interdiction, ainsi qu'une interdiction administrative d'entrée sur le territoire français à l'encontre de tout ressortissant étranger ne résidant pas habituellement en France lorsque sa présence constituerait « *une menace réelle, actuelle et suffisamment grave pour un intérêt fondamental de la société* »[1369]. Cette interdiction concerne également les ressortissants d'un État membre de l'Union européenne. Une circulaire du garde des Sceaux[1370] présente aux

de toute nature fournis par des destinataires de ces services]détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ».

[1363] Loi nº 2012-1 432 du 21 décembre 2012 *relative à la sécurité et à la lutte contre le terrorisme* publiée au Journal officiel du 22 décembre 2012 p. 20281.

[1364] Ibid. Article 1er.

[1365] Loi n° 2015-912 du 24 juillet 2015 *relative au renseignement.*

[1366] Ajout des articles 113-13 et 421-1-2-3 du Code pénal.

[1367] Loi nº 2014-1 353 du 13 novembre 2014 *renforçant les dispositions relatives à la lutte contre le terrorisme* publiée au Journal officiel du 14 novembre 2014 p. 19162.

[1368] Chapitre 1er : Création d'un dispositif de sortie du territoire.

[1369] Chapitre II : Création d'un dispositif d'interdiction administrative du territoire.

[1370] Circulaire du 5 décembre 2014 *de présentation de la loi nº 2014-1 353 renforçant les dispositions relatives à la lutte contre le terrorisme — Renforcement de la coordination de la lutte antiterroriste* NOR : JUSD1429083C.

procureurs les dispositions de cette loi : dispositions administratives, dispositions de droit pénal et de procédure pénale, ainsi qu'un renforcement de la coordination de la lutte antiterroriste au niveau national. Le décret relatif à l'interdiction de sortie du territoire est publié le 15 janvier 2015[1371].

La loi nº 2014-1 353 pénalise également l'entreprise individuelle à caractère terroriste. Elle renforce la répression de l'apologie du terrorisme et permet le blocage administratif de sites Internet faisant l'apologie du terrorisme ou y provoquant. Le décret d'application de ce déréférencement de sites est publié le 4 mars 2015[1372] et, en application de cette possibilité, le ministère de l'Intérieur a demandé le 16 mars 2015 aux fournisseurs d'accès Internet de bloquer l'accès à cinq sites faisant l'apologie du terrorisme ou diffusant la propagande du groupe État islamique[1373]. Cette possibilité de blocage de sites Internet, prévue dans la loi LOPPSI 2, n'avait pas encore été utilisée concrètement par l'administration.

Suite aux attentats de janvier 2015 à Paris[1374], sur le site du gouvernement français, la lutte contre le terrorisme[1375] est matérialisée par un nouveau projet de loi sur le renseignement pour « *Protéger les Français dans le respect des libertés* »[1376]. Le projet de loi relatif au renseignement a été déposé et enregistré par la présidence de l'Assemblée nationale le 19 mars 2015 en procédure accélérée. Son article 1er prévoit la création d'un livre VIII intitulé « *Du renseignement* » dans le code de la sécurité intérieure. Le Conseil d'État est reconnu compétent

---

[1371] Décret nº 2015-26 du 14 janvier 2015 *relatif à l'interdiction de sortie du territoire des ressortissants français projetant de participer à des activités terroristes à l'étrange*r publié au Journal officiel du 15 janvier 2015 p. 629.

[1372] Décret nº 2015-253 du 4 mars *2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* NOR : INTD1504662D publié au Journal officiel du 5 mars 2015 p. 4168.

[1373] Il s'agit des sites jihadmin.com, mujahida89.wordpress.com, islamic-news.info, is0lamnation.blogspot.fr, alhayatmedia.wordpress.com.

[1374] 7 janvier 2015, 12 personnes sont tuées dans l'attaque islamiste contre "Charlie Hebdo". 8 janvier 2015, un terroriste abat une policière, à Montrouge. 9 janvier 2015, ce même terroriste tue 4 otages dans un magasin juif de la porte de Vincennes.

[1375] http://www.gouvernement.fr/action/la-lutte-contre-le-terrorisme consulté le 25 mars 2015.

[1376] « *La France est l'une des dernières démocraties occidentales à ne pas disposer d'un cadre légal, cohérent et complet pour les activités de ses services de renseignement. En juillet 2014, le Président de la République et le Gouvernement ont décidé de répondre à cette lacune par une loi spécifique. Les attentats perpétrés en France en janvier 2015 et l'intensité de la menace terroriste ont souligné l'importance et l'urgence de cette réponse.*
« Le projet de loi sur le renseignement, présenté en Conseil des ministres du 19 mars a pour objectif de combler cette lacune, en donnant aux services de renseignement des moyens à la hauteur de la menace à laquelle ils sont confrontés tout en garantissant la protection des libertés publiques.
« Le projet de loi sur le renseignement se fixe deux objectifs : donner un cadre légal précis aux services de renseignement pour les autoriser à recourir à des moyens techniques d'accès à l'information ; garantir le respect des libertés publiques et le respect de la vie privée. Sur ce deuxième point, il prévoit notamment de subordonner le recours aux mesures de surveillance à l'autorité du pouvoir politique et à un double contrôle, celui d'une autorité extérieure indépendante, et celui du Conseil d'État ».

pour connaître des requêtes concernant la mise en œuvre des techniques de renseignement et de leur contentieux.

Alors que ce projet de loi est en première lecture à l'Assemblée nationale, le Président de la République annonce le 19 avril 2015 dans une émission de radio qu'il déférera la loi avant sa promulgation au Conseil constitutionnel, comme le lui permet la Constitution. Le Conseil constitutionnel, dans ce cas de saisine, devrait analyser le texte voté par le Parlement et soulever d'office les incompatibilités avec la Constitution, en analysant la loi article par article, bloquant ainsi toute QPC ultérieure par l'autorité de la chose jugée, ce qui n'est pas vérifié, au moins une QPC a été transmise au Conseil constitutionnel qui a déclaré non-conforme à la Constitution l'article L.811-5 du code de la sécurité intérieure tel qu'issu de la loi n°2015-912[1377].

La loi n° 2015-912[1378] relative au renseignement est promulguée après que le Conseil constitutionnel[1379] n'ait déclaré non conformes à la Constitution que trois articles. Cette loi est fortement contestée, car jugée liberticide. Elle ajoute un nouveau livre au code de la sécurité intérieure : le livre VIII intitulé « Du renseignement ». Le premier article de ce livre commence par : « *Art. L.801-1. - Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité.* » reprenant ainsi la jurisprudence constante du Conseil constitutionnel.

Dans le rapport de la Commission des lois de l'Assemblée nationale présenté lors de la discussion du projet de loi[1380], il est relevé que : « *Les services de renseignement disposent aujourd'hui de moyens juridiques morcelés, issus d'une lente sédimentation de dispositions législatives, sans cadre général* », sédimentation provenant de plusieurs lois[1381]. L'objectif de

[1377] Conseil constitutionnel, Décision n° 2016-590 QPC du 21 octobre 2016 *La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne]*.

[1378] Loi n° 2015-912 du 24 juillet 2015 *relative au renseignement* publiée au JORF n°0171 du 26 juillet 2015 p. 12735.

[1379] Conseil Constitutionnel, Décision n° 2015-713 DC du 23 juillet 2015 *Loi relative au renseignement*.

[1380] Jean-Jacques Urvoas, Rapport n° 2697 *fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la république, après engagement de la procédure accélérée, sur le projet de loi (n° 2669) relatif au renseignement*, enregistré à la Présidence de l'Assemblée nationale le 2 avril 2015, disponible en ligne à http://www.assemblee-nationale.fr/14/rapports/r2697.asp, consulté le 17 juillet 2017.

[1381] La loi du 10 juillet 1991 *régissant le cadre juridique des interceptions de sécurité*, la loi du 23 janvier 2006 *autorisant l'accès aux données de connexion, pour la prévention du terrorisme* et la loi du 18 décembre 2013 *unifiant les régimes d'accès aux données de connexion et la géolocalisation en temps réel.*

est de poursuivre l'amélioration du dispositif juridique d'encadrement et de contrôle des services de renseignement, encadrement réalisé dans plusieurs États européens.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) remplace la Commission nationale de contrôle des interceptions de sécurité (CNCIS) instituée par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications à la suite de l'affaire des écoutes de l'Élysée[1382]. Alors que la CNCIS était composée d'un président, nommé par le Président de la République dans une liste de quatre personnalités présentées par le Président du Conseil d'État et par le Président de la Cour de cassation, ainsi que d'un député et un sénateur, la nouvelle commission est composée de deux députés, deux sénateurs, deux membres du Conseil d'État, deux membres de la Cour de cassation et d'une personnalité nommée par le Président de la République. Son président nommé par le Président de la République est choisi parmi les membres de la commission issus du Conseil d'État ou de la Cour de cassation. En formation restreinte, la commission ne comprend ni député ni sénateur. Ainsi, la commission peut émettre des avis sans représentation des élus parlementaires.

De plus, en cas de recours concernant les interceptions et écoutes, alors qu'en cas d'enquête judiciaire l'autorité judiciaire est compétente, en cas d'écoute ou d'interception administrative entrant dans le cadre de la loi relative au renseignement, le Conseil d'État est compétent, il peut être saisi par la nouvelle commission en cas de litiges ou par tout individu y ayant intérêt.

Cette loi modifie le Code de la sécurité intérieure existant en matière de techniques de recueil de renseignements, de localisation, des interceptions de correspondances émises par la voie des communications électroniques, de la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques. La surveillance internationale initialement prévue dans la loi, mais déclarée non conforme à la Constitution par le Conseil constitutionnel a été établie par la loi du 30 novembre 2015[1383]. Elle autorise la surveillance des communications qui sont émises ou reçues à l'étranger et porte sur des correspondances ou sur des données de connexion.

[1382] « L'affaire des écoutes de l'Élysée définitivement close », 30 septembre 2008, Le Point, URL : http://www.lepoint.fr/actualites-societe/2008-09-30/l-affaire-des-ecoutes-de-l-elysee-definitivement-close/920/0/278356 consulté le 10 avril 2018.

[1383] Loi nº 2015-1 556 du 30 novembre *2015 relative aux mesures de surveillance des communications électroniques internationales*, publiée au JORF nº0278 du 1 décembre 2015 p. 22185.

Le 13 novembre 2015, la France subit plusieurs attaques terroristes coordonnées sur Paris[1384]. L'état d'urgence[1385] est décrété sur l'ensemble du territoire métropolitain pour une entrée en vigueur le 14 novembre 2015, sa demande d'extension à une durée de trois mois est annoncée par le Président de la République devant les parlementaires réunis en congrès à Versailles le 16 novembre 2015, il sera régulièrement prolongé jusqu'en novembre 2017. L'état d'urgence permet de restreindre la circulation des personnes, limiter les rassemblements et permet d'effectuer des perquisitions administratives c'est-à-dire sans l'autorisation préalable d'un magistrat. Durant son allocution, le Président de la République annonce qu'il demandera une évolution du cadre législatif afin de prendre en compte l'évolution de la technique depuis l'année 1955, date de la promulgation de la loi n° 55-285. Effectivement, la loi du 20 novembre 2015[1386], par son article 4, modifie cette loi de 1955.

Ainsi le ministre de l'Intérieur peut assigner à résidence toute personne physique « *à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace pour la sécurité et l'ordre publics* », et « *lorsque la personne assignée à résidence a été condamnée à une peine privative de liberté pour un crime qualifié d'acte de terrorisme ou pour un délit recevant la même qualification puni de dix ans d'emprisonnement et a fini l'exécution de sa peine depuis moins de huit ans, le ministre de l'Intérieur peut également ordonner qu'elle soit placée sous surveillance électronique mobile* ».

Les autorités administratives peuvent « *ordonner des perquisitions en tout lieu, y compris un domicile, de jour et de nuit, sauf dans un lieu affecté à l'exercice d'un mandat parlementaire ou à l'activité professionnelle des avocats, des magistrats ou des journalistes, lorsqu'il existe des raisons sérieuses de penser que ce lieu est fréquenté par une personne dont le comportement constitue une menace pour la sécurité et l'ordre publics* ». Le procureur de la République territorialement compétent doit être informé de cette décision de perquisition et la perquisition conduite en présence d'un officier de police judiciaire territorialement compétent, en présence de l'occupant ou, à défaut, de son représentant ou de deux témoins.

[1384] Attentats auprès du stade de France, aux terrasses de bars et restaurants du X^e^ et XI^e^ arrondissements, dans la salle du Bataclan, faisant 129 morts et 352 blessés.

[1385] Décret n° 2015-1 475 du 14 novembre 2015 *portant application de la loi n° 55-385 du 3 avril 1955* paru au JORF n°0264 du 14 novembre 2015 p. 21297.

[1386] Loi n° 2015-1 501 du 20 novembre 2015 *prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions*, publiée au JORF n° 270 du 21 novembre 2015 p. 21665.

« *Il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Les données auxquelles il aura été possible d'accéder dans les conditions prévues au présent article peuvent être copiées sur tout support* ». Ainsi, non seulement les données présentes sur un ordinateur présent dans les locaux perquisitionnés peuvent être accédées et copiées sur un support idoine, mais il en est de même des données non disponibles localement, mais disponibles sur un réseau de télécommunications et accessibles depuis ce terminal, ces données peuvent être sur un site dont l'adresse est présente dans l'historique de navigation de l'ordinateur ou dans le cloud référencé par l'ordinateur. Aucune information concernant l'éventuel cryptage de ces données n'est présente dans la loi.

Lors de la prorogation de juillet 2016[1387], la perquisition peut être étendue à tout local répondant aux conditions ayant provoqué la décision de perquisition initiale, étendant ainsi par contagion le périmètre de la perquisition. « *Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les données contenues dans tout système informatique ou équipement terminal présent sur les lieux de la perquisition peuvent être saisies soit par leur copie, soit par la saisie de leur support* »[1388]. L'autorisation d'exploitation des données saisies est demandée au juge des référés. Elles sont conservées durant le temps nécessaire à leur exploitation, mais « *en cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus […] peuvent être prorogés, pour la même durée, par le juge des référés* »[1389]. Cette prolongation permet, sans l'écrire explicitement, de décrypter des données cryptées. Les personnes présentes sur le lieu de perquisition peuvent être retenues pendant un délai de quatre heures si « *leur comportement constitue une menace pour la sécurité et l'ordre publics* ».

Cette loi de prorogation autorise le traitement de données de vidéosurveillance dans les établissements pénitentiaires. La Garde des Sceaux peut décider de la mise sous vidéosurveillance de détenus pour actes terroristes pour une durée de trois mois renouvelables.

[1387] Loi n° 2016-987 du 21 juillet 2016 *prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste*, publiée au JORF n°0169 du 22 juillet 2016.
[1388] Loi n° 2016-987 du 21 juillet 2016, art. 5.
[1389] Ibid.

Pour les besoins de lutte contre le terrorisme, des données concernant les personnes suspectées de préparer des actes de terrorisme peuvent être collectées auprès des opérateurs. Cette collecte peut être étendue aux personnes de son voisinage susceptibles de fournir des informations. Ainsi, après la contagion de la perquisition à des locaux, la collecte de données peut être également étendue par contagion à l'entourage des personnes surveillées, mais cette disposition de la loi du 21 juillet 2016 a été déclarée non conforme à la Constitution par le Conseil constitutionnel pour atteinte excessive au droit de la vie privée[1390].

L'état d'urgence est prorogé jusqu'au 1er novembre 2017[1391], à cette date, les mesures d'exception ont été incorporées à la législation pénale. Le Sénat a commencé l'examen de ce projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme le 17 juillet 2017 en procédure accélérée. Dans l'étude d'impact de ce projet de loi, il est écrit : « *Si le péril imminent prend un caractère durable, en particulier avec le développement de nouvelles formes de terrorisme, il devient nécessaire, pour tenir compte de cette appréciation de la menace, de doter l'État de nouveaux instruments permanents de prévention et de lutte contre le terrorisme, en réservant les outils de l'état d'urgence à une situation exceptionnelle* ».

La loi n° 2017-1510 est publiée au Journal officiel le 31 octobre 2017[1392]. Outre des dispositions permettant de recourir à des organismes de police privée pour sécuriser certains établissements ou zones définies par arrêté préfectoral[1393], et la possibilité de fermer des lieux de culte dans un but de prévention des actes de terrorisme[1394], le projet prévoit des mesures touchant les libertés individuelles des personnes physiques, en particulier la liberté d'aller et venir, et favorisant leur surveillance[1395]. La perquisition de locaux et l'enregistrement de données sont conservés, mais nécessitent la demande de l'autorisation de réaliser une visite ou une saisie au juge des libertés et de la détention ainsi que de placer les opérations sous son autorité et son contrôle, y compris l'autorisation d'exploitation des données saisies[1396]. Ces mesures peuvent être demandées suite à l'interception de conversations privées manifestant le soutien ou l'adhésion à des actes de terrorisme. De plus, cette loi est utilisée pour transcrire la directive PNR en droit français tant

[1390] Conseil constitutionnel, Décision nº 2017-648 QPC du 4 août 2017 *La Quadrature du Net et autres [Accès administratif en temps réel aux données de connexion]*.
[1391] Loi nº 2017-1 154 du 11 juillet 2017 *prorogeant l'application de la loi nº 55-385 du 3 avril 1955 relative à l'état d'urgence*, publiée au JORF nº0162 du 12 juillet 2017.
[1392] Loi n° 2017-1510 du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme* publiée au JORF n°0255 du 31 octobre 2017.
[1393] Loi n° 2017-1510 du 30 octobre 2017, Art. 1.
[1394] Ibid. Art. 2.
[1395] Ibid. Art. 3.
[1396] Ibid. Art. 4.

pour les données de réservation ou PNR, que pour les données d'information des passagers ou API[1397] lues lors de l'enregistrement à partir des passeports ou documents d'identité[1398]. Elle prévoit la création d'un traitement automatique des données à caractère personnel relatives au transport maritime des passagers, tant pour les croisières que pour les transports transmanche[1399]. Elle redéfinit l'interception des communications par voie hertzienne[1400], interception déjà prévue, mais déclarée non conforme à la Constitution par le Conseil constitutionnel[1401]. Mais cette interception restait possible jusqu'en fin 2017 pour permettre au gouvernement de préparer une nouvelle loi tenant compte des restrictions émises.

Cette loi qui transpose dans la législation ordinaire des dispositions de l'état d'urgence afin de lutter en permanence contre le terrorisme, encadre la liberté d'aller et venir, et pérennise les techniques de renseignement des individus, l'interception des communications par voies hertziennes et par le réseau Internet, la captation de données à caractères personnelles, mais dans les faits instaure une véritable surveillance de masse afin de détecter les risques de terrorisme. Ainsi pour lutter contre le terrorisme, les libertés individuelles se trouvent restreintes, ces restrictions étant jugées compatibles avec la Constitution par le Conseil constitutionnel.

c) La jurisprudence du Conseil constitutionnel dans la lutte contre le terrorisme.

La quasi-totalité des lois adoptées pour lutter contre le terrorisme attente aux libertés individuelles et en conséquence a été soumise au Conseil constitutionnel[1402] avant leur promulgation pour en vérifier la conformité avec la Constitution en faisant application de sa jurisprudence classique[1403]. Le Conseil constitutionnel a ainsi vu son rôle de protecteur des

[1397] En anglais *Advanced Passenger Information* ou API.
[1398] Loi n° 2017-1510 du 30 octobre 2017, Art. 13.
[1399] Ibid. Art.14.
[1400] Ibid. Art. 15.
[1401] Conseil constitutionnel, Décision nº 2016-590 QPC du 21 octobre 2016 *La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne]*.
[1402] Seule la loi du 15 novembre 2001, *relative à la sécurité quotidienne*, n'a pas été déférée au Conseil constitutionnel.
[1403] Pierre Mazeaud, *La lutte contre le terrorisme dans la jurisprudence du Conseil constitutionnel*, Visite à la cour suprême du Canada, 24 au 26 avril 2006.

droits fondamentaux confirmé au travers d'un contrôle de proportionnalité entre les atteintes aux libertés et l'intérêt général[1404].

Mais alors que la Constitution donne au juge judiciaire le rôle de protection des libertés individuelles et de la propriété privée[1405], et que l'article 136 du Code de procédure pénale prévoit que, dans les cas d'atteinte à la liberté individuelle, le juge judiciaire est exclusivement compétent, cette compétence n'est pas générale et absolue. En France, la protection des libertés fondamentales est d'origine prétorienne et le juge administratif en a été le premier garant en protégeant l'individu contre l'arbitraire de l'administration dès 1873[1406]. Ce n'est qu'en 1971, que le Conseil constitutionnel a donné à cette protection un statut constitutionnel[1407] en incluant le préambule de ladite Constitution, la Déclaration des droits de l'homme et du citoyen de 1789 et le préambule de la Constitution de 1946, dans le droit positif.

Dans la prolongation de sa jurisprudence antérieure, le Conseil constitutionnel n'a exclu que peu d'articles de la loi relative au renseignement pour atteinte disproportionnée aux libertés fondamentales, alors que de nombreuses critiques sont formulées et qu'un recours devant la Cour de justice de l'Union européenne a été initié par des avocats. Cette attitude du Conseil a perduré lors de son examen des lois de lutte contre le terrorisme par le moyen des Questions prioritaires de constitutionnalité, mais il n'a pas été saisi des lois de prorogation de l'état d'urgence malgré les atteintes aux libertés des individus dans les lois qui outre la prorogation ajoutaient de nouveaux dispositifs de surveillance. Cette attitude du Conseil constitutionnel semble marquer un certain abandon de la protection des libertés au détriment de la sécurité[1408].

2) L'efficacité de cet arsenal

L'arsenal législatif est préventif et répressif, mais est-il efficace ? Lors de la préparation de la loi nº 2014-1 353 du 13 novembre 2014, le rapport de la commission des lois de l'Assemblée

[1404] Valérie Goesel-Le Bihan, « Le contrôle de proportionnalité dans la jurisprudence du Conseil constitutionnel : figures récentes », *Revue française de droit constitutionnel*, 2007/2 (n° 70), pp. 269-295. URL : https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2007-2-page-269.htm consulté le 15 février 2018.
[1405] Constitution Article 66 « *Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi* ».
[1406] Tribunal des conflits, 8 février 1873, Blanco.
Conseil d'État, 19 février 1875, Prince Napoléon.
[1407] Conseil constitutionnel, Décision nº 71-44 DC du 16 juillet 1971, *Loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association.*
[1408] Armand Gilles, « Que reste-t-il de la protection constitutionnelle de la liberté individuelle ? », *Revue française de droit constitutionnel*, 2006/1 (nº 65), pp. 37-72. à http://www.cairn.info/revue-francaise-de-droit-constitutionnel-2006-1-page-37.htm, consulté le 5 septembre 2017.

nationale[1409] précisait que « *plusieurs projets d'attentats émanant de djihadistes revenus de Syrie sur notre territoire ont été empêchés ces derniers mois grâce à l'intervention [des services de police et de gendarmerie nationales et des services de renseignements]* ». Cette surveillance des individus a montré ses limites avec les assassinats perpétrés par Mohammed Merah en mars 2012 à Toulouse et Montauban, et surtout avec les actions terroristes de janvier 2015 à Paris des frères Kouachi et de Coulabaly, tous les trois ayant été l'objet de surveillance par les services de renseignements. La presse fait état de « fichés S » lors d'attentats. Les suspects ont réussi, après avoir attiré l'attention sur une radicalisation, à sortir d'une surveillance étroite en adoptant une attitude neutre et non provocatrice[1410]. De plus les attentats de décembre 2015, préparés à partir de la Belgique n'ont pas été anticipés.

Dans le dossier de presse de présentation de la loi sur le renseignement, le gouvernement précise[1411] : « *Avant les drames de janvier [les 7, 8 et 9 janvier 2015], 5 projets d'actions terroristes sur le territoire national avaient été déjoués par la DGSI depuis août 2013, impliquant des individus de retour en France ou qui n'avaient pas quitté le territoire national. En tout, ce sont près de 3 000 personnes qu'il convient de surveiller* ».

a) Le livre blanc de la lutte contre le terrorisme

Résultat de travaux lancés en mai 2005, le livre blanc de la lutte contre le terrorisme[1412] montre que la France a pris en compte le danger terroriste, phénomène mondial, et a élaboré des pistes de riposte pour y faire face. Le danger terroriste y est clairement défini comme d'origine djihadiste. Le terrorisme islamiste puise son inspiration idéologique dans le salafisme[1413] fondé sur le rejet des innovations sociales ou politiques, ce courant de pensée est hostile par nature au système démocratique. Sa référence est le souvenir, en partie fantasmé, d'un « âge d'or » de l'islam originel. Il rejette le monde tel qu'il est devenu. Il se présente comme une alternative à

[1409] Assemblée nationale, *rapport n°2173*, enregistré le 22 juillet 2014 à la Présidence de l'Assemblée nationale.
[1410] Willy Le Devin, « Attentat de Trèbes: deux convocations et des questions », 27 mars 2018, *Libération,* URL : http://www.liberation.fr/france/2018/03/27/attentat-de-trebes-deux-convocations-et-des-questions_1639256 consulté le 11 avril 2018.
[1411] http://www.gouvernement.fr/action/la-lutte-contre-le-terrorisme consulté le 28 mars 2015.
[1412] *La France face au terrorisme, Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006.
[1413] De *Salafs*, les Anciens, qui désignent les premiers compagnons du prophète Mahomet.

la mondialisation. Il propose le retour aux pratiques du califat initial[1414] fondées sur une interprétation rigoriste du Coran.

Le livre blanc insiste sur la nécessité d'adaptation permanente des moyens de prévention et de lutte contre le terrorisme. La nécessité d'une coordination internationale de la lutte contre le terrorisme y est rappelée.

En annexe, le livre blanc liste vingt-sept actions attribuées au terrorisme dans le monde entre 1992 et 2005. En complément, il cite vingt-quatre menaces répertoriées comme visant la France entre 1998 et mars 2006. Ces menaces sont soit des déclarations menaçant la France ou les intérêts français dans le monde, soit des arrestations de terroristes ou des démantèlements de réseaux terroristes préparant des actions sur le territoire de la France.

b) Le rapport parlementaire sur l'efficacité de la loi de 2006

Début 208, un rapport d'information fait un bilan de la mise en application de la loi du 23 janvier 2006[1415]. Ce rapport a été décidé par la commission des lois de l'Assemblée nationale faute d'avoir obtenu du gouvernement les évaluations annuelles sur l'application de la loi. Si la plupart des décrets ou arrêtés ministériels nécessaires à l'application de la loi ont été publiés, le rapport constate que si le décret en Conseil d'État[1416] concernant la procédure de réquisition administrative des données conservées par les opérateurs de télécommunication a été publié, certaines modalités restent en attente de publication d'arrêtés ministériels, de plus le décret définissant les modalités d'application de la procédure de réquisition administrative des données conservées par les hébergeurs de site Internet est toujours en attente après l'avis de la Commission de l'informatique et des libertés du 20 décembre 2007, suite aux exigences de facturation et de délai exigées par les opérateurs téléphoniques dans le cadre de la loi du 21 juin 2004 relative à l'économie numérique.

Le rapport constate que sauf quelques points mineurs n'entravant pas l'application de la loi, la loi du 23 janvier 2006 est appliquée et applicable. Ce rapport ne précise pas si cette loi est

[1414] Le mot désigne à la fois l'autorité du calife successeur du prophète Mahomet sur l'ensemble de la communauté musulmane et les territoires placés sous son contrôle.

[1415] Éric Diard, Julien Dray, *Rapport d'information sur la mise en application de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* enregistré le 5 février 2008 à la Présidence de l'Assemblée nationale.

[1416] Décret n°2006-1651 du 26 décembre 2006, après avis de la CNIL du 28 septembre 2006 et du CNCIS du 12 juillet 2006.

réellement efficace, mais les rapporteurs demandent à ce que les dispositions temporaires soient prorogées jusqu'en fin 2012.

L'introduction du rapport conclut : « *Dans le domaine de la lutte contre le terrorisme, évaluer l'efficacité des moyens de prévention et de répression est une entreprise très difficile. En effet, la circonstance que la France n'a pas subi d'acte terroriste d'origine étrangère sur son sol depuis 1996 ne doit pas être perçue comme le signe que notre pays serait à l'abri d'une nouvelle vague d'attentats majeurs. La France reste en effet une cible de choix du terrorisme islamiste. C'est pourquoi le dispositif de lutte antiterroriste doit se remettre en cause en permanence afin d'essayer d'avoir toujours un temps d'avance sur les terroristes* ». Les attentats de 2012 et 2015 confirment cette conclusion et le besoin permanent d'adaptation dans la lutte contre le terrorisme.

B) La lutte contre le terrorisme au niveau international

La lutte contre le terrorisme est une nécessité mondiale. Les pays démocratiques ont dû adapter leur législation pour faire face à cette menace. Cette adaptation s'est parfois faite en renonçant aux protections légalement existantes concernant les libertés et droits des individus, comme aux États-Unis d'Amérique avec le USA Patriot Act[1417]. En Europe également, des législations spécifiques de lutte contre le terrorisme sont apparues, souvent en réaction à des attentats.

1) Les législations en Europe

En Europe, la lutte contre le terrorisme a également fait l'objet de législations spéciales. Avec les soulèvements pour l'indépendance de l'Irlande, l'Angleterre a édicté des lois d'exception pour lutter contre les terroristes irlandais, avant d'avoir à faire face aux attentats islamiques du métro de Londres. L'Italie et l'Allemagne ont subi le terrorisme d'extrême gauche avant de connaître des attentats antisionistes (jeux olympiques de Munich).

[1417] Jean-Claude Monod, « Vers un droit international d'exception ? », *Esprit*, 2006/8 (Août/septembre), pp. 173-193. URL : https://www.cairn.info/revue-esprit-2006-8-page-173.htm consulté le 8 janvier 2018.

En Grande-Bretagne, le *Prevention of terrorism Act*[1418] a remplacé depuis 2005 le *Antiterrorism, Crime and Security Act* 2001[1419]. Le ministre de l'Intérieur[1420] peut imposer des « ordonnances de contrôle »[1421] sur les personnes suspectées de terrorisme, qu'elles soient britanniques ou non. Ces ordonnances autorisent des restrictions sur les libertés de mouvement et d'expression, la possession d'objets, l'accès à Internet. Elle a été complétée : par la répression de la préparation à un acte de terrorisme, de l'entraînement au terrorisme et de l'encouragement au terrorisme ; par l'instauration d'une garde à vue de 28 jours pour prévenir un acte de terrorisme ; par l'instauration d'un registre de surveillance pour le terrorisme ; par le prélèvement d'empreintes digitales et d'ADN. Le gouvernement peut agir sans passer par le parlement en cas de proclamation de l'état d'urgence.

En matière de renseignement, la Grande-Bretagne dispose du British Security Service (« *military intelligence* » section 5 communément appelé MI-5) pour le renseignement intérieur, le Secret intelligence service ou SIS compétent à l'extérieur du territoire, et du *Governement communication headquarter* ou GCHQ, chargé de la collecte des renseignements techniques. Le GCHQ constitue le plus grand service d'interception des communications occidental après la NSA américaine, avec laquelle il entretient des relations étroites. Le MI5 collabore étroitement avec le GCHQ. Le British Security Service (MI-5) n'a pas de compétence judiciaire, et ne peut accomplir, à la différence de la DGSI, aucun acte judiciaire (perquisitions...).

Le système britannique repose sur une forte responsabilité de l'exécutif, en l'occurrence les ministres de tutelle, qui sont seuls responsables de la délivrance des autorisations d'opérations (« warrant ») aux services. La législation (*Intelligence Service act* 1994, *British security service act* et RIPA 2000) ne réglemente pas en tant que tel l'usage de telle ou telle technique, mais raisonne davantage par rapport à la nature de l'atteinte à la vie privée qu'elle représente (ex : accès au domicile, filature, interceptions des communications). Un warrant peut ainsi intervenir

[1418] Prevention of Terrorism Act 2005, An Act *to provide for the making against individuals involved in terrorism-related activity of orders imposing obligations on them for purposes connected with preventing or restricting their further involvement in such activity; to make provision about appeals and other proceedings relating to such orders; and for connected purposes.* [11th March 2005].

[1419] Anti-terrorism, Crime and Security Act 2001, *An Act to amend the Terrorism Act 2000; to make further provision about terrorism and security; to provide for the freezing of assets; to make provision about immigration and asylum; to amend or extend the criminal law and powers for preventing crime and enforcing that law; to make provision about the control of pathogens and toxins; to provide for the retention of communications data; to provide for implementation of Title VI of the Treaty on European Union; and for connected purposes*. [14th December 2001]

[1420] *The Secretary of State*.

[1421] *Control orders*.

dans n'importe quel domaine de la vie privée. Cette approche a permis à la législation anglaise de s'adapter aux évolutions technologiques, sans qu'il soit nécessaire de mettre à jour les textes trop fréquemment[1422].

En Allemagne, la loi de lutte contre le terrorisme de 2002 permet aux services de renseignement de demander des informations aux banques, aux entreprises de télécommunications, aux compagnies aériennes et à l'Office fédéral pour la migration des réfugiés.

La justice allemande peut poursuivre les membres d'organisations terroristes même si aucun délit n'a été commis sur le territoire de l'Allemagne. Les étrangers peuvent être expulsés s'ils ont commis des crimes graves dans ou à l'extérieur de l'Allemagne. Le dispositif a été complété en 2007 par la possibilité de localisation des téléphones portables, de brouillage du réseau téléphonique ou d'écoutes téléphoniques[1423]. En 2017, l'Allemagne a modifié la gestion des données personnelles pour mieux lutter contre le terrorisme[1424].

En Belgique, la loi sur le parquet fédéral de 2002 instaure une justice antiterroriste. Le *Belgium antiterrorism Act* de 2003 reconnaît comme infraction terroriste le fait de participer aux activités d'une organisation terroriste. Après l'attentat du Musée juif de Bruxelles en mai 2004, les policiers peuvent créer de faux profils pour infiltrer les réseaux djihadistes sur Internet. Le renseignement est basé sur la dualité de la Sûreté de l'État (SE) qui est un service de renseignement civil placé à titre principal sous l'autorité du ministre de la Justice, en charge de la sécurité intérieure et extérieure de l'État, et du Service général du renseignement et de la sécurité (SGRS) qui est le service de renseignement militaire placé sous l'autorité du ministre de la Défense nationale et dont la mission est de rechercher, analyser et gérer des informations sur des activités menaçant ou susceptibles de menacer l'intégrité du territoire national[1425].

Mais, ce sont les États-Unis d'Amérique qui ont promulgué la législation de lutte contre le terrorisme la plus liberticide, utilisant les techniques numériques pour intercepter les communications internationales de toute nature.

[1422] Extrait de *Projet de loi relatif au renseignement* – Étude d'impact, Assemblée nationale, 18 mars 2015.

[1423] Delphine Nerbollier, « L'Allemagne face au défi de la lutte contre le terrorisme », 10 octobre 2016, *La Croix,* URL : https://www.la-croix.com/Monde/Europe/LAllemagne-face-defi-lutte-contre-terrorisme-2016-10-10-1200795198, consulté le 8 janvier 2018.

[1424] Elisa Braun, « Contre le terrorisme, l'Allemagne bascule dans le fichage de ses citoyens », 27 avril 2017, *Le Figaro.fr tech & web,* URL : http://www.lefigaro.fr/secteur/high-tech/2017/04/27/32001-20170427ARTFIG00221-contre-le-terrorisme-l-allemagne-bascule-dans-le-fichage-de-ses-citoyens.php consulté le 8 janvier 2018.

[1425] Sébastien Boussois, « Lutte contre le terrorisme : la Belgique, maillon faible ? », *Politique étrangère*, 2017/4 (Hiver), pp. 173-185. URL : https://www.cairn.info/revue-politique-etrangere-2017-4-page-173.htm consulté le 8 janvier 2018.

2) Les États-Unis d'Amérique et le USA PATRIOT Act

La fin du XX[e] siècle a été marquée par des attentats sur le territoire des États-Unis d'Amérique : Oklahoma City, jeux Olympiques d'Atlanta, attaque au camion piégé contre le World Trade Center en 1993. Au niveau international, des attentats ont également eu lieu contre la base américaine de Dhahran en Arabie saoudite en 1996, contre les ambassades américaines au Kenya et en Tanzanie en 1998 et contre la frégate USS Cole au Yémen en 2000[1426].

Les attentats du 11 septembre 2001 ont marqué un changement de stratégie des États-Unis d'Amérique dans leur vision du terrorisme, ils ne le considèrent plus comme une menace contre leurs intérêts dans le monde, mais comme un danger intérieur et soumettent donc la politique nationale à cette exigence. L'administration de George W. Bush va promulguer une législation d'exception et modifier sa politique extérieure en attaquant directement des pays considérés comme soutien du terrorisme mondial : l'Irak, l'Afghanistan, et en tentant d'isoler l'Iran et la Corée du Nord[1427].

Le USA Patriot Act[1428] est une loi antiterroriste[1429] votée par le Congrès des États-Unis et signée par George W. Bush le 28 octobre 2001, soit un mois et demi après les attentats du 11 septembre.

L'un des objectifs de cette loi est d'effacer la distinction juridique entre les enquêtes effectuées par les services de renseignement extérieur (CIA, NSA) et les agences fédérales responsables des enquêtes criminelles (FBI) dès lors qu'elles impliquent des terroristes étrangers. Cette loi crée les statuts de combattant ennemi et de combattant illégal qui permettent au gouvernement des États-Unis de détenir sans limites et sans inculpation toute personne soupçonnée de projet terroriste, l'incarcération sans procès de détenus dans la base de Guantanamo est l'application directe de cette disposition. Dans la pratique cette loi autorise les services de sécurité à accéder aux données informatiques détenues par les particuliers et les entreprises, sans autorisation préalable et sans en informer les utilisateurs, en ayant supprimé les restrictions liées aux écoutes

---

[1426] Pierre Mélandri, « « Le terrorisme, voilà l'ennemi ». Les attentats et la politique étrangère des États-Unis », *Vingtième Siècle. Revue d'histoire*, 2002/4 (n° 76), pp. 45-63. URL : https://www.cairn.info/revue-vingtieme-siecle-revue-d-histoire-2002-4-page-45.htm consulté le 11 avril 2018.

[1427] « La politique étrangère américaine », *Revue internationale et stratégique*, 2004/2 (n° 54), pp. 177-194. URL : https://www.cairn.info/revue-internationale-et-strategique-2004-2-page-177.htm consulté le 8 janvier 2017.

[1428] Acronyme de "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (qui pourrait se traduire en français par « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme »).

[1429] Jean-Claude Paye, « L'état d'exception : forme de gouvernement de l'Empire ? », *Multitudes*, 2004/2 (n° 16), pp. 179-190. URL : https://www.cairn.info/revue-multitudes-2004-2-page-179.htm.

téléphoniques, à la surveillance des courriers électroniques, des dossiers médicaux, des transactions bancaires et des perquisitions menées en l'absence des personnes concernées[1430].

Le USA Patriot Act a été renouvelé par deux votes du Congrès en 2006, renouvellement promulgué par George W. Bush, et en 2011, renouvellement promulgué par Barack Obama jusqu'en juin 2015.

Cette loi est combattue par plusieurs juristes, car contraires aux droits de l'homme et au droit à un procès équitable. Toute entreprise américaine doit fournir les « données sensibles » demandées par l'administration fédérale, même si celles-ci sont stockées en Europe[1431].

Le USA Patriot Act a été complété en 2006, par le Military Commissions Act[1432], amendé en 2009, qui autorise le recours à des méthodes dures d'interrogatoire contre les suspects de terrorisme, la création de centres de détention clandestins à l'étranger et permet le jugement des détenus de Guantanamo par des tribunaux militaires. En mars 2009, le ministère de la Justice rend publiques sept directives légales secrètes, rédigées en 2001 et 2002, concernant la détention et le procès des personnes « combattants ennemis » et du transfert vers des pays tiers de membres d'Al Qaïda ou de talibans capturés sur le territoire américain[1433]. En décembre 2014, un rapport publié par le Congrès[1434] a levé le voile sur les traitements et tortures infligés par la CIA à des détenus, et ce, en contradiction avec les lois des États-Unis d'Amérique et les obligations liées aux traités internationaux.

[1430] Les neuf titres de l'USA Patriot Act sont :
Titre I : Augmenter la sécurité intérieure contre le terrorisme
Titre II : Procédures augmentées de surveillance
Titre III : Réduction du blanchiment d'argent international et Lois de financement antiterroriste de 2001
Titre IV : Protection des frontières
Titre V : Enlèvement des obstacles sur l'investigation dans le terrorisme
Titre VI : Aide aux victimes du terrorisme, des officiers de sécurité publique et des familles
Titre VII : Partage accru des informations pour la protection d'infrastructures critiques
Titre VIII : Renforcement de la législation pénale contre le terrorisme
Titre IX : Amélioration du renseignement.

[1431] Ce qui est interdit par la législation de l'Union européenne et contraire à la directive 95/46/CE.

[1432] Public Law 109-366 – October 17, 2006.

[1433] Charlotte Lepri, « Obama et la lutte contre le terrorisme : comment gérer l'héritage Bush ? », *Revue internationale et stratégique*, 2009/4 (n° 76), pp. 163-168. URL : https://www.cairn.info/revue-internationale-et-strategique-2009-4-page-163.htm consulté le 8 janvier 2018.

[1434] Disponible sur le site du sénateur démocrate Dianne Feinstein, présidente de la commission du renseignement, à http://www.feinstein.senate.gov/public/index.cfm?p=senate-intelligence-committee-study-on-cia-detention-and-interrogation-program consulté le 29 décembre 2015

Mais, c'est le programme PRISM, dénoncé par Edward Snowden, qui permet de mettre en place une surveillance de masse internationale[1435] et qui met en exergue la prédominance des États-Unis d'Amérique dans le contrôle du réseau Internet.

Sous-section 2. Une domination américaine

Le réseau Internet, de par son origine, est contrôlé par les États-Unis d'Amérique. Le premier modem[1436] a été créé dans les laboratoires Bell[1437] à Murray Hill dans l'État du New Jersey. Ce dispositif ouvre la voie du développement des réseaux de transmission entre ordinateurs. Sous l'égide de l'ARPA[1438] et du MIT[1439], un premier réseau permet de connecter quatre ordinateurs en décembre 1969. Ce sera le début du réseau ARPANET[1440]. À partir des travaux du français Louis Pouzin, chercheur à l'IRIA[1441], et de l'invention du datagramme[1442] dans le projet Cyclades[1443], le protocole TCP/IP[1444] et le réseau Internet vont pouvoir se développer.

Le réseau a pu se développer grâce à l'invention des noms de domaine qui permet d'utiliser un nom mnémonique ou URL[1445] en lieu et place de l'adresse IP du serveur. Les services d'enregistrement comprenant les domaines de premier niveau[1446], la gestion des Serveurs DNS[1447] Racine et des adresses Internet est confiée à SRI International, via son service DDN-NIC, par contrat avec le ministère de la défense américain. En 1998, une association

[1435] Cf. Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 1. § 2 -B)2) Les États-Unis d'Amérique et le USA PATRIOT Act.

[1436] Modulateur-démodulateur est un équipement qui permet de convertir un signal analogique en signal numérique et réciproquement. Ce dispositif est à l'origine de la transmission des données sur les réseaux de transmission de la voix, c'est-à-dire le réseau téléphonique.

[1437] *Bell Telephone Laboratories* ou *AT&T Bell Laboratories* plus connus sous l'appellation de *Bell Labs*. Dans ce laboratoire que Ken Thompson a développé un système d'exploitation dénommé Unics qui deviendra par la suite UNIX.

[1438] *Defense Advanced Research Projects Agency* (DARPA ou ARPA) sous tutelle du Département de la Défense des États-Unis.

[1439] *Massachusetts Institute of Technology*.

[1440] Contraction de ARPA Network.

[1441] Institut de Recherche en Informatique et en Automatique, créé en 1967 et devenu l'INRIA, Institut National de Recherche en Informatique et en Automatique, le 27 décembre 1979.

[1442] Technique de commutation par paquets, dans laquelle chaque paquet comporte toutes les informations nécessaires à son acheminement.

[1443] Projet expérimental français ayant pour but de créer un réseau global de télécommunication utilisant la commutation de paquets, créé en 1971, conçu par Louis Pouzin, il fut abandonné en 1978.

[1444] TCP/IP ensemble des protocoles utilisés pour le transfert des données sur Internet : TCP (Transmission Control Protocol) et IP (Internet Protocol).

[1445] À partir de l'anglais *Uniform Resource Locator*.

[1446] *Top Level Domain* ou TLD.

[1447] De l'anglais *Domain Name Server*.

californienne à but non lucratif travaillant pour le compte du ministère du commerce américain assure la tutelle de cette gestion.

La domination nord-américaine sur Internet est également utilisée par l'administration américaine pour une surveillance de masse dans le cadre de la lutte contre le terrorisme. Elle est amplifiée par l'origine nord-américaine des grands acteurs du réseau et de leur soumission à cette administration.

§ 1 - Une approche américaine sécuritaire et hégémonique

Depuis les attentats du 11 septembre 2011 sur les tours de Manhattan, la paranoïa sécuritaire des États-Unis d'Amérique n'a fait que s'aggraver. Outre le *USA Patriot Act*, les États-Unis d'Amérique ont « imposé » des mesures sécuritaires : *Passenger Name Record, ESTA* pour le voyageur entrant ou transitant par avion sur le territoire des États-Unis, mais ils ont aussi, en utilisant les moyens techniques à leur disposition espionné le réseau Internet, intercepté les messageries électroniques et écouté les conversations transitant sur les réseaux. Cette écoute généralisée a été révélée par Edward Snowden[1448].

Selon ses révélations, la NSA aurait capté des métadonnées des appels téléphoniques aux États-Unis. Il a aussi dévoilé des systèmes d'écoute sur Internet[1449] utilisant des programmes de surveillance *PRISM, XKeyscore, Tempora* et autres. Il révèle également des écoutes téléphoniques de certains dirigeants européens, dont Madame Angela Merkel, chancelière de l'Allemagne.

La NSA et le FBI auraient accès aux serveurs des géants américains de l'Internet, dont Microsoft, Apple, Yahoo!, Google et Facebook, via un programme secret au nom de code « PRISM » mis en place depuis 2007[1450]. Un portail permettrait à la NSA de se connecter aux serveurs des entreprises pour consulter des informations sur les utilisateurs présumés

[1448] Edward Joseph Snowden est un informaticien américain, ancien employé par la Central Intelligence Agency (CIA) et la National Security Agency (NSA), qui a révélé à partir du 6 juin 2013, certains détails des programmes de surveillance de masse américains et britanniques.

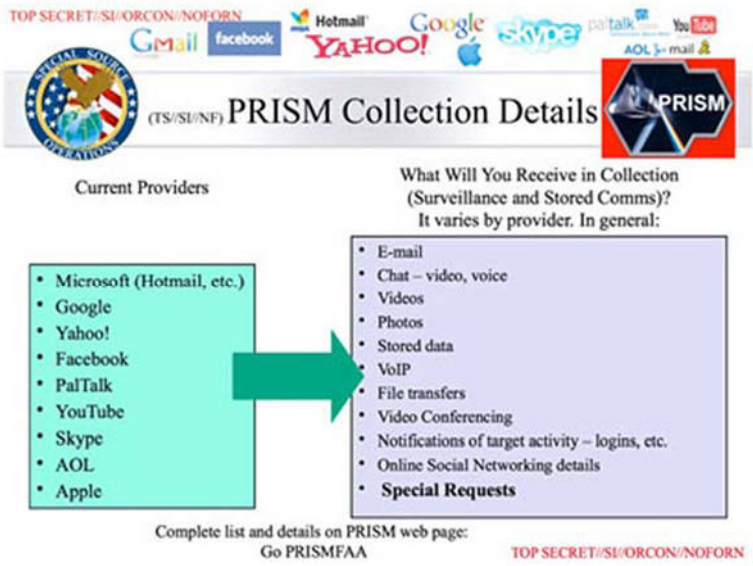
[1449] Le Monde.fr avec AFP, « Surveillance d'Internet : un ancien employé de la CIA à l'origine des fuites », 9 juin 2013, *LeMonde.fr,* URL : http://www.lemonde.fr/ameriques/article/2013/06/09/un-ancien-employe-de-la-nsa-derriere-les-revelations-sur-les-ecoutes-numeriques_3426888_3222.html#b77c0qYFGAKhIYKC.99 consulté le 16 décembre 2015.

[1450] Le Monde.fr avec AFP, « Le FBI aurait accès aux serveurs de Google, Facebook, Microsoft, Yahoo! et d'autres géants d'Internet », 7 juin 2013, *LeMonde.fr,* URL : http://www.lemonde.fr/ameriques/article/2013/06/07/le-fbi-a-acces-aux-serveurs-des-geants-d-Internet_3425810_3222.html#OEF9XUIrZqgC8Yqk.99 consulté le 16 décembre 2015.

« raisonnablement » être à l'étranger, c'est-à-dire hors du territoire des États-Unis d'Amérique, les personnes hors du territoire américain ne sont pas protégées par la loi contre une surveillance faite sans ordonnance de justice. Selon le Guardian, la NSA peut consulter « *les courriers électroniques, les chats vidéo et audio, les vidéos, les photos, les chats comme Skype, les transferts de fichiers, les détails des réseaux sociaux, et plus* ». Les communications par Skype peuvent être espionnées en direct. Il s'agit de « *l'un des accès les plus riches [...] pour la NSA* », selon le Guardian[1451]. En 2017, lors des attaques par WannaCry utilisant une faille de sécurité du logiciel Windows, il a été révélé que la NSA connaissait cette faille et, l'utilisant pour pénétrer des ordinateurs, ne l'avait pas signalée.

Devant ces révélations, la Commission de l'informatique et des libertés a réagi en France et a exprimé : « *son inquiétude et sa réprobation à l'égard de traitements qui auraient un tel objet*

Figure 1 PRISM - source Guardian



ou un tel effet. À cet égard, le traitement PRISM constitue une violation de la vie privée des citoyens européens d'une ampleur inédite et illustre concrètement la menace que représente la mise en place d'une société de surveillance »[1452]. La Commission de l'informatique et des libertés propose des « *réponses juridiques et opérationnelles : un cadre réglementaire*

[1451] Glenn Greenwald, Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", 7 juin 2013, *The Guardian* disponible à http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data consulté le 16 décembre 2015.

[1452] CNIL, « Affaire PRISM : ce que fait la CNIL », 24 octobre 2013, accessible à l'URL : http://www.cnil.fr/nc/linstitution/actualite/article/article/affaire-prism-ce-que-fait-la-cnil/ consulté le 16 décembre 2015.

européen : […] la CNIL a demandé avec force que tout transfert de données relatives à des citoyens européens à la demande d'États tiers soit subordonné à l'autorisation des autorités des pays des citoyens concernés. Les amendements adoptés par la commission " LIBE " du Parlement européen, le 21 octobre dernier, sur ce projet de règlement, montrent que ces préoccupations ont été entendues. […] la CNIL considère que l'échelon européen est le niveau pertinent de réponse en la matière, et que l'Europe doit parler d'une voix unie ; la nécessité d'un accord intergouvernemental : elle s'est […] prononcée en faveur d'accords internationaux entre les États membres de l'Union européenne et les États-Unis pour encadrer les échanges de données de renseignement entre ces pays. Ceci permettra en effet aux entreprises sollicitées à ce titre de s'opposer à la divulgation de ces données en l'absence d'un tel accord. »

Ces révélations ont été également reprises par la Cour de justice de l'Union européenne pour étayer sa décision d'annulation de l'accord de Safe Harbor[1453]. M. Schrems, citoyen autrichien résidant en Autriche est un utilisateur des serveurs Facebook et à ce titre a accepté les conditions d'utilisation des services de Facebook, c'est-à-dire accepté un contrat avec Facebook Ireland, filiale de Facebook Inc. M. Schrems a saisi le commissaire irlandais afin d'interdire à Facebook Ireland de transférer ses données personnelles vers le territoire des États-Unis, arguant que la protection de ses données à caractère personnel n'était pas suffisamment garantie compte tenu des pratiques en vigueur dans ce pays, révélées par M. Snowden. Le commissaire a refusé de se saisir de la plainte, car il n'était pas démontré que la NSA avait accédé aux données personnelles de M. Schrems et que par la décision 2000/520 la Commission européenne avait reconnu le caractère adéquat de la protection des données personnelles aux États-Unis d'Amérique. La Haute Cour de justice, saisie par M. Schrems, a constaté que « *la surveillance électronique et l'interception des données à caractère personnel transférées depuis l'Union vers les États-Unis répondaient à des finalités nécessaires et indispensables à l'intérêt public*. », mais elle a jouté que « *la NSA et d'autres organes fédéraux avaient commis des "excès considérables"* » démontrés par les révélations de M. Snowden. Mais compte tenu de la directive 95/46/CE et de la décision 2000/520, la Haute Cour a soumis à la Cour de justice de l'Union européenne la question préjudicielle de savoir si un organe « *chargé d'appliquer la législation sur la protection des données saisi d'une plainte relative au transfert de données à*

[1453] Cour de justice de l'Union européenne (grande chambre), décision du 6 octobre2015, *affaire Maximilien Schrems contre Data rotection Commisioner.*

caractère personnel vers un pays tiers […], dont le plaignant soutient que le droit et les pratiques n'offriraient pas des protections adéquates à la personne concernée, est-il absolument lié par la constatation contraire de l'Union contenue dans la décision 2000/520 ? »
Après avoir rappelé qu'au titre de l'article 28, paragraphes 1 et 6, de la directive 95/46/CE « *que les pouvoirs des autorités nationales de contrôle concernent les traitements de données à caractère personnel effectués sur le territoire de l'État membre dont ces autorités relèvent, de sorte qu'elles ne disposent pas de pouvoirs, sur le fondement de cet article 28, à l'égard des traitements de telles données effectués sur le territoire d'un pays tiers.* », la Cour a constaté que « *l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel au sens de l'article 2, sous b), de la directive 95/46/CE* » en conformité avec une décision précédente : « *le transfert des données PNR au CBP constitue un traitement* »[1454].
Ainsi après avoir constaté que « *une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte »* et que « *une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte* » et que « *la Commission n'a pas fait état, dans la décision 2000/520, de ce que les États-Unis d'Amérique "assurent" effectivement un niveau de protection adéquat en raison de leur législation interne ou de leurs engagements internationaux* », la Cour conclut que « *l'article 1er de cette décision méconnaît les exigences fixées à l'article 25, paragraphe 6, de la directive 95/46, lu à la lumière de la Charte, et qu'il est de ce fait invalide.* » De même, la Cour conclut à l'invalidité de l'article 3 de la décision pour outrepassement par la Commission de sa compétence, car cet article prive les autorités nationales des pouvoirs tirés de l'article 28 de la directive 95/46/CE. Les autres articles de la décision ne pouvant être dissociés, la Cour conclut à l'invalidité de la décision 200/520 concernant la sphère de sécurité ou Safe Harbor permettant le transfert des

[1454] Cour de justice de l'Union européenne (grande chambre) arrêt du 30 mai 2008, affaires C-317/04 et C-318/04 *Parlement européen contre Conseil de l'Union européenne et Commission des Communautés européennes*.

données à caractère personnel du territoire de l'Union européenne vers le territoire des États-Unis d'Amérique.

Ainsi, la Cour de justice de l'Union européenne a indirectement mis en cause la politique sécuritaire des États-Unis d'Amérique comme disproportionnée vis-à-vis des libertés fondamentales face au but d'ordre public à atteindre.

La domination des États-Unis d'Amérique reste importante sur Internet. La gestion des noms de domaines de premier niveau est, aujourd'hui, décentralisée, mais la gestion et la maintenance des serveurs DNS Racine restent contrôlées par le gouvernement américain. De plus, les principaux fournisseurs de l'Internet sont d'origine nord-américaine, qu'ils s'agissent des GAFA ou des principaux éditeurs de logiciel, y compris les logiciels de protection des ordinateurs personnels.

§ 2 - Une dépendance américaine « extraterritoriale »

Si la gestion de l'Internet reste de par son historique sous contrôle de l'administration américaine, de nombreuses sociétés œuvrant sur l'Internet sont des sociétés américaines et placent leur prestation sous le régime des lois américaines[1455]. Par ailleurs, la législation américaine tend à imposer son emprise sur des sociétés qui ne sont pas américaines. Le financement en dollars de personnes et de pays jugés par les États-Unis coupables d'activités terroristes a ainsi entraîné le paiement de fortes amendes par des banques françaises[1456] ou européennes[1457] qui pourtant n'avaient pas enfreint la législation de leurs pays respectifs. Mais elle protège les entreprises américaines placées sous protection des lois américaines : après la marée noire de 1978 sur les côtes de Bretagne, provoquée par l'Amoco Cadis, immatriculé au Libéria, mais affrété par la compagnie américaine Amoco Transport, filiale de Standard Oil, les communes touchées et l'État français ont intenté un procès en Amérique et ont obtenu, dans un jugement prononcé le 24 janvier 1994, soit 14 ans après la catastrophe, par la Cour d'appel des

[1455] Cf. l'affaire Yahoo! déjà citée.
[1456] BNP Paribas : amende de 8,9 milliards de dollars en 2014, Crédit Agricole : accord en cours entre 900 millions et un milliards de dollars, Société Générale : enquête en cours.
[1457] UniCredit en Italie, Deutsche Bank en Allemagne : enquêtes en cours ; Commerzbank en Allemagne : amende de 1,45 milliards de dollars.

États-Unis pour le septième circuit[1458] la condamnation d'Amoco et une compensation financière de 1 257 millions de francs, soit la moitié des préjudices estimés. Dans l'environnement numérique, YAHOO! condamnée par la justice française a fait appel à la justice américaine pour ne pas se soumettre à la décision française[1459].

A) Les prestataires GAFA

Google, Apple, Facebook et Amazon dominent le monde occidental de l'Internet, ce sont toutes des sociétés de droit américain qui collectent et traitent des données personnelles, sans respecter la directive européenne 95/46/CE et sa transposition dans les États membres. Google a reconnu de facto qu'il scanne les messages échangés sur la messagerie GMAIL en annonçant en 2017 qu'il renonçait à cette pratique. Respecteront elles le Règlement général sur la protection des données et les obligations découlant du consentement des utilisateurs ?

Dans la déclaration des droits et responsabilités de Facebook, qui correspondent aux conditions d'utilisation, il est écrit : « *La version d'origine de ce document est en anglais (États-Unis). En cas de conflit entre la traduction de ce document et la version d'origine, la version d'origine prévaut* »[1460]. Dans cette déclaration qui est approuvée implicitement par tout utilisateur de Facebook, il y est écrit : « *En utilisant les Services Facebook ou en y accédant, vous acceptez la présente Déclaration, qui est susceptible d'être mise à jour à l'occasion, conformément à la section 13 ci-dessous* ». Ainsi, outre le fait que ces conditions sont implicitement acceptées lors de l'utilisation des services Facebook, ces conditions peuvent évoluer du fait de Facebook avec un simple avertissement de ce changement sur la page *Facebook Site Governance*. L'acceptation des conditions d'utilisation des services Facebook n'est donc pas un contrat d'adhésion équilibré puisqu'après son acceptation, il peut être modifié de façon unilatérale par le fournisseur de service[1461]. Il s'agit d'un contrat « d'adhésion étendue » qui, une fois accepté

[1458] *in the Matter of Oil Spill By the Amoco Cadiz Off the Coast of France on March 16, 1978*., 954 F.2d 1279 (7th Cir. 1992) at http://federal-circuits.vlex.com/vid/spill-amoco-cadiz-off-france-march-37678690, consulté le 10 décembre 2015.

[1459] Voir Partie 1. Titre 1. Chapitre 1. Section 1. Sous-section 1. § 1 -C) La difficile harmonisation internationale des réglementations en matière de liberté d'expression dans un monde numérique.

[1460] Accessible à https://fr-fr.facebook.com/legal/terms?locale=fr_FR, consulté le 11 décembre 2015.

[1461] L'article 1110 du Code civil définit le contrat d'adhésion comme étant « *celui dont les conditions générales, soustraites à la négociation, sont déterminées à l'avance par l'une des parties* ». L'article 1171 introduit une règle sur les clauses abusives dans un contrat d'adhésion : « *Dans un contrat d'adhésion, toute clause qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite.*

implicitement par l'utilisateur, rend automatiquement opposables à cet utilisateur les modifications effectuées par l'autre partie sans qu'il soit nécessaire de les lui signaler.

En cas de litiges, ces mêmes conditions précisent : « *Vous porterez toute plainte, action en justice ou contestation ("action") afférente à cette Déclaration ou à Facebook exclusivement devant un tribunal américain du Northern District de Californie ou devant un tribunal d'État du comté de San Mateo, et vous acceptez de respecter la juridiction de ces tribunaux dans le cadre de telles actions. Le droit de l'État de Californie régit cette Déclaration, de même que toute action entre vous et nous, sans égard aux dispositions en matière de conflits de lois.* » récusant ainsi toute application du droit international en matière de compétence des tribunaux entre particuliers et professionnels tels le Règlement n° 44/2001 du 22 décembre 2000 (Bruxelles 1) sur la compétence ou les règles françaises en matière de droit international privé et de la protection de la partie faible. Le Tribunal de grande instance de Paris a estimé en mars 2015 que les tribunaux français étaient compétents pour juger le réseau social Facebook, dans le cadre d'une affaire l'opposant à un utilisateur. La décision ouvre une brèche dans la défense habituelle de la firme, qui renvoie aux juridictions californiennes. Dans son arrêt du 12 février 2016, la Cour d'appel de Paris a confirmé l'ordonnance du TGI de Paris du 5 mars 2015[1462] qui avait jugé que la clause attributive de compétence au profit des tribunaux du comté de Santa Clara en Californie, figurant dans les conditions générales de Facebook, constituait une clause abusive, donc considérée comme nulle et non écrite.

Dans les conditions générales d'utilisation de Google qui prévoit également la compétence des tribunaux de Californie, il est ajouté : « *Dans certains pays, des tribunaux pourraient refuser d'appliquer la loi de l'État de Californie dans certains cas de litiges. Si vous résidez dans l'un de ces pays, les lois de votre pays s'appliqueront à tout litige résultant des présentes, en cas de non-application de la loi de l'État de Californie. Dans le cas contraire, vous reconnaissez que les éventuels litiges liés aux présentes Conditions d'Utilisation seront régis par les lois de l'État de Californie, États-Unis, à l'exclusion des règles de conflit de lois de cet État. Si la justice de votre pays ne vous autorise pas à vous pourvoir devant les tribunaux du comté de Santa Clara, Californie, États-Unis, les litiges relevant des présentes seront portés devant les tribunaux*

« L'appréciation du déséquilibre significatif ne porte ni sur l'objet principal du contrat ni sur l'adéquation du prix à la prestation ». La modification unilatérale du contrat après l'adhésion peut donc être considérée comme clause abusive.

[1462] « *La clause des CGU de Facebook imposant un tribunal californien est abusive* », Légalis, 23 février 2016, disponible à https://www.legalis.net/actualite/la-clause-des-cgu-de-facebook-imposant-un-tribunal-californien-est-abusive/, consulté le 13 juillet 2017.

compétents de votre lieu de résidence. »[1463] en conformité avec les règles de droit international privé. Google a ainsi anticipé la décision des tribunaux français, laissant aux tribunaux la décision d'accepter la loi californienne ou de la récuser.

Si les informations, données, images ou vidéo, publiées par l'utilisateur restent sa propriété, Facebook peut en disposer librement et gratuitement sans limitation de territoire : « *vous nous accordez une licence non exclusive, transférable, sous-licenciable, sans redevance et mondiale pour l'utilisation des contenus de propriété intellectuelle que vous publiez sur Facebook ou en relation avec Facebook (licence de propriété intellectuelle).* »[1464] et ceci en contradiction avec l'impossibilité de transférer des données personnelles collectées sur le territoire européen vers des pays non adéquats, et de les utiliser dans un autre but que celui défini lors de l'acceptation de la collecte initiale.

Dans cette même clause, il est précisé que : « *Lorsque vous supprimez votre contenu de propriété intellectuelle, ce contenu est supprimé d'une manière similaire au vidage de corbeille sur un ordinateur.* » ce qui signifie que dans les faits, ce contenu reste stocké sur le support de stockage et ses caches, mais n'est plus accessible par l'utilisateur. Il reste cependant disponible pour Facebook et ses traitements statistiques, ainsi que par les utilisateurs de Facebook qui les auraient utilisées au titre de la clause 2.4 des conditions d'utilisation : « *Lorsque vous publiez du contenu ou des informations avec le paramètre Public, cela signifie que vous permettez à tout le monde, y compris aux personnes qui n'utilisent pas Facebook, d'accéder à ces informations et de les utiliser, mais aussi de les associer à vous (c'est-à-dire votre nom et votre photo de profil)* ». Ces conditions générales sont en non-conformité avec le Règlement général sur la protection des données, puisqu'avec le droit à l'oubli, introduit par ce règlement, en cas de dénonciation du consentement, les traitements déjà réalisés demeurent licites, mais tout nouveau traitement devient illicite. En cas de demande d'effacement, les données ne peuvent plus être utilisées.

Facebook a prévu de contourner la protection des données personnelles existant en Union européenne en ajoutant une clause spécifique à ces conditions d'utilisation[1465]. Cette clause

---

[1463] Conditions d'utilisation de Google, accessible à https://www.google.fr/intl/fr/policies/terms/regional.html consulté le 11 décembre 2015.

[1464] Déclaration des droits et responsabilités de Facebook, Clause 2.1.

[1465] « ***16. Clauses spéciales applicables aux internautes en dehors des États-Unis***
Nous nous efforçons de créer une communauté sans frontières avec des standards cohérents pour tous, tout en respectant les lois locales. Les clauses ci-après s'appliquent aux internautes qui interagissent avec Facebook en dehors des États-Unis :
1. Vous acceptez que vos données personnelles soient transférées et traitées aux États-Unis.

permet de ne pas respecter la directive 95/46/CE en indiquant que l'utilisateur autorise le transfert de ses données et leur traitement aux États-Unis d'Amérique alors que la directive interdit ce transfert hors du territoire européen vers des pays non adéquats, les États-Unis depuis l'invalidation de l'accord de Safe Harbor par la Cour de justice de l'Union européenne[1466] était devenu un pays non adéquat suite à la plainte de M. Schrems contre le transfert par Facebook des données personnelles collectées en Irlande vers des serveurs situés aux États-Unis d'Amérique, jusqu'au nouvel accord du *Privacy Shield*. L'acceptation des conditions d'utilisation de Facebook est un accord avec Facebook Ireland Limited[1467] pour les résidents de l'Union européenne, d'où la plainte déposée devant les tribunaux d'Irlande en conformité avec le règlement Bruxelles I.

Après l'arrêt Google Spain et l'arrêt Schrems de la Cour de justice de l'Union européenne, concernant Google et Facebook, les GAFA ne sont plus hors de portée de la justice européenne, comme semble l'indiquer la mise en demeure suivie d'amende infligée par la CNIL à Google concernant les données collectées par Street view, en particulier les données techniques relatives au Wi-Fi[1468], ou l'amende pour refus de déréférencement[1469].

B) Les fournisseurs de logiciels

D'autres fournisseurs de service américains dominent la fourniture de logiciels utilisés dans un monde numérisé. Il s'agit des principaux fournisseurs que sont Microsoft et Adobe, entre autres, qui fournissent non seulement des logiciels, mais aussi des espaces de stockage dans le Cloud

2. Si vous vous trouvez dans un pays sous le coup d'un embargo des États-Unis ou mentionné dans la liste « Specially Designated Nationals » du Département du trésor américain, vous ne pouvez pas conduire d'activités commerciales sur Facebook (comme faire de la publicité ou effectuer et recevoir des paiements), ni exploiter un site WEB ou une application de la plateforme. Vous n'utiliserez pas Facebook s'il vous est interdit de recevoir des produits, services ou logiciels provenant des États-Unis.

3. Certaines clauses propres aux internautes résidant en Allemagne peuvent être consultées [à https://www.facebook.com/terms/provisions/german/index.php]. »

[1466] Cour de justice de l'Union européenne, 6 octobre 2015, Affaire *Maximillian Schrems/Data Protection Commissioner*

[1467] Déclaration des droits et responsabilités de Facebook, Clause 18.1.

[1468] *Street View : la CNIL inflige une amende à Google,* 21 mars 2011, Le Monde Technologies, à http://www.lemonde.fr/technologies/article/2011/03/21/street-view-la-cnil-inflige-une-amende-a-google_1496083_651865.html, consulté le 3 octobre 2017.

[1469] *« Droit à l'oubli » : Google condamné à 100 000 euros d'amende*, 24 mars 2016, Le Monde à http://www.lemonde.fr/pixels/article/2016/03/24/droit-a-l-oubli-google-condamne-a-100-000-euros-d-amende_4889733_4408996.html, consulté le 3 octobre 2017.

et des fournisseurs de logiciel de protection contre les attaques virales ou autres tels que Symantec.

1) Antivirus et autres logiciels de « protection »

Pour faire face aux risques d'intrusion sur les PC, des éditeurs de logiciel distribuent des suites à installer sur ces PC. Ces suites détectent les virus, vers ou chevaux de Troie qui peuvent chercher à s'introduire sur ces machines et tentent de les éradiquer. Elles surveillent également les accès Internet pour éviter l'intrusion via les accès réseau ainsi que les messageries. L'utilisateur qui installe ces suites fait confiance à ces programmes pour protéger son ordinateur, mais il fait aussi confiance à ces éditeurs en leur confiant des données sensibles lors de certaines transactions : identité, données bancaires, etc. Ces données sont supposées ne pas être connues des éditeurs, mais elles sont stockées dans des bases gérées par ces éditeurs. Bien que cryptées, les éditeurs peuvent décrypter ces données puisqu'ils disposent des clés primaires. De plus, certaines éditions non seulement stockent les mots de passe et données d'identité, mais elles peuvent sauvegarder automatiquement des photos, des fichiers financiers ou tout autre fichier important[1470] choisi par l'utilisateur. Cette sauvegarde est réalisée sur le cloud, sans précision du lieu de stockage.

2) Logiciels et espaces sur le cloud

De nombreux autres éditeurs américains proposent des espaces de stockage sur le Cloud : Microsoft, Adobe, Nuance, etc. Ces espaces de stockage sont généralement fournis avec l'achat d'une suite logicielle, par exemple Office pour Microsoft.

Cet espace de stockage dans le Cloud est proposé pour permettre un stockage indépendant du lieu de travail, en se connectant au service depuis n'importe quel ordinateur, il devient possible d'avoir accès aux fichiers sauvegardés sur le cloud. Bien entendu, pour ouvrir un compte, il est nécessaire de fournir des informations personnelles. Toutefois, Microsoft reconnaît que lors de l'utilisation de ces services, certaines informations peuvent être collectées sans que l'utilisateur

[1470] Extrait de la documentation en ligne de Norton Security accessible à http://fr.norton.com/norton-security-with-backup accédé le 14 décembre 2015.

en soit conscient[1471]. Dans ce même document, Microsoft reconnaît qu'il peut partager avec d'autres organismes les informations ainsi collectées[1472]. Mais, Microsoft n'indique pas où il stocke les données ainsi collectées. Ces données peuvent être traitées aux États-Unis d'Amérique ou dans tout pays où Microsoft, ses filiales ou prestataires de service sont implantés, c'est-à-dire pratiquement n'importe où dans le Monde. Microsoft indique simplement qu'il adhère au cadre juridique du Safe Harbor (Sphère de sécurité), ce qui depuis la décision de la Cour de justice de l'Union européenne d'annuler l'accord de Safe Harbor, rend cette exigence insuffisante. Avec le Règlement général sur la sécurité des données, ce type de clause qui ne s'appuie pas sur le consentement des utilisateurs, sera contraire à la réglementation de l'Union.

Dans le cas d'Adobe, pour l'Union européenne, ce sont les lois de l'Irlande qui régissent la collecte et le traitement des données personnelles[1473]. Toutefois, Adobe reconnaît que les données peuvent être transférées et traitées n'importe où dans le monde, car Adobe possède « *des serveurs localisés dans le monde entier. Et les entreprises auxquelles [Adobe recourt] pour [l'] aider à gérer [ses] activités sont situées dans différents pays à travers le monde (par exemple, Argentine, Australie, Inde, Irlande, Singapour, Philippines, Royaume-Uni et États-Unis).* » Adobe reconnaît aussi s'appuyer sur l'accord Safe Harbor pour ces transferts et traitements.

Les éditeurs américains qui collectent des données personnelles, s'appuient sur l'accord Safe Harbor, ou depuis son invalidation sur l'accord Privacy shield, pour transférer et traiter les données collectées hors de l'Union européenne, et prévoient des traitements de ces données autres que celles ayant induit la collecte, que feront-ils lors de l'application effective du Règlement général sur la protection des données ?

[1471] « *Microsoft recueille des données pour fonctionner efficacement et vous offrir les meilleures expériences grâce à nos services. Vous fournissez certaines de ces données directement, lorsque vous créez un compte Microsoft, envoyez une requête de recherche à Bing, utilisez une commande vocale dans Cortana, téléchargez un document dans OneDrive, ou lorsque vous nous demandez de l'aide. Nous en obtenons certaines en enregistrant votre manière d'interagir avec nos services, par exemple en utilisant des technologies telles que les cookies, et en recevant des rapports d'erreur ou des données d'utilisation du logiciel que vous utilisez sur votre appareil. Nous obtenons également des données auprès de tiers (notamment d'autres sociétés).* » (texte disponible à l'URL : https://www.microsoft.com/fr-fr/privacystatement/default.aspx consulté le 14 décembre 2015).

[1472] « *Nous partageons vos données personnelles avec votre consentement ou au besoin pour terminer toute transaction ou fournir tout service que vous avez demandé ou autorisé. Nous partageons également des données avec les filiales contrôlées par Microsoft ; avec les prestataires travaillant en notre nom ; lorsque cela est exigé par la loi ou pour répondre à une procédure judiciaire ; pour protéger nos clients ; pour protéger des vies humaines ; pour maintenir la sécurité de nos services ; et pour protéger les droits ou la propriété de Microsoft.* » (même source).

[1473] En ligne à l'URL : http://www.adobe.com/fr/privacy.html consulté le 14 décembre 2015.

Si les GAFA ou l'administration américaine tentent de contourner la législation européenne de protection des données, d'autres contournements peuvent être autorisés par des traités internationaux moins protecteurs.

Sous-section 3. Une coopération internationale

Les attentats peuvent avoir une portée internationale, ainsi en juin 1914, l'attentat contre l'Archiduc François-Ferdinand d'Autriche précipite l'Europe puis le monde dans la Première Guerre mondiale. Une coordination internationale existe tant au niveau de l'Organisation des Nations Unies que de l'Union européenne.

§ 1 - Les conventions internationales

Des conventions internationales existent pour tenter de lutter tant contre la criminalité internationale, la cybercriminalité ou le terrorisme.

A) La convention de Budapest

La convention de Budapest est l'instrument juridique international en matière de lutte contre la cybercriminalité[1474]. Le traité a été rédigé par le Conseil européen et signé le 23 novembre 2001 à Budapest. Il est entré en vigueur le 1er juillet 2004. En 2011 pour les 10 ans de la convention, lors d'une conférence, 64 pays ont échangé sur les mesures à prendre pour lutter contre la cybercriminalité. Plus de 120 pays ont également coopéré avec le Conseil de l'Europe pour renforcer et harmoniser les législations contre la cybercriminalité.
La convention définit les infractions d'accès illégal, d'interception illégale, d'atteinte à l'intégrité des données, d'atteinte à l'intégrité du système, des infractions informatiques, falsifications ou fraudes informatiques[1475], et des infractions liées à la pornographie enfantine ou aux atteintes à la propriété intellectuelle. La tentative et la complicité sont également

[1474] Brigitte Pereira, « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », *Revue internationale de droit économique*, 2016/3 (t. XXX), pp. 387-409. URL : https://www.cairn.info/revue-internationale-de-droit-economique-2016-3-page-387.htm consulté le 8 janvier 2018.
[1475] Reprenant ainsi les incriminations pénales définies par la loi Godfrain dès 1988 (Loi n° 88-19 du 5 janvier 1988 *relative à la fraude informatique*).

retenues comme infractions. Chaque pays signataire doit adopter des « sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ».

La convention prévoit des principes généraux de coopération internationale et d'entraide. Aujourd'hui, 42 États ont signé et ratifié ce traité. Il est à noter que la France qui a signé la Convention le 23 novembre 2001, ne l'a ratifié que le 10 janvier 2006 pour une entrée en vigueur le 1er mai 2006.

Dans une société où la technique informatique évolue très rapidement, la réponse législative ou étatique peut sembler lente. Aujourd'hui, en France, de nombreux magistrats demandent la création d'un pôle de compétence spécialisé au sein de la magistrature, comme il en existe en matière financière.

B) Les conventions onusiennes

Au niveau de l'ONU, le terrorisme peut être défini comme : « *Tout acte qui vise à tuer ou à blesser grièvement des civils ou des non-combattants, et qui, du fait de sa nature ou du contexte dans lequel il est commis, doit avoir pour effet d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à agir ou à renoncer à agir d'une façon quelconque* »[1476].

Sur le site de l'ONU[1477], il est précisé : « *18 instruments universels (c'est-à-dire 14 Conventions et quatre amendements) ont été élaborés au sein même du système des Nations Unies, et visent des activités terroristes particulières. Par l'intermédiaire de l'Assemblée générale de l'ONU, les États membres se sont attachés à mieux coordonner leurs initiatives antiterroristes et à poursuivre l'élaboration de normes juridiques. Le Conseil de sécurité a lui aussi, lutté activement contre le terrorisme par ses résolutions et la création de plusieurs organes subsidiaires* ». Mais l'efficacité opérationnelle de ces instruments reste à démontrer.

[1476] « *Dans une liberté plus grande* », Rapport du secrétaire général des Nations unies, mars 2005, p. 67.

[1477] Équipe spéciale de lutte contre le terrorisme, « Coordination et cohérence de la lutte de l'Organisation des Nations Unies contre le terrorisme », Nations Unies, URL : http://www.un.org/fr/terrorism/index.shtml consulté le 30 mars 2015.

C) Les objectifs stratégiques de l'Union européenne

Dans l'Union européenne, au lendemain des attentats de Madrid de mars 2004, une cellule d'analyse de la menace terroriste a été créée au sein du « Centre de situation » (SITCEN) placé sous l'autorité du secrétaire général du conseil, haut représentant pour la Politique étrangère et de sécurité commune (PESC). Ce centre de situation produit une évaluation de la menace, fondée sur les sources que lui fournissent les services de renseignement, les militaires, les diplomates et les services de police des différents États membres. De plus, dans le cadre de l'OTAN, un comité spécial élabore des documents analytiques sur la menace terroriste qui pourrait affecter l'Alliance.

La stratégie européenne peut être résumée en quatre points précis : assurer la prévention, assurer une meilleure protection des cibles potentielles, désorganiser les réseaux existants et améliorer la capacité de réaction et de gestion des conséquences en cas d'attentat[1478].

La coordination opérationnelle des services des États membres est essentielle pour lutter contre le terrorisme. Cette coordination prend des formes variables, mais elle concerne essentiellement le domaine judiciaire et policier, avec en particulier des échanges d'information sur les risques et menaces terroristes. Après l'attention du musée juif de Bruxelles, cet échange d'informations a permis de localiser et d'appréhender le terroriste présumé en France et de le remettre entre les mains de la justice belge.

La nouvelle coopération en matière de lutte contre le terrorisme, souhaitée par les 28 États membres lors de la réunion du 19 janvier 2015, soulève un débat au cœur de l'Union européenne : faut-il aller vers plus d'intégration supranationale ou céder à la tentation du repli national ? À long terme, les États membres doivent aussi réfléchir à un moyen de consolider leurs relations avec leurs voisins méditerranéens et arabes et à une coordination de leurs politiques en matière de sécurité et de renseignement afin de s'assurer d'un environnement stable et sécuritaire.

Dans un discours prononcé dans le grand amphithéâtre de la Sorbonne, le 26 septembre 2017, Emmanuel Macron, Président de la République, a appelé l'Europe à se doter d'une force commune d'intervention, d'un budget de défense commun et d'une doctrine commune pour agir. Il a également proposé la fondation d'une Académie européenne du renseignement

[1478] Conseil de l'Union européenne, « Stratégie de l'UE visant à lutter contre le terrorisme », *Lutte contre le terrorisme,* 10 novembre 2017, URL : http://www.consilium.europa.eu/fr/policies/fight-against-terrorism/eu-strategy/ consulté le 8 janvier 2018.

réunissant les capacités de renseignement de tous les États membres de l'Union européenne pour lutter contre le terrorisme, considéré comme l'un des principaux défis actuels[1479].
Une coopération internationale nécessite un échange d'informations entre administrations ou États. Cet échange d'information peut concerner des données à caractère personnel, données qui sont l'objet d'une protection au sein de l'Union européenne.

§ 2 - Les échanges d'informations

Dans la continuité d'un mouvement bien amorcé, la LOPPSI 2 accroît les possibilités d'échange d'informations entre les services de l'État et les organismes de protection sociale au nom de la lutte contre la fraude aux aides sociales. La Cour de justice de l'Union européenne a dans sa décision du 1er octobre 2015, encadré les échanges de données entre administrations[1480] en statuant que : « *les articles 10, 11 et 13 de la directive 95/46 doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales […] qui permettent à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement* ».
Mais les échanges d'information peuvent être réalisés entre un État et les prestataires de service sur Internet. Edward Snowden fait état de telles transmissions de données à caractère personnel entre la NSA et les prestataires nord-américains.

A) Un échange entre l'État et les GAFA

Les États cherchent à obtenir des prestataires de service Internet des informations à caractère personnel hors des procédures judiciaires, ou à censurer certains services. Selon Google[1481], entre le 1er juillet 2009 et le 30 juin 2011, YouTube était inaccessible en Chine, et tous les

[1479] Discours disponible sur le site de l'Élysée à http://www.elysee.fr/videos/new-video-76/, visionné le 3 octobre 2017.
[1480] Cour de justice de l'Union européenne, troisième chambre, Décision du 1er octobre 2015, Affaire C-201/14, *Smaranda Bara e.a. contre Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*.
[1481] Google, *Transparency Report,* URL : http://www.google.com/transparencyreport/governmentrequests/ consulté le 5 mai 2015. Au 11 avril 2018, ces informations sont disponibles par accès à l'URL : https://transparencyreport.google.com/ consultée le 11 avril 2018.

services Google inaccessibles en Libye entre le 1er janvier 2011 et le 30 juin 2011. En France, durant cette même période, une seule ordonnance de tribunal a entraîné la suppression de 180 éléments de Google Groupes, relatifs à un cas de diffamation à l'encontre d'un homme et de sa femme. Mais le nombre de demandes de renseignements sur les utilisateurs reçues a augmenté de 29 % par rapport à la période de référence, soit 1 312 requêtes dont 47 % ont été satisfaites. Cette augmentation de requêtes a été de 39 % pour l'Allemagne. Il est à remarquer que durant la même période, sur les 5 950 requêtes reçues aux États-Unis d'Amérique, 93 % ont été satisfaites. Il est à noter que durant la campagne présidentielle, M. Emmanuel Macron avait précisé : « *Il est essentiel que ces entreprises acceptent un système de réquisition légale de leurs services cryptés, comparable à celui qui existe aujourd'hui pour le secteur des opérateurs de télécoms* »[1482].

L'utilisation des acteurs d'Internet pour tenter d'obtenir des informations à caractère personnel devient une réalité. La surveillance des individus à travers les usages du numérique risque de s'accroître dans les années à venir. La loi sur le renseignement de 2015 légalise cette surveillance dans le cadre de la lutte contre le terrorisme.

B) Une captation et des échanges entre les États

La lutte contre le terrorisme ou la cybercriminalité ne peut se limiter à une lutte nationale et nécessite la coopération entre États. Cette coopération implique des échanges de données entre les administrations chargées de la sécurité, cette coopération peut être volontaire et contrôlée, elle peut aussi être imposée par un État dominant. Si les données à caractère personnel peuvent être échangées au sein de l'Union européenne avec un niveau de protection homogène, il n'en est pas toujours ainsi lors d'échanges de données avec d'autres États qui n'ont pas mis en place un tel niveau de protection. Les États-Unis d'Amérique ont imposé à l'Union européenne la transmission des données passager (PNR) pour tous les vols entre l'Europe et les États-Unis, avant que cette transmission au sein de l'Europe ne soit approuvée[1483]. Les États-Unis ont

[1482] Emmanuel Macron, *Discours de la politique de lutte contre le terrorisme*, 10 avril 2017 - Retranscription du discours d'Emmanuel Macron à Paris, disponible en ligne à https://en-marche.fr/article/meeting-macron-politique-lutte-contre-le-terrorisme, consulté le 1 juillet 2017.

[1483] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 *relative à l'utilisation des données passagers (PNR) pour la prévention des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière* publiée au Journal officiel de l'Union européenne du 4 mai 2016.

également, de fait, avec l'ESTA[1484] restauré un visa pour les ressortissants européens pour entrer sur leur territoire par avion.

1) Des accords d'échange de données entre l'Union européenne et les États-Unis d'Amérique non équilibrés

La protection des données personnelles aux États-Unis d'Amérique n'a pas le niveau acquis en Europe. Dans le cadre de la question préalable soumise à la Cour de justice de l'Union européenne, concernant le transfert de données personnelles du territoire de l'Union européenne vers le territoire des États-Unis d'Amérique[1485], la Cour a constaté que « *les données à caractère personnel des citoyens de l'[Union] transférées aux États-Unis dans le cadre de la sphère de sécurité peuvent, en effet, être consultées et traitées par les autorités américaines d'une manière incompatible avec les motifs pour lesquels elles avaient été initialement collectées dans l'[Union] et avec les finalités de leur transfert vers les États-Unis* » et que « *les révélations de M. Snowden avaient démontré que la NSA et d'autres organes fédéraux avaient commis des "excès considérables"* » contraires au principe de proportionnalité. La Cour en a conclu que les données personnelles transférées vers le territoire des États-Unis ne disposaient pas d'une protection d'un niveau équivalent à celui garanti sur le territoire de l'Union européenne. Elle en a déduit l'invalidation de l'accord de Safe Harbor conclu entre la Commission européenne et les États-Unis d'Amérique. Cette décision de 2015 confirme les critiques formulées par plusieurs organismes européens, dont le Parlement. Après l'invalidation de l'accord, l'Union européenne et les États-Unis d'Amérique ont négocié un nouvel accord permettant le transfert de données vers le territoire américain : le *Privacy shield* ou bouclier de protection des données, entré en vigueur le 1er août 2016. Si cet accord contient des avancées par rapport au Safe Harbor, il demeure en retrait par rapport à la protection des données européenne[1486].

Mais il existe un autre accord de transfert de données à caractère personnel vers les États-Unis négocié en 2004, 2007, puis 2012 : l'accord PNR. Au départ, un PNR ou *Passenger Name Record* (données de dossier passager) est un enregistrement créé par les compagnies aériennes

[1484] *Electronic System for Travel Authorization*.
[1485] Cour de Justice de l'Union Européenne (Grande chambre), affaire C-362/14 *Schrems c/ Data Protection Commissioner*.
[1486] Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, WP 238 adopted on 13 April 2016, disponible à http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf, consulté le 13 juillet 2017.

pour enregistrer les réservations de vol. Pour permettre une communication entre compagnies et l'utilisation de systèmes centraux de réservation, cet enregistrement a été normalisé par l'AITA, association internationale de transport aérien (ou en anglais IATA *international Air Transport Association*).

Suite aux attentats du 11 septembre 2001, le Congrès a voté deux lois demandant l'accès au PNR, l'*Aviation and Transportation Security Act*[1487] le 19 novembre 2001 et le *Enhanced Border Security and Visa Entry Reform Act* of 2002[1488]. L'administration Bush a négocié un premier accord en mai 2004 avec l'Union européenne, connu sous le nom d'accord PNR États-Unis – Union européenne, approuvé par le Conseil le 17 mai 2004. En septembre 2004, le Parlement européen a présenté un recours contre la Commission devant la Cour européenne de justice qui a invalidé l'accord[1489]. Un nouvel accord, l'accord PNR 2007, a été signé le 23 juillet 2007 à Bruxelles et le 26 juillet 2007 à Washington[1490]. Les modifications demandées par le Parlement n'ont pas été prises en compte dans ce nouvel accord à l'exception du nombre de données transmises qui passe de 34 à 19. De plus, la durée totale de rétention des données passe de trois ans et demi à quinze ans[1491] et les données transmises peuvent être accédées par des pays tiers. Le 19 avril 2012, le Parlement européen a adopté le nouvel accord de transfert des dossiers passagers vers les États-Unis, malgré ces défauts[1492].

D'autres accords inter-étatiques sont en cours de négociation. Le 26 juillet 2017, la Cour de justice de l'Union européenne a déclaré que l'accord PNR prévu entre le Canada et l'Union européenne ne pouvait être conclu dans sa forme actuelle[1493]. Dans son avis, la Cour « *relève 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 à des autorités publiques canadiennes, européennes ou étrangères comportent une ingérence dans le droit fondamental au respect de la vie privée* ». Ainsi en 2017, soit plus de dix ans après

[1487] Public Law 107–71 - Nov. 19, 2001.
[1488] Public Law 107-173 - May 14, 2002 - [H.R. 3525].
[1489] Cour de justice, arrêt du 30 mai 2006, Parlement européen c/ Commission et c. Conseil, C-317/04 et C-318/04, in Recueil, 2006, p. I- 04721.
[1490] Décision 2007/551/PESC/JAI du Conseil du 23 juillet 2007 *relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007).*
[1491] Les deux ans de validité de l'autorisation plus un an, puis archivage des données pendant douze ans.
[1492] Résolution législative du Parlement européen du 19 avril 2012 sur *le projet de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure* (17433/2011 – C7-0511/2011 – 2011/0382(NLE)).
[1493] Cour de justice de l'Union européenne, Avis 1/15 de la Cour (grande chambre) 26 juillet 2017.

sa décision d'invalidation de l'accord PNR USA-UE de 2004 pour inadéquation de procédure, la Cour a jugé sur le fond le nouvel accord en préparation, et arrêté que ce futur accord dérogeait aux règles de protection de la Charte des droits fondamentaux de l'Union européenne[1494]. Mais la Cour considère par ailleurs que « *l'accord envisagé ne dépasse pas les limites du strict nécessaire en ce qu'il permet le transfert des données PNR de l'ensemble des passagers aériens vers le Canada* ». La Cour précise les nouvelles dispositions à prévoir dans l'accord concernant la protection des données à caractère personnel pour respecter la Charte : désignation des données à transférer, traitement non discriminatoire, non communication des données à un pays non membre de l'Union européenne sauf en cas d'accord existant entre l'Union et ce pays, droit à l'information individuelle des passagers, surveillance des règles de protection par une autorité de contrôle indépendante. Suite à cet avis, la Commission européenne a déclaré « *prendre acte de l'avis et être disposée à discuter avec le Canada des moyens de répondre aux préoccupations de la Cour* »[1495]. La Commission ajoute que si l'avis de la Cour ne porte officiellement que sur l'accord PNR envisagé avec le Canada, elle « *collaborera avec ses autres partenaires internationaux pour garantir que les transferts de données vers des pays non membres de l'UE sont conformes à l'avis de la Cour, au traité et à la charte des droits fondamentaux* ».

Au niveau de l'Union européenne, suite à une demande du Conseil européen des 25 et 26 mars 2004, la directive 2004/82/CE[1496] a été adoptée sans l'avis du Parlement européen. Elle se fonde sur l'accord de Schengen, et règle les échanges de données API ou informations préalables relatives aux passagers, dans un but officiel de lutte contre le terrorisme d'une part, et d'autre part contre l'immigration illégale, en autorisant « *l'utilisation de ces données comme élément de preuve dans des procédures visant à l'application des lois et des règlements sur l'entrée et l'immigration, notamment des dispositions relatives à la protection de l'ordre public et de la sécurité nationale* »[1497]. Dans un rapport de 2012, il est constaté que seuls dix États membres avaient implémenté dans sa totalité la directive[1498].

[1494] Le Traité de Lisbonne donne à cette charte une valeur juridique contraignante (TUE Art. 6).
[1495] Commission européenne, déclaration du 26 juillet 2017.
[1496] Directive 2004/82/CE du Conseil du 29 avril 2004 *concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.*
[1497] Directive 2004/82/CE, Considérant 12.
[1498] European Commission, *Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82*, Final Report for Directorate-General for Home Affairs, 17 September 2012.

Une nouvelle Directive PNR[1499] a été validée par le Parlement européen, elle a été publiée au Journal officiel de l'Union européenne du 4 mai 2016 et devra être transposée dans la loi nationale de chaque État membre au plus tard le 25 mai 2018. Elle contraint les compagnies aériennes à fournir aux autorités nationales les données des passagers pour tous les vols à partir d'un pays tiers vers l'Union européenne et inversement.

Le même jour, le Parlement européen a approuvé le Règlement général de protection des données[1500] et la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention, d'enquêtes et de poursuites pénales[1501]. Ce vote groupé de ces trois textes montre l'importance donnée par le Parlement européen à la protection des données à caractère personnel et la volonté de limiter les atteintes à cette protection à une juste adéquation ou proportionnalité entre la protection individuelle garantie au niveau européen et la sécurité collective des États membres.

En France, l'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme[1502] contraint les compagnies ferroviaires, aériennes et maritimes à transmettre les données PNR à la police et à la gendarmerie, ces données peuvent être rapprochées du Fichier des personnes recherchées (FPR) et du système d'information Schengen (SIS). Le 26 septembre 2014, un décret autorise la création d'un « système API-PNR France »[1503]. Le « système API-PNR France » porte sur les données de réservation (« Passenger Name Record », dites PNR) et les données d'enregistrement et d'embarquement (« Advance Passenger Information », dites API) de tous les passagers aériens. Il permet d'effectuer un rapprochement entre les données collectées et d'autres fichiers de police judiciaire et administrative, relatifs à des personnes ou des objets recherchés ou surveillés[1504].

[1499] 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.*

[1500] 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).*

[1501] 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.*

[1502] Loi nº 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* publiée au JORF nº0020 du 24 janvier 2006 p. 1129.

[1503] Décret n° 2014-1095 du 26 septembre 2014 *portant création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure.*

[1504] CNIL, « Le "système API-PNR France" » in *Les grands fichiers en fiche*, 10 août 2016.

2) Des échanges de renseignements de police sur des individus

Le SIS (Système d'Information Schengen), dont l'infrastructure technique se trouve à Strasbourg, prévoit que les autorités de chaque État parties peuvent « *signaler aux fins de non-admission »* les étrangers dont l'entrée sur leur territoire leur paraît dangereuse pour la sécurité ou l'ordre public, ou qui ont fait l'objet d'une interdiction de séjour. Son objectif est aussi la surveillance discrète et le contrôle spécifique pour la répression d'infractions pénales, la prévention de menaces pour la sécurité publique ou pour la prévention de menaces graves pour la sûreté de l'État.

S'agissant des personnes, peuvent être intégrés les éléments relatifs à l'état civil et les alias, les signes physiques particuliers, objectifs et inaltérables, l'indication éventuelle qu'elles sont armées ou violentes et la conduite à tenir en cas de découverte. Est interdite la mention d'informations dites sensibles révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que celles relatives à la santé ou à la vie sexuelle. De plus, le STIC l'alimente à l'envi, alors même que ce dernier fichier est truffé d'erreurs.

Depuis sa création, le fichage et l'interconnexion des fichiers de police que permettent le SIS n'ont eu de cesse d'être enrichis, depuis les hooligans jusqu'aux manifestants antimondialisation et même, toutes les personnes désirant se rendre en France. Le fichier SIS a évolué vers le fichier SIS II qui contient des données biométriques (photo, empreintes digitales)[1505]. Selon la CNIL, en 2015, 70 millions de signalements existaient dans le SIS II[1506]. Selon cette fiche de la CNIL, « *peuvent faire l'objet d'un signalement dans ce fichier les personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition, les personnes disparues, les personnes recherchées dans le but de rendre possible leur concours dans le cadre d'une procédure judiciaire, les personnes ou objets recherchés aux fins de contrôle discret ou de contrôle spécifique, les objets recherchés aux fins de saisie ou de preuve dans le cadre d'une procédure pénale, les ressortissants de pays tiers signalés aux fins de non-*

[1505] Règlement (CE) n° 871/2004 du Conseil du 29 avril 2004 *concernant l'attribution de certaines fonctions nouvelles au Système d'information Schengen, y compris dans le cadre de la lutte contre le terrorisme* publié au Journal officiel de l'Union européenne du 30 avril 2004.

[1506] Commission nationale de l'informatique et des libertés, « SIS II : Système d'information Schengen II », *Les grands fichiers en fiches,* 17 aout 2016, URL : https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii consulté le 8 janvier2016.

admission ou d'interdiction de séjour à la suite d'une décision administrative ou judiciaire, les ressortissants de pays tiers signalés et jouissant du droit de libre circulation dans la Communauté ». Europol et Eurojust peuvent accéder au fichiers SIS II.

Le système d'information d'Europol (SIE) contient tout un ensemble de données à caractère personnel relatives à des personnes soupçonnées d'avoir commis ou de commettre une infraction, directement accessibles en consultation par les officiers de liaison Europol (OLE) et les services de police nationaux via les Unités nationales Europol (UNE). Un système d'analyse permet d'étudier un phénomène ou un groupe criminel particulier à partir des données relatives aux auteurs, témoins et victimes d'infractions. Son caractère sensible explique la limitation de son accès aux seuls analystes. Un système d'index permet aux OLE des États non participants de consulter l'index des données contenues dans le fichier, afin, le cas échéant, de s'y associer. Comme pour les fichiers de police français, des données concernant les victimes et les témoins des infractions y sont enregistrées. La loi n°78/17 n'est pas applicable aux fichiers gérés par Interpol[1507].

Europol s'est vu accorder le droit d'interroger le SIS pour mener à bien ses missions, les organismes et États tiers peuvent participer à la constitution des fichiers de travail à des fins d'analyse, et le délai de conservation des données à caractère personnel contenues dans ces fichiers a été étendu de trois à cinq ans.

Ainsi, au travers des diverses interconnections des fichiers et des échanges entre services de police, des données à caractère personnel peuvent être captées dans un pays membre de l'Union européenne et traitées dans tout autre pays membre, sans que la personne physique concernée n'en soit ni avertie ni consciente. Si la protection des données à caractère personnel est garantie par des textes nationaux ou des textes de l'Union européenne, cette protection est atténuée par les États afin de pouvoir lutter efficacement contre la criminalité internationale et le terrorisme. La société numérique favorisant la criminalité sur Internet doit en permanence chercher un juste équilibre entre efficacité de la lutte et protection des libertés.

[1507] Lire à ce sujet, « Historique de la commission » en ligne à l'URL : https://www.interpol.int/fr/Media/Files/CCF/Documents/Historique-de-la-Commission consulté le 8 janvier 2018. Laurent Grosse, « L'accord de siège de 2008 entre le France et INTERPOL », *Annuaire Français de Droit International* 2008, CNRS Éditions, pp. 615-628.

Chapitre 2. Surveillance et liberté, des moyens de protection insuffisants et inadéquats

Les atteintes aux libertés au nom de la sécurité ont toujours existé dans notre pays. Albert Decourteix écrivait en 1879 : « *Ce n'est que depuis 1789 que nous avons une législation qui protège notre liberté et nous donne des garanties précieuses ; mais cette législation n'est pas suffisante pour nous défendre contre toutes sortes d'atteintes ; de plus, nous devons reconnaître qu'elle a été très mal appliquée dans des circonstances où notre sécurité exigeait qu'elle fût rigoureusement observée* »[1508]. Comme pour lui donner raison, la III[e] République, après des attentats d'origine anarchiques, adoptait les lois scélérates[1509] dénoncées par Léon Blum et Jean Jaurès.

Les dérives liées à la sécurité ne sont donc pas apparues avec les techniques modernes et l'explosion du numérique. Mais les techniques numériques donnent aux forces de sécurité des moyens puissants pour surveiller une personne physique à son insu. Sans anticiper sur la mise à disposition de logiciels espions sur Internet, décrits ultérieurement, la loi dite LOPPSI 2[1510] autorise la pose de logiciels de captation sous contrôle du juge d'instruction ou du Premier ministre pour une période de quatre mois, renouvelable. Cette loi sécuritaire a été sanctionnée par le Conseil constitutionnel dans plusieurs de ces articles au nom du respect des libertés.

[1508] Albert Decourteix, *La Liberté individuelle et le droit d'arrestation*, Marchal et Billard, 1879, p. 139.

[1509] Ces lois ont été votées pour répondre à l'inquiétude de l'opinion et répondre à une série d'attentats anarchistes. La loi du 12 décembre 1893 suit l'attentat d'Auguste Vaillant visant les députés, et a pour objet de modifier la loi du 29 juillet 1881 sur la presse pour réprimer l'apologie, ou provocation indirecte, et permettre à un juge d'ordonner une saisie et une arrestation préventive. La loi du 18 décembre 1893 modifie la loi de 18 décembre 1853 sur les associations de malfaiteurs et vise les groupes anarchistes en permettant l'arrestation de tout membre ou sympathisant. Enfin, la loi du 28 juillet 1894 qui suit l'assassinat du président de la République Sadi Carnot par un jeune anarchiste à Lyon, a pour objet de réprimer directement les menaces anarchiques, elle permet une véritable chasse aux sorcières et aboutira au procès des Trente ouvert le 6 août 1894 devant la cour d'assises de la Seine durant lequel 30 inculpés furent jugés, allant de théoriciens de l'anarchie à de simples cambrioleurs, tous rassemblés dans une même accusation d'association de malfaiteurs.

[1510] Loi n° 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure*.

L'équilibre entre sécurité et liberté est difficile à cerner et le Conseil constitutionnel a veillé à la proportionnalité des moyens et au respect des libertés fondamentales[1511].

Cette loi LOPPSI 2 permet d'installer sur un PC, ou tout autre dispositif numérique, un logiciel, en fait un cheval de Troie, qui va enregistrer toutes les données qui transitent sur ce dispositif et l'envoyer via Internet à un serveur particulier qui va enregistrer ces données, permettant aux forces de sécurité de les visualiser et de les consigner, à l'insu de la personne physique surveillée. La loyauté des moyens qui était la règle avant cette loi LOPPSI 2 disparaît. Toute personne physique impliquée directement ou indirectement dans une enquête pourra ainsi sur décision d'un juge d'instruction, ou du Premier ministre, se voir ainsi surveillée légalement, avec violation de son domicile privé[1512].

Cet espionnage légal a d'abord été introduit par la loi DADVSI[1513], puis les lois HADOPI 1[1514] et HADOPI 2[1515], les lois LOPPSI 1 et 2 conservent cette possibilité d'utiliser les traces numériques laissées par toute personne physique ou tout serveur informatique lorsqu'il utilise des techniques numériques de communication. Si les lois HADOPI permettent la surveillance des accès aux sites de téléchargement illégal, limitée à certains modes de téléchargements, la loi LOPPSI permet l'installation de logiciel dans l'ordinateur de la personne physique par introduction à son domicile, avec autorisation préalable du juge des libertés. Ce n'est donc plus par surveillance des accès aux sites que la surveillance est activée, mais toute information présente ou transitant sur l'ordinateur personnel est ou peut être collectée et analysée. Cette loi encadre également le traitement des données obtenues par les caméras de télésurveillance, et limite, après censure du Conseil constitutionnel[1516], ce traitement aux seules forces de police et de gendarmerie, en tant qu'officiers de police judiciaire.

Les techniques numériques permettent d'observer le comportement des individus, des entreprises, voire des États. Les révélations d'Edward Snowden sur le programme PRISM, tout

---

[1511] Rhita Bousta, « Contrôle constitutionnel de proportionnalité. La spécificité française à l'épreuve des évolutions récentes », *Revue française de droit constitutionnel*, 2011/4 (n° 88), pp. 913-930. URL : https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2011-4-page-913.htm consulté le 11 avril 2018.

[1512] « Loppsi II : un patchwork répressif », *Plein droit*, 2011/1 (n° 88), pp. 1-2. URL : https://www.cairn.info/revue-plein-droit-2011-1-page-1.htm consulté le 11 avril 2018.

[1513] Loi n° 2006-961 du 1 août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information*, publiée au JORF n°178 du 3 août 2006 p. 11529.

[1514] Loi n° 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur Internet,* publiée au JORF n°0135 du 13 juin 2009 p. 9666.

[1515] Loi n° 2009-1 311 du 28 octobre 2009 *relative à la protection pénale de la propriété littéraire et artistique sur Internet*, publiée au JORF n°0251 du 29 octobre 2009 p. 18290.

[1516] Conseil constitutionnel, Décision n° 2011-625 DC du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure,* considérants n°s16 à 19.

comme le rapport du Sénat américain sur les agissements de la CIA[1517] montrent que les agences gouvernementales peuvent s'immiscer dans l'intimité des individus sans contrôle réel des organes chargés de les surveiller. Le rapport sénatorial précise que la CIA a menti au Congrès et à la Maison-Blanche et a activement évité ou empêché la supervision du programme par le Congrès[1518].

En France, une délégation parlementaire au renseignement a été créée en 2007[1519]. Cette délégation est commune à l'Assemblée nationale et au Sénat et a pour mission « *de suivre l'activité générale et les moyens des services spécialisés à cet effet placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget* ». Sa mission a été élargie en 2013[1520], elle « *exerce le contrôle parlementaire de l'action du Gouvernement en matière de renseignement et évalue la politique publique en ce domaine* ». La Commission nationale de contrôle des interceptions de sécurité (CNCIS) doit lui présenter sur demande des rapports d'activité. Cette commission a été créée en 1991 pour vérifier la légalité des autorisations d'interception (écoutes téléphoniques non judiciaires) suite à l'affaire des écoutes de l'Élysée. La loi relative au renseignement de 2015[1521] l'a remplacée par la Commission nationale de contrôle des techniques de renseignement (CNCTR). Cette nouvelle commission s'assure que l'autorisation et la mise en œuvre sur le territoire national des techniques de recueil de renseignements procèdent d'une autorité ayant légalement compétence pour le faire, résultent d'une procédure conforme, respectent les missions confiées aux services les assurant et sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation. Comme pour les avis de la Commission de l'informatique et des libertés pour les traitements des données personnels par l'administration, les avis défavorables de la CNCTR ne bloquent pas l'autorisation du Premier ministre, l'autorisation donnée doit simplement indiquer les motifs pour lesquels cet avis défavorable n'a pas été suivi. De plus, en cas d'urgence, le Premier ministre peut délivrer l'autorisation sans avis préalable de la

[1517] Cf. Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 2. § 1 - Une approche américaine sécuritaire et hégémonique.

[1518] Senate Select Committee on Intelligence, *Committee Study of the CIA's Detention and Interrogation Program Findings and Conclusions*: "*#6: The CIA has actively avoided or impeded congressional oversight of the program"*.

[1519] Loi nº 2007-1 443 du 9 octobre 2007 *portant création d'une délégation parlementaire au renseignement* publiée au JORF nº235 du 10 octobre 2007 p. 16558.

[1520] Loi nº 2013-1 168 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* publiée au JORF nº0294 du 19 décembre 2013 p. 20570.

[1521] Loi nº 2015-912 du 24 juillet 2015 *relative au renseignement* publiée au JORF nº0171 du 26 juillet 2015 p. 12735.

commission. La CNCTR rédige un rapport d'activité annuel, elle doit répondre aux demandes d'avis du Premier ministre, du président de l'Assemblée nationale, du président du Sénat et de la délégation parlementaire au renseignement.

Les moyens de surveillance des individus existent et peuvent être légalement utilisés par les forces de police et de gendarmerie pour des motifs d'ordre public, les interceptions sont légalement mises à disposition des services de renseignements, de police et de gendarmerie par décision d'un magistrat ou par décision administrative en cas de danger pour la Nation. Ces moyens peuvent être mis en œuvre furtivement sans aucun contrôle jusqu'à leur détection inopportune ou leur dénonciation ou révélation. Les textes de protection existent, localement ou internationalement, des organismes de contrôle sont créés, ils peuvent dénoncer des abus, mais doivent les détecter par eux-mêmes alors que les moyens ne leur sont pas toujours donnés ou attendre une révélation d'un lanceur d'alerte. De plus, les textes protecteurs vieillissent et deviennent obsolètes face à une technique innovante en permanence et de plus en plus pressante.

Section 1. L'individu sous surveillance permanente

Lors de ses incursions sur le réseau Internet, l'individu est pisté, suivi, analysé[1522]. Mais, d'autres techniques numériques permettent de le surveiller et de le localiser sans incursion de sa part sur Internet. La télésurveillance et la géolocalisation permettent de le suivre et le localiser à son insu, les interceptions de correspondances sont également utilisées pour le surveiller[1523]. Toutes ces pratiques sont réglementées, mais les révélations d'Edward Snowden montrent que les États peuvent, eux aussi, ne pas respecter leur propre réglementation[1524].

Pour se protéger, la royauté disposait des lettres de cachet qui permettaient d'embastiller tout individu pouvant attenter par ses actes ou ses paroles à la sécurité du roi. Avec le *USA Patriot Act*, George W. Bush a doté les États-Unis d'Amérique de la possibilité d'arrêter et d'emprisonner toute personne suspectée de préparer un attentat contre les États-Unis d'Amérique, et ce sans l'intervention d'un juge. Les États-Unis d'Amérique se dotent ainsi de lois qui ne respectent pas la séparation des pouvoirs, le pouvoir réglementaire prenant le pas sur le pouvoir judiciaire pour des raisons de sécurité intérieure.

La France se dote aussi avec certaines lois de moyens de lutte contre le terrorisme, mais certains projets de loi sécuritaire se sont vus censurés partiellement par le Conseil constitutionnel au nom de la protection constitutionnelle des libertés. Mais, en France, depuis 2013, le pouvoir réglementaire substitue la protection judiciaire des libertés au profit d'une protection administrative.

[1522] Brochet Laura, « Décrypter, comprendre et maîtriser sa présence en ligne. **Identités numériques. Expressions et traçabilité**, *Jean-Paul Fourmentraux* (dir.), Paris, CNRS Éditions, 2015, 238 p., ISBN : 978-2-271-08702-7, 8 € », *L'Observatoire*, 2016/1 (N° 47), pp. 94-95. URL : https://www.cairn.info/revue-l-observatoire-2016-1-page-94.htm consulté le 11 avril 2018.

[1523] Emmanuel Valjavec, « Internet, un nouvel espace de liberté sous surveillance », *Études*, 2013/3 (Tome 418), pp. 317-327. URL : https://www.cairn.info/revue-etudes-2013-3-page-317.htm consulté le 9 janvier 2018.

[1524] Zygmunt Bauman, Didier Bigo, Paulo Esteves *et al.*, « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », *Cultures & Conflits*, 2015/2 (n° 98), pp. 133-166. URL : https://www.cairn.info/revue-cultures-et-conflits-2015-2-page-133.htm consulté le 9 janvier 2018.

Sous-section 1. La télésurveillance et la géolocalisation

En Europe, le Royaume-Uni a installé un nombre impressionnant de caméras de vidéosurveillance, une caméra pour onze habitants en moyenne[1525]. Si la première caméra y a été installée en 1960, les caméras de surveillance ont été utilisées par le gouvernement de Madame Thatcher pour surveiller en 1984 la grève des mineurs. Aujourd'hui, les caméras de vidéosurveillance y sont présentes sur la voie publique, mais aussi dans les hôpitaux et les écoles, sans que leur efficacité en termes de prévention ne soit démontrée.

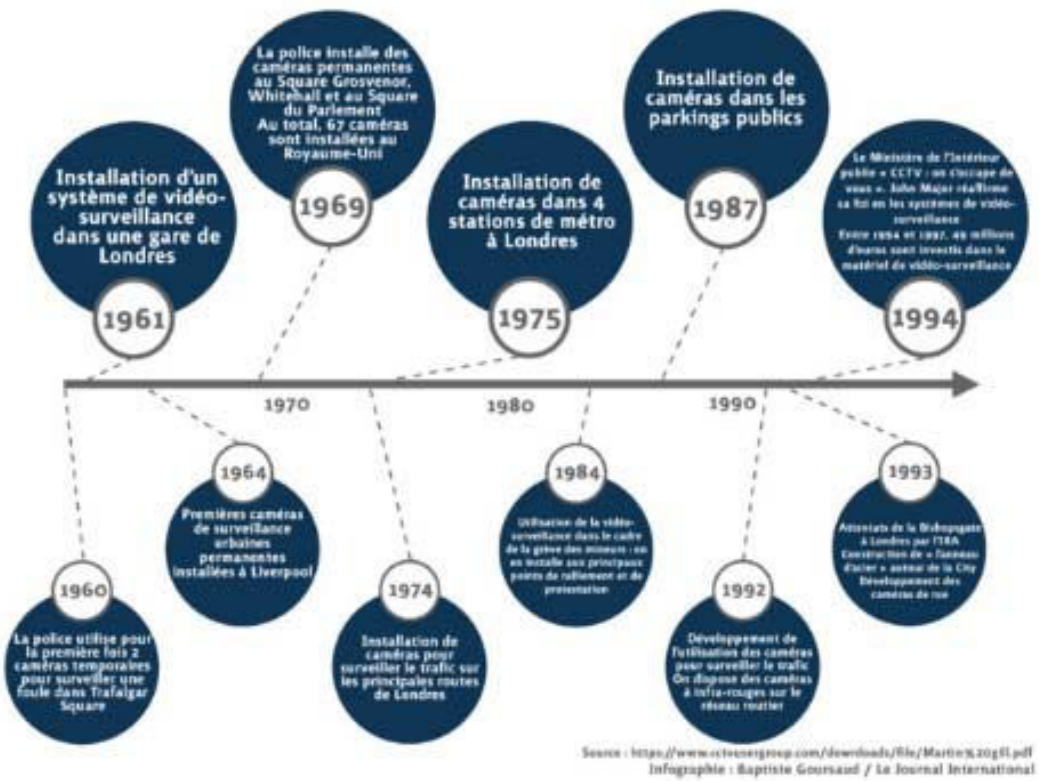


Figure 2 Chronologie de la politique anglaise de vidéosurveillance — Crédit Baptiste Goursaud

En France, comme dans d'autres pays européens, la surveillance des espaces privés et publics par l'intermédiaire de caméras de surveillance est utilisée depuis plusieurs années. Cette surveillance a fait l'objet de textes réglementant son usage et prévenant les abus[1526].

[1525] Alexis Demoment et Elliot Maccarinelli, « Les citoyens contre la vidéo-surveillance », *Le Journal International*, 11 février 2015, à http://www.lejournalinternational.fr/Les-citoyens-contre-la-video-surveillance_a2286.html consulté le 4 janvier 2016.

[1526] Lire sur le sujet la fiche pratique de la Commission nationale de l'informatique et des libertés, « Vidéosurveillance / vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », 21 juin 2012, URL : https://www.cnil.fr/fr/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de-la-vie consulté le 9 janvier 2018.

§ 1 - Sécurité et télésurveillance

Dans les magasins, il est fréquent de voir des caméras filmant les abords des caisses ou certains rayons. La loi informatique et libertés oblige le commerçant à déclarer les installations de surveillance qui enregistrent les images et permettent de reconnaître des individus. Si le dispositif filme des lieux non ouverts au public, entrepôt, salle des coffres, une déclaration auprès de la Commission de l'informatique et des libertés est nécessaire, sauf si un Correspondant informatique et liberté a été désigné, auquel cas un simple enregistrement du dispositif dans son registre est suffisant. Si le dispositif est utilisé pour la surveillance d'espaces ouverts au public, une demande d'autorisation doit être adressée au préfet du département, ou au préfet de police pour Paris, qui est seul habilité à fournir cette autorisation d'installation[1527]. Les employés doivent être consultés et informés de l'installation de caméras de télésurveillance sur leur lieu de travail[1528]. Les images ne peuvent pas être librement accessibles aux employés et clients, seul le personnel de direction ou de sécurité peut visualiser les images enregistrées et conservées au maximum durant un mois[1529].

La télésurveillance dans les magasins est assujettie aux règles générales encadrant la télésurveillance dans les locaux privés ouverts ou non au public, ces règles sont extraites de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés lorsque les caméras fixent des lieux non ouverts au public, du code de la sécurité intérieure[1530], du Code du travail[1531], du Code civil[1532], du Code pénal[1533].

[1527] D'après CNIL, Article « Vidéosurveillance — Vidéoprotection » accessible à http://www.cnil.fr/les-themes/videosurveillance/actualite/article-videosurveillance-videoprotection/article/videosurveillance-videoprotection-dans-les-commerces/ consulté le 4 janvier 2016.

[1528] Code du travail, Art. L.2323-32, L.1221-9, L.1222-4 et L.1121-1.

[1529] Lire la fiche technique de la Commission nationale de l'informatique et des libertés, « La vidéosurveillance - vidéoprotection au travail », 19 octobre 2015, URL : https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail consulté le 9 janvier 2018.

[1530] Articles L.223-1 et suivants, relatifs à la lutte contre le terrorisme ; Articles L.251-1 et suivants, lorsque les caméras filment des lieux ouverts au public ou la voie publique.

[1531] Article L.2323-32 relatif a l'information et la consultation des instances représentatives du personnel ; Articles L.1221-9 et L.1222-4 relatifs à l'information individuelle des salariés ; Article L.1121-1 relatif au principe de proportionnalité.

[1532] Article 9 relatif à la protection de la vie privée.

[1533] Article 226-1 relatif à l'enregistrement de l'image d'une personne à son insu dans un lieu privé ; Article 226-16 relatif à la non-déclaration auprès de la CNIL ; Article 226-18 relatif à la collecte déloyale ou illicite de données à caractère personnel ; Article 226-20 relatif à la durée de conservation excessive des données à caractère personnel ; Article 226-21 relatif au détournement de la finalité du dispositif ; Article R625-10 relatif à l'absence d'information des personnes.

La vidéosurveillance est également utilisée pour des raisons de sécurité sur la voie publique[1534], le nombre de caméras filmant la voie publique a fortement augmenté sous l'impulsion des pouvoirs publics pour lutter contre l'insécurité. Seules les autorités publiques, mairies, peuvent filmer la voie publique pour prévenir des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés aux risques d'agression, de vol ou de trafic de stupéfiants. En septembre 2015, la ville de Paris a décidé de s'équiper de 165 caméras supplémentaires qui s'ajoutent aux 1 144 déjà existantes[1535]. Les entreprises ou les établissements publics ne peuvent filmer que les abords de leurs bâtiments, par exemple les façades extérieures. Les caméras ne doivent pas filmer l'intérieur des immeubles d'habitation ni leurs entrées, afin de protéger l'intimité de la vie privée des personnes y habitant.

Ces dispositifs de surveillance doivent être autorisés par le préfet, ou le préfet de police pour Paris, pour une période de cinq ans, renouvelable. Il est également possible d'installer un dispositif de vidéosurveillance lors d'une manifestation ou d'un rassemblement de grande ampleur, en suivant la même procédure. Le préfet peut aussi demander à une commune de s'équiper en moyens de vidéoprotection en cas de menaces terroristes. Dans ce cas, le conseil municipal doit en délibérer dans un délai de trois mois.

La vague sécuritaire a vu l'explosion des caméras de vidéosurveillance, renommées caméras de vidéoprotection. Le texte de référence en matière de vidéosurveillance est la loi d'orientation et de programmation pour la sécurité (LOPS) du 21 janvier 1995[1536]. Son article 10-I dispose : « *Les enregistrements visuels de vidéosurveillance ne sont considérés comme des informations nominatives, au sens de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, que s'ils sont utilisés pour la constitution d'un fichier nominatif* ». Ainsi, enregistrer une scène de rue ne relève pas d'un traitement de données à caractère personnel si cet enregistrement n'est pas associé à une personne physique. Cet article est devenu : « *Les enregistrements visuels de vidéoprotection répondant aux conditions fixées au II sont soumis aux dispositions ci-après, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi nº 78-17 du 6*

[1534] Code de la sécurité intérieure, Article L.223-1.
[1535] Le Figaro.fr, « Vidéosurveillance : 165 caméras de plus à Paris », 29 septembre 2015, *LeFigaro.fr,* URL : http://www.lefigaro.fr/flash-actu/2015/09/29/97001-20150929FILWWW00351-videosurveillance-165-cameras-de-plus-a-paris.php consulté le 13 avril 2018.
[1536] Loi nº 95-73 du 21 janvier 1995 *d'orientation et de programmation relative à la sécurité* publiée au JORF nº 20 du 24 janvier 1995 p. 1249.

janvier 1978 relative à l'informatique, aux fichiers et aux libertés. » après modification en 2011 par la loi LOPPSI. Ainsi l'enregistrement qui permet d'identifier des personnes physiques est soumis à la loi nº 78-17 et doit être déclaré ou autorisé par la CNIL. Depuis mars 2011, la CNIL est compétente pour contrôler l'ensemble des dispositifs de vidéosurveillance sur le territoire national.

Les textes encadrant la vidéosurveillance sur la voie publique sont, outre la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et l'article 9 du Code civil, les articles L.223-1 et suivants et L.251-1 et suivants du code de la sécurité intérieure.

Dans une circulaire en date du 14 septembre 2011[1537], le Premier ministre s'appuyant sur un avis du Conseil d'État en date du 24 mai 2011[1538] remet en cause une loi du 21 janvier 1995, et supprime la déclaration préalable à la Commission nationale de l'informatique et des libertés des systèmes de vidéosurveillance qui n'intègrent pas de reconnaissance faciale, mais dont les images sont rapprochées de fichiers tiers, y compris des fichiers contenant des photographies de personnes, afin de les reconnaître[1539]. Cette même circulaire précise : « *les systèmes comportant des caméras d'enregistrement filmant des lieux non ouverts au public relèvent de la loi du 6 janvier 1978, et ainsi de la compétence de la Commission nationale de l'informatique et des libertés, lorsqu'un nombre significatif des personnes filmées sont connues de celles qui*

[1537] Circulaire du 14 septembre 2011 *relative au cadre juridique applicable à l'installation de caméras de vidéoprotection sur la voie publique et dans des lieux ou établissements ouverts au public, d'une part, et dans des lieux non ouverts au public, d'autre part*, NOR : PRMX1124533C

[1538] Conseil d'État, Section de l'intérieur - Avis nº 385.125 - 24 mai 2011, *Libertés publiques ― Ordre public – Vidéo protection – Enregistrement des images sur la voie publique et dans les lieux privés – Champs d'application respectifs de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.*

[1539] Extrait de la circulaire : « *Les systèmes de vidéo protection mis en œuvre sur la voie publique ou dans des lieux et établissements ouverts au public relèvent du régime juridique fixé par les articles 10 et 10-1 de la loi no 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité [LOPS]. L'installation de tels systèmes de vidéo protection est soumise à l'obtention d'une autorisation préfectorale prise après avis de la commission départementale de la vidéo protection, présidée par un magistrat judiciaire.*

« Par exception, le I de l'article 10 susmentionné prévoit que les systèmes dont les images sont utilisées " dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques" sont soumis à la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« Comme le précise le Conseil d'État dans un avis du 24 mai 2011, les dispositifs de vidéo protection ne relèvent de cette exception et ne doivent donc être soumis à la Commission nationale de l'informatique et des libertés - CNIL -, préalablement à leur installation, que si les traitements automatisés ou les fichiers dans lesquels les images sont utilisées sont organisés de manière à permettre, par eux-mêmes, l'identification des personnes physiques, du fait des fonctionnalités qu'ils comportent (reconnaissance faciale notamment).

« En revanche, le seul fait que les images issues de la vidéo protection puissent être rapprochées, de manière non automatisée, des données à caractère personnel contenues dans un fichier ou dans un traitement automatisé tiers (par exemple, la comparaison d'images enregistrées et de la photographie d'une personne figurant dans un fichier nominatif tiers) ne justifie pas que la CNIL soit saisie préalablement à l'installation du dispositif de vidéo protection lui-même ».

ont accès aux images. » La Commission de l'informatique et des libertés se trouve compétente pour les systèmes de vidéosurveillance dans les lieux non ouverts au public dès lors que les personnes visionnant les images connaissent les individus pouvant fréquenter lesdits lieux, mais pas pour un dispositif sur la voie publique même lors d'un rapprochement des images avec des photographies des individus. Cette particularité permet aux forces de police de rechercher des individus ciblés lors d'une manifestation sur la voie publique, mais interdit tout traitement automatique des images enregistrées pour une reconnaissance faciale de masse.

Cette précision aurait pu être établie par voie législative, la loi LOPPSI 2 du 15 mars 2011[1540] ayant modifié partiellement l'article 10 de la loi du 21 janvier 1995. Cette loi LOPPSI 2 ayant été déclarée non conforme en de nombreux articles[1541] dont certains concernant la vidéo protection, le gouvernement a certainement préféré obtenir une interprétation du Conseil d'État, moins contraignante, plutôt qu'une non-conformité à la Constitution. Le Conseil a censuré les extensions d'autorisation des installations de vidéosurveillance sur la voie publique, l'exploitation des données collectées par des personnes privées, la surveillance de la voie publique reste ainsi de la seule compétence de la police administrative.

Outre le changement de dénomination de vidéosurveillance en vidéoprotection, la loi LOPPSI 2 prévoit que les dispositifs de vidéoprotection installés sur la voie publique et dans les lieux ouverts au public sont soumis aux dispositions du code de la sécurité intérieure. Ils doivent obtenir une autorisation préfectorale, après avis d'une commission départementale présidée par un magistrat. Les dispositifs de vidéosurveillance installés dans les lieux non ouverts au public (bureaux d'une entreprise, immeubles d'habitation) sont quant à eux soumis aux dispositions de la loi du 6 janvier 1978 modifiée, dite « Informatique et Libertés ». À ce titre, ils font l'objet d'une déclaration à la CNIL[1542].

La reconnaissance faciale d'une personne physique sur la voie publique, techniquement réalisable, ne peut être réalisée que si le traitement a fait l'objet d'une déclaration à la CNIL. En 2012, la Commission de l'informatique et des libertés a autorisé la société VESALIS à

[1540] Loi n° 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure,* publiée au JORF n°0062 du 15 mars 2011 p. 4582.
[1541] Conseil constitutionnel, Décision n° 2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*.
[1542] Commission nationale de l'informatique et des libertés, *Vidéosurveillance / vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée,* 21 juin 2012, en ligne à https://www.cnil.fr/fr/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de-la-vie, consulté le 7 juillet 2017.

réaliser une expérience de reconnaissance faciale dans un stade avec des volontaires[1543], mais a entouré son autorisation du rappel que de tels traitements constituent des traitements de données biométriques soumis à un contrôle préalable particulier de la CNIL, compte tenu du caractère sensible de ce type de données.

La présence de caméras s'est généralisée, elles sont présentes dans les transports en commun, métro, RER et bus. Elles équipent les rues des grandes agglomérations. En 2015, la ville de Paris a décidé de s'équiper de 165 caméras venant s'ajouter aux 1 144 caméras existantes. Ces caméras viennent s'ajouter à celles de la RATP, de la SNCF, des musées, des enceintes sportives. Ce sont ainsi plus de 13 000 caméras qui peuvent être visionnées par la Préfecture de police[1544]. Une carte interactive permet d'indiquer les emplacements des caméras de télésurveillance dans Paris[1545]. Mais ces caméras ne font pas que de la vidéoprotection, elles peuvent aussi être utilisées pour verbaliser certaines infractions[1546].

Elles nous surveillent aussi dans les magasins. Une installation dans un lieu privé est autorisée, et ce sans autorisation préalable dès lors que la caméra ne permet pas de visionner le voisinage ou la voie publique. Dans un immeuble d'habitation en copropriété, l'installation de telles caméras est alors réalisable dès qu'elle est votée en assemblée générale des copropriétaires. Aucune sécurité n'existe alors sur le visionnage des personnes physiques qui entrent ou sortent de la copropriété, la vie privée des personnes physiques peut ainsi se trouver objet de surveillance et d'indiscrétion, seules les entrées et sorties dans les appartements sont protégées et ne peuvent pas être filmées.

La vidéosurveillance permet de savoir qu'une personne physique était présente en un lieu donné et à une date connue. Mais il existe d'autres moyens techniques de connaître la localisation d'une personne physique.

[1543] Commission nationale de l'informatique et des libertés, Délibération 2010-097 du 6 janvier 2012, disponible à l'URL : https://www.donneespersonnelles.fr/deliberations-cnil/deliberation-2010-097 consulté le 11 avril 2018.

[1544] Le Figaro.fr, « Vidéosurveillance : 165 caméras de plus à Paris », 29 septembre 2015, *Le Figaro.fr*, URL : http://www.lefigaro.fr/flash-actu/2015/09/29/97001-20150929FILWWW00351-videosurveillance-165-cameras-de-plus-a-paris.php consulté le 28 février 2018.

[1545] Disponible à l'URL : http://www.click2map.com/v2/click2map/cameras_videoosurveillance_paris, consultée le 4 octobre 2017.

[1546] Jérôme Comin, « Vidéo-verbalisation à Paris : la carte des caméras de surveillance », *20 minutes*, URL : https://www.20minutes.fr/societe/1122061-20130320-20130320-cameras-videosurveillance-verbaliser-automobilistes-a-paris consulté le 28 février 2018.

§ 2 - Géolocalisation

Les outils numériques s'ils permettent via la vidéosurveillance et la reconnaissance faciale d'identifier un individu dans l'espace public, permettent aussi de le localiser sans le voir grâce à la géolocalisation, géolocalisation des appareils communicants et géolocalisation des traces numériques[1547].

L'utilisation des moyens modernes de paiement, de contrôles d'accès laisse des traces du passage des individus à un endroit. La RATP, avec la carte Navigo, a vu la Commission de l'informatique et des libertés[1548] s'intéresser à la liberté de déplacement des usagers des transports en commun[1549]. Avec la généralisation du GPS, il est devenu aisé de connaître sa position en tout point du globe ainsi que l'itinéraire pour aller d'un point à un autre. Cette technique, initialement réservée aux militaires américains, s'est généralisée et la Chine et l'Europe développent des systèmes concurrents et compatibles avec le système américain. Des balises GPS permettent de suivre un mobile dans son déplacement, la technique est utilisée par les navigateurs pour connaître leur position plus précisément qu'avec un sextant, mais aussi pour donner leur position aux équipes chargées de les suivre à partir du continent.

Aujourd'hui, tous les smartphones sont capables de se localiser grâce à deux techniques : le GPS et la triangulation des hot spots Wi-Fi, et ils peuvent être localisés grâce à la triangulation des antennes relais utilisées pour transmettre les communications ou les données. APPLE et Google recueillent les informations de géolocalisation des smartphones utilisant leur système d'exploitation. En avril 2011, deux chercheurs en sécurité, Alasdair Allen et Pete Warden[1550], découvrent que les iPhone et iPad d'APPLE stockent les informations de localisation dans un fichier et que les données ainsi collectées sont transmises quotidiennement à APPLE. APPLE a reconnu l'existence de ce fichier, mais assure que les données transmises sont anonymes et utilisées pour améliorer les bases de géolocalisation desdits appareils. Après intervention de la CNIL, Apple a produit un correctif qui diminue la taille de cette base et permet d'arrêter la collecte en désactivant la fonction de géolocalisation.

[1547] Christophe Terrier, « La valeur des données géographiques », *L'Espace géographique*, 2011/2 (Tome 40), pp. 103-108. URL : https://www.cairn.info/revue-espace-geographique-2011-2-page-103.htm consulté le 9 janvier 2018.

[1548] Article « *Testing de la CNIL auprès de la RATP : l'exercice du droit des usagers à se déplacer anonymement n'est pas garanti* » du 6 janvier 2009, à http://www.cnil.fr/la-cnil/actu-cnil/article/article/testing-de-la-cnil-aupres-de-la-ratp-lexercice-du-droit-des-usagers-a-se-deplacer-anonymement/ consulté le 5 mai 2012.

[1549] Cf. Partie 1. Titre 1. Chapitre 1. Section 1. Sous-section 2. § 2 -A) La liberté de déplacement et la géolocalisation

[1550] Open-source application at http://petewarden.github.io/iPhoneTracker/ consultée le 7 décembre 2015.

Google avec le système Android agit de manière similaire[1551], mais la localisation ainsi obtenue est associée au compte Google du possesseur du smartphone et n'est donc pas anonyme. Il est ainsi possible via le compte Google de la personne de connaître ses déplacements en interrogeant un serveur spécifique[1552], sauf si la géolocalisation a été désactivée manuellement sur le Smartphone[1553]. Cette désactivation peut être annulée lors de l'installation d'une nouvelle application nécessitant la géolocalisation pour fonctionner, par exemple les applications de TripAdvisor ou de Uber, voire une application de prévision météorologique. Il est possible d'avoir la carte des lieux où la personne a été localisée, et en agrandissant de voir les trajets précis effectués en un lieu[1554].

Les procédés de géolocalisation du Smartphone existent à travers l'utilisation de données GPS, mais ils peuvent aussi utiliser les points d'accès Wi-Fi. Les entreprisses comme Google, collectent les coordonnées des points d'accès Wi-Fi qu'ils soient publics ou privés. Ces données sont stockées dans des bases de données et utilisées pour permettre à un appareil mobile, utilisant Android, système d'exploitation développé par Google, de se localiser avec précision. La Commission nationale de l'informatique et des libertés a infligé une amende de 100 000 euros à Google en 2011 pour non-déclaration de traitement de données et pour collecte des données de localisation Wi-Fi à l'insu des personnes concernées[1555].

Dans une étude commune CNIL-INRIA, réalisée en 2013, un tiers des applications sur smartphone accédaient aux données de géolocalisation[1556]. Durant l'été 2014, une nouvelle étude a confirmé l'intérêt d'accès aux données personnelles, dont les données de géolocalisation, par les applications pour smartphone[1557].

[1551] Tristan Nirot, *surveillance:// Les libertés au défi du numérique : comprendre et agir*, C&F éditions, 2016, pp. 14-16.

[1552] Accessible par l'URL : https://maps.google.com/locationhistory/ .

[1553] Yann Bruna, « La déconnexion aux technologies de géolocalisation. Une épreuve qui n'est pas à la portée de tous », *Réseaux*, 2014/4 (n° 186), pp. 141-161. URL : https://www.cairn.info/revue-reseaux-2014-4-page-141.htm consulté le 11 avril 2018.

[1554] Voir les exemples en Annexe 2.

[1555] Christophe Aufray, « *Géolocalisation : la Cnil inflige 100 000 euros d'amende à Google* » le 21 mars 2011 dans ZDNet.fr à http://www.zdnet.fr/actualites/geolocalisation-la-cnil-inflige-100-000-euros-d-amende-a-google-39759236.htm consulté le 5 mai 2012.

[1556] *Voyage au cœur des smartphones et des applications mobiles avec la CNIL et Inria*, 9 avril 2013, accessible à http://www.inria.fr/actualite/mediacenter/cnil-et-inria, consultée le 7 janvier 2016.

[1557] « Les données personnelles, ingrédient de base des recettes à succès sur smartphone » in *La lettre innovation et prospective de la CNIL*, n°8, novembre 2014 accessible à http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/Lettre_IP_N-8-Mobilitics.pdf, consulté le 7 janvier 2016.

Résultats généraux, comparaison entre les deux saisons	**iOS 5** (tests de novembre 2012 à janvier 2013)		**Android « Jelly Bean »** (tests de juin à septembre 2014)	
Nombre d'applications	**total : 189**		**total : 121**	
Qui communiquent sur le réseau	176	93%	80	66%
Qui accèdent à l'UDID/android	87	46%	41	34%
Qui accèdent à la géolocalisation	58	31%	29	24%
Qui accèdent au carnet d'adresses	15	8%	20	17%
Qui accèdent au calendrier	3	2%	4	3%
Qui accèdent au nom de l'appareil	30	16%	non mesuré	
Qui accèdent au nom d'opérateur	non mesuré		28	23%
Qui accèdent à l'IMEI (identité d'équipement mobile)	non mesuré		24	20%
Qui accèdent à l'adresse MAC WiFi	non mesuré		9	7%
Qui accèdent au numéro de téléphone	non mesuré		7	6%
Qui accèdent à l'identifiant de carte SIM (ICCID)	non mesuré		6	5%
Qui accèdent à la liste des points d'accès WiFi (SSID)	non mesuré		5	4%

Figure 3 Résultats généraux (source CNIL-INRIA)

Au terme de cette étude, la CNIL en déduit que « *La géolocalisation est donc, en volume, la donnée la plus collectée : elle représente à elle seule plus de 30 % des événements détectés par nos outils* »[1558], et en conclut que « *Ces accès si nombreux […] soulèvent dès lors en eux-mêmes une question de protection de la vie privée, transformant le téléphone en un instrument permanent de localisation de son propriétaire* »[1559], et que « *l'intérêt d'une amélioration en ce domaine serait important puisque les travaux de Sébastien Gambs, de l'IRISA, ou d'Yves-Alexandre de Montjoye, du MIT et de l'Université catholique de Louvain, ont notamment montré qu'une base de données de localisation permettait de déduire des informations détaillées sur les habitudes et modes de vie des personnes : lieux de vie et de travail, sorties, loisirs, mobilités, mais aussi éventuellement fréquentation d'établissements de soins ou de lieux de culte...* ». Cette géolocalisation permanente est donc, pour la CNIL, source d'atteinte à la vie privée des possesseurs de smartphones, mais au-delà du constat, la Commission de l'informatique et des libertés reste globalement impuissante et ne peut formuler qu'un souhait : « *Conformément à l'avis du G29 d'avril 2013*[1560] *concernant les applications mobiles, la CNIL souhaite que l'ensemble des acteurs de l'écosystème (éditeurs d'application, éditeurs des systèmes d'exploitation et responsables des magasins d'applications, tiers fournisseurs de*

[1558] Ibid.
[1559] Ibid.
[1560] Groupe de travail « article 29 » Avis 02/2013 sur les applications destinées aux dispositifs intelligents du G29 adopé le 27 février 2013, accessible à http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_fr.pdf accédé le 7 janvier 2016.

services et d'outils) prenne la juste mesure de leurs responsabilités respectives pour améliorer l'information et les outils de maîtrise des données personnelles. »[1561].

La Commission nationale de l'informatique et des libertés met en garde les utilisateurs de Facebook qui envisagent d'utiliser le nouveau service « *places* », la confidentialité des données personnelles ainsi collectées n'étant pas garantie[1562].

Ces moyens de géolocalisation sont utilisés par les services de police lors de recherche de personnes disparues ou de recherche d'auteurs d'agressions avec vol de téléphone portable ou de moyens de paiement.

Ces moyens sont également mis à disposition des particuliers via des sites Internet. Ainsi, un site propose un logiciel à installer sur un smartphone, logiciel qui permet de géolocaliser le smartphone, d'activer à distance son microphone, de lire les SMS reçus et émis et de connaître l'historique des appels émis et reçus à partir de ce smartphone[1563]. Ce logiciel est présenté comme un logiciel permettant de géolocaliser un smartphone dérobé, mais aussi comme un logiciel de protection et de suivi des enfants. De fait, un tel logiciel, en vente libre, est un logiciel espion qui, une fois installé sur un smartphone, permet de surveiller à son insu le porteur de l'appareil, même en dehors de son utilisation effective.

La géolocalisation des moyens de communication peut aussi être utilisée lors d'enquêtes. En 2010, la Cour européenne des droits de l'homme a retenu l'applicabilité de l'article 8 de la Convention en matière de géolocalisation[1564]. En s'appuyant sur cet arrêt, le 22 octobre 2013, la Cour de cassation[1565] a considéré que la technique de géolocalisation constitue une ingérence dans la vie privée au titre de l'article 8 de la Convention européenne des droits de l'homme, et qu'à ce titre, elle doit être exécutée sous le contrôle d'un juge. Le même jour, la Cour de cassation[1566] a considéré que l'ingérence de l'autorité publique dans la vie privée se doit d'être effectuée non pas sous le contrôle du Procureur de la République, magistrat dépendant à l'égard

---

[1561] CNIL, Article *Mobilitics, saison 2 : nouvelle plongée dans l'univers des smartphones et de leurs applications*, 15 décembre 2014, à http://www.cnil.fr/linstitution/actualite/article/article/mobilitics-saison-2-nouvelle-plongee-dans-lunivers-des-smartphones-et-de-leurs-applications/?tx_ttnews%5BbackPid%5D=91&cHash=497ed7bf0a1b668cf702e2cfb41dbf99 consulté le 7 janvier 2016.

[1562] « La CNIL met en garde contre le service de géolocalisation de Facebook » dans *Le Monde.fr* du 20 octobre 2010 à http://www.lemonde.fr/technologies/article/2010/10/20/la-cnil-met-en-garde-contre-le-service-de-geolocalisation-de-facebook_1428569_651865.html consulté le 5 mai 2012

[1563] Sur le site Spytic.fr, consulté le 5 mai 2012

[1564] Cour Européenne des Droits de l'Homme, 5e Section, 2 septembre 2010, *Uzun c/ Allemagne*, Requête nº 35623/05

[1565] Cour de cassation, criminelle, Chambre criminelle, 22 octobre 2013, 13-81.945, Publié au bulletin

[1566] Cour de cassation, criminelle, Chambre criminelle, 22 octobre 2013, 13-81.949, Publié au bulletin

des autorités publiques, mais sous le contrôle d'un juge judiciaire, indépendant vis-à-vis des autorités publiques. À la suite de ces deux arrêts, les opérations de géolocalisation effectuées sous le contrôle d'un procureur sont interrompues, mais les enquêtes diligentées sous le contrôle d'un juge d'instruction se poursuivent. Cette situation a amené le gouvernement à faire voter la loi sur la géolocalisation[1567]. Cette loi permet à un officier de police judiciaire de mettre en place une procédure de géolocalisation dans le cadre d'une enquête de flagrance, d'une enquête préliminaire sur autorisation du procureur de la République pour une durée maximale de quinze jours, au-delà de ce délai, sur demande du procureur, le juge des libertés peut l'autoriser pour une durée d'un mois renouvelable. Dans le cadre d'une instruction, le juge d'instruction peut autoriser une telle procédure pour une durée de quatre mois, renouvelable.

La géolocalisation ne concerne pas que les smartphones, elle peut aussi concerner les véhicules automobiles utilisés tant à titre privé qu'à titre professionnel[1568]. Les dispositifs GPS conservent également dans leur mémoire les divers trajets réalisés et les positions des endroits parcourus même sans activer le programme de guidage. La Commission de l'informatique et des libertés a émis des conditions d'utilisation des logiciels de géolocalisation par données GSM ou GPS dans le cadre professionnel[1569].

Dans le cadre du travail, les dispositifs de géolocalisation peuvent être utilisés pour l'optimisation des tournées de livraison ou pour une meilleure gestion de la flotte d'entreprise, mais ces dispositifs doivent être déclarés à la Commission de l'informatique et des libertés et

[1567] Loi nº 2014-372 du 28 mars 2014 *relative à la géolocalisation* publiée au JORF nº0075 du 29 mars 2014 p. 6123.

[1568] Un dispositif d'appel d'urgence avec géolocalisation doit équiper tous les véhicules neufs en 2018 (Cécilia Beaudoin, « Automobile : le système d'urgence embarqué bientôt obligatoire », 5 avril 2018, *Radins.com,* URL : https://www.radins.com/actualites/automobile-le-systeme-durgence-embarque-bientot-obligatoire,40875.html consulté le 13 avril 2018).

[1569] Fiche pratique Commission nationale de l'informatique et des libertés, « Les dispositifs de géolocalisation GSM/GPS », URL : http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/les-dispositifs-de-geolocalisation-gsmgps/ consulté le 5 mai 2012.

les employés doivent être informés de l'utilisation de ces dispositifs[1570] et ceux-ci ne peuvent être utilisés dans un but de surveillance permanente[1571].

Dans le cas de véhicules professionnels, la Cour de cassation[1572] a estimé que l'installation d'un dispositif de géolocalisation dans le véhicule d'un salarié ayant une liberté dans l'organisation de ses déplacements n'est pas justifiée, et a rappelé qu'un système de géolocalisation ne peut être utilisé par un employeur que pour les finalités déclarées auprès de la Commission nationale de l'informatique et des libertés et portées à la connaissance des employés. En 2010, la cour d'appel de Dijon[1573] a condamné un employeur qui avait licencié un employé en s'appuyant sur les données d'un système de géolocalisation pour prouver l'utilisation dudit véhicule à titre personnel par l'employé, alors que le dispositif n'avait ni été déclaré à la CNIL, ni fait l'objet d'une information auprès des employés.

Concernant les véhicules individuels, le 22 juillet 2014, la Commission de l'informatique et des libertés a sanctionné une société de location de véhicules[1574] qui avait installé un système de géolocalisation des véhicules loués, dispositif fonctionnant 24 h/24 7jours/7, sans possibilité de paramétrage ou d'arrêt. Le gérant de la société pouvait ainsi connaître à tout moment la localisation de ses véhicules. La sanction, une amende de 5 000 euros a été rendue sur le

---

[1570] La CNIL précise dans la note « *La géolocalisation des véhicules des salariés* » en date du 29 décembre 2015 : « *Des dispositifs de géolocalisation peuvent être installés dans des véhicules utilisés par des employés pour :*

- *Suivre, justifier et facturer une prestation de transport de personnes, de marchandises ou de services directement liée à l'utilisation du véhicule. Par exemple : les ambulances dans le cadre de la dématérialisation de la facturation de l'assurance maladie.*
- *Assurer la sécurité de l'employé, des marchandises ou des véhicules dont il a la charge, et notamment retrouver le véhicule en cas de vol. Par exemple, avec un dispositif inerte activable à distance à compter du signalement du vol.*
- *Mieux allouer des moyens pour des prestations à accomplir en des lieux dispersés, notamment pour des interventions d'urgence. Par exemple : identifier l'employé le plus proche d'une panne d'ascenseur ou l'ambulance la plus proche d'un accident.*
- *Accessoirement, suivre le temps de travail, lorsque cela ne peut être réalisé par un autre moyen.*
- *Respecter une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés.*
- *Contrôler le respect des règles d'utilisation du véhicule définies par l'employeur* ».

[1571] Dans la même note, la CNIL ajoute que ces dispositifs ne doivent pas être utilisés pour :

- « *Pour contrôler le respect des limitations de vitesse.*
- *Pour contrôler un employé en permanence* ».

[1572] Cour de cassation, civile, chambre sociale, 3 novembre 2011, 10-18.036, Publié au bulletin.

[1573] Relaté par CNIL, *Article Géolocalisation des véhicules : la justice condamne un employeur qui n'a pas suivi les règles « informatique et libertés »,* 25 octobre 2010, URL : http://www.cnil.fr/linstitution/actualite/article/article/geolocalisation-des-vehicules-la-justice-condamne-un-employeur-qui-na-pas-suivi-les-regles-i/ consulté le 7 janvier 2016.

[1574] CNIL, *Délibération de la formation restreinte n° 2014-294 du 22 juillet 2014 prononçant une sanction pécuniaire publique à l'encontre de la société X*, disponible à l'URL : http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D_2014-293-sanction_LOC_CAR_DREAM.pdf consultée le 7 janvier 2016.

fondement du caractère excessif des données au regard des finalités pour lesquelles elles sont collectées et traitées. La sanction a été rendue publique.

Sous-section 2. Les interceptions de communications privées

Outre la vidéosurveillance et la géolocalisation, il est possible de surveiller un individu en interceptant ses communications privées qui ont maintenant pratiquement toujours lieu sous forme numérique, qu'il s'agisse des communications orales via le téléphone ou via des applications comme SKYPE ou WhatsApp. Les communications écrites sont réalisées par des messages courts, SMS ou MMS, ou des courriels, voire les CHAT, hybrides des communications orales et écrites. La correspondance privée a toujours été protégée par la loi[1575].

§ 1 - La protection des communications privées

Les courriers papier sont facilement protégeables, par sceaux ou autres procédés de cryptage, et le détournement de correspondance est défini et sanctionné pénalement[1576]. À l'ère du numérique, la correspondance papier devient marginale et les échanges de messages se font via les messageries électroniques (*e-mail*), les réseaux sociaux ou les messages courts (*SMS* ou TEXTO®). Les échanges par voie de télécommunication sont assimilés à la correspondance privée subissant par conséquent la même protection. En effet, dès lors qu'un message est exclusivement destiné à une ou plusieurs personnes déterminées et individualisées, il est susceptible de protection, peu importe le procédé de communication. Les échanges téléphoniques entrent donc également dans la correspondance privée.

La loi relative au secret des correspondances émises par la voie des communications électroniques[1577] rappelle dès son article 1 : « *Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et*

[1575] Code des postes et des communications électroniques.
[1576] Code pénal, Articles 226-15 et 432-9 et code des postes et des communications électroniques, Article L.33-1.
[1577] Loi nº 91-646 du 10 juillet 1991 *relative au secret des correspondances émises par la voie des communications électroniques*, publiée au JORF nº162 du 13 juillet 1991 p. 9167.

dans les limites fixées par celle-ci. ». Elle précise les conditions dans lesquelles une interception peut avoir lieu soit pour des raisons judiciaires[1578] soit pour des raisons de sécurité[1579].

Seules les informations relatives à l'objet de la procédure peuvent faire l'objet d'une transcription par une personne habilitée. Les informations non liées à l'objet de la procédure doivent être occultées, mais dans les faits, la personne habilitée y a accès et les lit même si leur retranscription pour la procédure n'est pas réalisée. La Cour de cassation a rappelé que le tri des pièces est assuré par des enquêteurs tenus au secret professionnel et que seule est prohibée l'utilisation de pièces non liées à la procédure[1580].

La convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950 rappelle en son article 8, « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». La France a été condamnée pour absence de base légale à une interception de conversation au moyen de dispositifs d'écoute installés dans une propriété privée[1581]. La loi Perben II[1582] a légalisé cette pratique ultérieurement.

L'Union européenne a complété la directive 95/46/CE par la directive 2002/58/CE[1583] concernant la vie privée et les communications électroniques, et considère que « *les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance.* » La directive inclut donc les métadonnées relatives aux communications dans son champ de protection. La directive 97/66[1584] fait obligation aux États membres de garantir « *au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un*

[1578] Code de procédure pénale, Sous-section I : Des transports, des perquisitions et des saisies, Article 97 et Sous-section II : Des interceptions de correspondances émises par la voie des télécommunications, Articles 100 à 100-7

[1579] Recherche des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées.

[1580] Cour de cassation, Chambre criminelle, 29 juin 2011 nº 10-85.479, *Affaire Schoering-Plough — DGCCRF.*

[1581] Cour européenne des droits de l'homme, 31 mai 2005, nº 59842/00, *Vetter c/ France*.

[1582] Loi nº 2004-204 du 9 mars 2004 *portant sur l'adaptation de la justice aux évolutions de la criminalité* publiée au JORF nº59 du 10 mars 2004 p. 4567.

[1583] 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*, Journal officiel nº L 201 du 31/07/2002 pp. 37–0047.

[1584] Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications,* publiée au JOCE L24 du 30 janvier 1998 p. 1.

réseau public de télécommunications ou de services de télécommunications accessible au public. En particulier, [les États membres] interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées ». Cette directive a été transposée en droit français par ordonnance et décrets[1585].

En Belgique, la protection des correspondances privées est inscrite dans la Constitution[1586].

§ 2 - Les interceptions étatiques, légalisées ou non légalisées

Techniquement, les messages, contenu et métadonnées, sont stockés sur un support informatique par l'entité qui fournit le service de correspondance, ainsi que les prestataires qui en assurent l'acheminement. Ces fichiers ne sont pas tous gérés sur le territoire de l'Union européenne, ils peuvent se retrouver sur des serveurs situés en Amérique du Nord, voire dans des pays autres disposant d'une législation plus permissive. Avec l'informatique en nuage (*cloud computing*), la localisation des données et des traitements devient de plus en plus difficile à contrôler[1587].

Si en France ou dans l'Union européenne, les textes protègent les personnes physiques contre les abus de violation de leur correspondance privée, les interceptions et saisies étant encadrées par la loi, certains États n'ont pas un arsenal juridique aussi protecteur. En 2010, l'Arabie saoudite et les Émirats Arabes Unis ont décidé de suspendre les services des BlackBerry[1588], exigeant de pouvoir surveiller les communications électroniques des téléphones multimédias

---

[1585] Textes de transposition : Ordonnance n° 2001-670 du 25 juillet 2001 *portant adaptation au droit communautaire du code de la propriété intellectuelle et du code des postes et télécommunications* publiée au JORF n°173 du 28 juillet 2001 p. 12132 ; Décret n° 2002-36 du 8 janvier 2002 *relatif à certaines clauses types des cahiers des charges annexés aux autorisations délivrées en application de l'article L.33-1 du code des postes et télécommunications* publié au JORF n°8 du 10 janvier 2002 p. 585 ; Décret n° 2003-752 du 1er août 2003 relatif aux annuaires universels et aux services universels de renseignements et modifiant le code des postes et télécommunications publié au JORF n°180 du 6 août 2003 p. 13581 ; Décret n° 2003-755 du 1er août 2003 *modifiant le code des postes et télécommunications* publié au JORF n°180 du 6 août 2003 p. 13584.

[1586] Constitution Belge, article 29 : « *Le secret des lettres est inviolable.*
« La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste. »

[1587] Gustavo Gomez Mejia, « De quoi le "nuage" est-il le nom ? Le statut des supports face aux régimes du *cloud computing* », *Communication & langages*, 2014/4 (N° 182), pp. 77-93. URL : https://www.cairn.info/revue-communication-et-langages1-2014-4-page-77.htm consulté le 9 janvier 2018.

[1588] Margaux Bergey, « L'Arabie Saoudite bannit la messagerie du BlackBerry », 4 août 2010, *Le Figaro.fr,* URL : http://www.lefigaro.fr/international/2010/08/03/01003-20100803ARTFIG00581-le-blackberry-coupe-en-arabie-saoudite-des-vendredi.php consulté le 9 janvier 2018.

du fabricant canadien *Research in Motion* (RIM). RIM affirme alors n'accorder aucune dérogation à son système de cryptage[1589].

L'Inde a également menacé RIM d'interdire certains services des appareils de RIM[1590], évoquant des questions de sécurité nationale et la difficulté d'un « monitoring du BlackBerry ». Ce dernier a toujours été opposé à cette collaboration pour le moins ambiguë, mais en 2012, il a finalement fait machine arrière. RIM accepte d'installer un serveur BlackBerry à Bombay, un des pôles économiques du pays. À terme, ce serveur doit être en mesure de fournir aux autorités indiennes des données susceptibles d'être impliquées dans des dossiers juridiques. Selon les agences de sécurité indienne, le dispositif de cryptage de BBM (*BlackBerry Messenger*) était une contrainte majeure, attendu qu'elle ne leur permettait pas d'intercepter des communications sur leur territoire, ce qui semblerait représenter un risque pour la sécurité nationale[1591]. La sécurité du système de RIM n'est pas absolue, car déjà, au Canada, si les autorités policières sont munies d'un mandat, RIM est tenu de fournir les messages cryptés visés par ce mandat[1592]. RIM est une société de droit canadien. Mais, le cas canadien reste dans la légalité de la protection des correspondances personnelles, un mandat est nécessaire et le gouvernement ne dispose pas des clés de décryptage.

L'accès aux autres messageries instantanées ou non, par les gouvernements reste posé et semble aujourd'hui laissé à la discrétion des opérateurs Google, Yahoo! ou autres. Ces sociétés étant des sociétés américaines de droit américain, souvent californien, et la protection des données personnelles avec le *USA Patriot Act*[1593] étant moins stricte qu'en Europe, le secret de ces messageries a été mis en cause par les révélations d'Edward Snowden.

Au niveau européen, la directive 2006/24/CE[1594] impose aux opérateurs une rétention des données de connexion de plusieurs mois, entre 6 mois et vingt-quatre mois, afin de pouvoir

---

[1589] François Pitti, « La diplomatie économique des entreprises », *Géoéconomie*, 2011/1 (n° 56), p. 105-118. URL : https://www.cairn.info/revue-geoeconomie-2011-1-page-105.htm consulté le 11 avril 2018.

[1590] Damien Leloup, « Cryptage du BlackBerry : RIM cherche un compromis en Inde », 4 aout 2010, *Le Monde.fr Technologies,* URL : http://www.lemonde.fr/technologies/article/2010/08/04/cryptage-du-blackberry-rim-cherche-un-compromis-en-inde_1395127_651865.html consulté le 9 janvier 2018.

[1591] Article du 21 février 2012 sur http://www.journaldugeek.com/2012/02/21/rim-se-plie-aux-exigences-de-linde-et-autorise-lacces-aux-donnees-des-utilisateurs/, consulté le 5 mai 2012.

[1592] Article du 5 janvier 2012 sur http://blogues.radio-canada.ca/surleweb/2012/01/05/le-cryptage-du-blackberry-perce-par-des-policiers-probablement-pas/, consulté le 5 mai 2012.

[1593] USA Patriot Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to intercept and Obstruct Terrorism Act*) du 26 octobre 2001.

[1594] 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* publiée au Journal officiel de l'Union européenne L 105/54 du 13 avril 2006.

répondre aux sollicitations des forces de police dans le cas d'enquêtes judiciaires. Cette directive a été transposée[1595] dans le droit français avec une durée de rétention d'un an. Cette directive a été jugée non conforme aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et la Cour de justice de l'Union européenne l'a invalidée[1596]. Les législations nationales ayant transposé cette directive restent cependant valides.

La lutte contre le terrorisme a entraîné la promulgation de lois qui autorisent les interceptions de communications sur les réseaux électroniques ainsi que les écoutes des conversations[1597], rendant ainsi le secret des communications moins efficace et opérant. Cette lutte est en conflit avec la défense des libertés mais est aussi contrainte par les évolutions techniques permanentes.

[1595] Décret n° 2006-358 du 24 mars 2006 *relatif à la conservation des données des communications électroniques* publié au JORF n°73 du 26 mars 2006 p. 4609.

[1596] Cour de justice de l'Union européenne, 8 avril 2017, Arrêt dans les affaires jointes C-293/12 et C-594/12 *Digital Rights Ireland et Seitlinger e. a.*

[1597] Partie 1. Titre 2. Chapitre 2. Section 2. Sous-section 1. § 1 - La surveillance des individus à leur insu.

Section 2. La course inégale entre la législation et la technique

La défense des libertés est effective dans notre droit positif depuis quelques années, cette défense initialisée au siècle des Lumières, a vu ses premières concrétisations avec la Révolution française et la Déclaration des droits de l'homme et du citoyen. Ces libertés ont été ensuite oubliées avec la Terreur et les régimes qui lui ont succédé. Il a fallu attendre la troisième République pour voir les premières lois protégeant les libertés, lois qui nous sont parvenues et sont toujours efficaces. Durant la Seconde Guerre mondiale, l'Europe a vu ces libertés réduites, les arrestations arbitraires, les privations de liberté voire les exterminations sont devenues la loi. Depuis 1945, l'Europe connaît des régimes démocratiques et a instauré des mécanismes de protection des libertés efficaces. Il aura fallu environ deux siècles entre la proclamation des libertés comme droit universel de l'humanité et la mise en œuvre opérationnelle et légale de la protection de ces libertés.

Aujourd'hui, le développement des techniques numériques peut remettre en question cette protection. En 1946, au lendemain de la Seconde Guerre mondiale, le premier calculateur électronique programmable était annoncé. Ce calculateur nécessitait plusieurs jours pour sa programmation et n'effectuait que 1 000 multiplications par seconde. Dans les années 1970, les premiers calculateurs universels sont apparus et l'informatique est entrée dans les sociétés industrielles et commerciales. Les données étaient souvent stockées sur des bandes magnétiques qui obligeaient à lire séquentiellement ces supports et à les réécrire sur une seconde bande en cas de modification. Dans les années 1980, les premiers ordinateurs personnels sont apparus, leur unité de stockage était une disquette souple. Ces ordinateurs personnels ne pouvaient pas communiquer entre eux. À cette époque la Direction générale des Télécommunications va pourtant lancer les projets Annuaire électronique et Télétel. Les progrès des télécommunications et l'accroissement de puissance des calculateurs ainsi que les nouvelles capacités de stockage des données vont permettre vers 1995 d'ouvrir Internet dans les pays nord-américains et en Europe occidentale. Ce sera alors la naissance des moteurs de recherche, des réseaux sociaux et des techniques de communication et de téléchargement et streaming[1598].

[1598] Pour un survol de l'histoire de l'informatique, lire, par exemple, Yannis Delmas-Rigoutsos, *Histoire de l'informatique, d'Internet et du Web,* 28 août 2014, en ligne à l'URL : https://delmas-rigoutsos.nom.fr/documents/YDelmas-histoire_informatique.pdf consulté le 11 avril 2018.

Après ces innovations, l'Internet des objets est apparu et est en train de se généraliser. À terme, Internet va connecter les humains et les objets dans un réseau globalisé[1599]. Devant une telle évolution de la technique, il devient difficile au législateur de protéger les libertés face aux nouvelles opportunités techniques. Les moyens techniques permettent une surveillance et un fichage des individus aux limites de la légalité qui reste toujours en retard par rapport à l'évolution rapide des techniques.

Sous-section 1. Des moyens numériques détournés pour des besoins de sécurité

La technique numérique peut être intrusive et difficilement décelable, aussi son utilisation pour la surveillance des personnes physiques ou des groupes d'individus doit être encadrée par la loi afin de s'opposer à l'arbitraire d'une administration tentaculaire dans une société sécuritaire[1600]. En 1906, Jean Cruet écrit[1601] : « *Ni les lois révolutionnaires ni les lois postérieures n'ont déterminé avec une rigoureuse précision les limites du droit individuel, de l'activité privée à l'égard de l'autorité gouvernementale, et souvent même la loi n'est intervenue que pour consacrer le pouvoir discrétionnaire de l'administration.*

« En d'autres termes, malgré le progrès rapide accompli depuis l'établissement définitif du régime démocratique en France, le législateur n'a pas transformé en véritables droits, juridiquement reconnus, juridictionnelle ment garantis, et par conséquent opposables à l'administration, les libertés essentielles de l'individu.

« Certes, la loi ne peut tout prévoir et tout dire, et si elle parvenait à supprimer d'une manière absolue l'arbitraire dans les rapports de l'administration et des administrés, elle réduirait la fonction administrative à l'application automatique de textes rigides, s'adaptant mal aux

[1599] Benhamou Bernard, « L'Internet des objets. Défis technologiques, économiques et politiques », *Esprit*, 2009/3 (Mars/avril), pp. 137-150. URL : https://www.cairn.info/revue-esprit-2009-3-page-137.htm consulté le 10 janvier 2018.

[1600] Zygmunt Bauman, Didier Bigo, Paulo Esteves *et al.*, « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », *Cultures & Conflits*, 2015/2 (n° 98), pp. 133-166. URL : https://www.cairn.info/revue-cultures-et-conflits-2015-2-page-133.htm consulté le 9 janvier 2018.

[1601] Jean Cruet, *Étude juridique de l'arbitraire gouvernemental et administratif, des cas où l'autorité gouvernementale et administrative n'est pas tenue, sous des sanctions efficaces, de respecter les droits individuels et la légalité*, éditions Arthur Rousseau, 1 906, Introduction p. 6.

circonstances de temps et de fait. L'arbitraire, dans une certaine mesure, c'est la liberté de l'administration.
« Mais il ne convient pas que la liberté de l'administration puisse porter atteinte aux libertés des administrés. »

Ainsi, au début du 20e siècle, la toute-puissance de l'administration était source d'incertitude et de risque pour la liberté individuelle. À cette époque, les techniques utilisées restaient des techniques classiques manuelles, les fichiers consistaient en un classement de fiches[1602] individuelles, manuscrites. La surveillance des individus était réalisée par recoupement de témoignages ou par filature et surveillance, voire par délation. Cette surveillance nécessitait la coopération de plusieurs personnes. Aujourd'hui, les techniques utilisées permettent de s'introduire dans la vie privée des individus à leur insu, de façon furtive et discrète, sans traces visibles ou perceptibles, et d'enregistrer automatiquement les informations collectées[1603]. Cette décision de surveillance relève du pouvoir réglementaire depuis les législations de lutte contre la grande criminalité et le terrorisme, le pouvoir judiciaire, garant constitutionnel des libertés individuelles, étant limité à la liberté d'aller et venir et à la sûreté[1604].

§ 1 - La surveillance des individus à leur insu

La surveillance d'un individu ou d'un groupe d'individus est facilitée par les techniques numériques grâce aux traces laissées par toute activité numérique[1605]. La loi LOPPSI sur la sécurité autorise la surveillance des ordinateurs, contenu et échanges. La police peut s'introduire discrètement chez les suspects pour installer des logiciels de captation de données[1606]. Pour le gouvernement, ce n'est qu'une modernisation des écoutes téléphoniques.

[1602] D'où le mot fichier désignant un ensemble de fiches ou d'enregistrements.
[1603] François-Bernard Huyghe, « Des écoutes aux interceptions électroniques », dans *Les écoutes téléphoniques.* Paris, Presses Universitaires de France, « Que sais-je ? », 2009, pp. 11-43. URL : https://www.cairn.info/les-ecoutes-telephoniques--9782130579519-page-11.htm consulté le 9 janvier 2018.
[1604] Jacques Perriault, « Traces numériques personnelles, incertitude et lien social », *Hermès, La Revue*, 2009/1 (n° 53), pp. 13-20. URL : https://www.cairn.info/revue-hermes-la-revue-2009-1-page-13.htm consulté le 9 janvier 2018.
[1605] Cf. Partie 2. Titre 1. Chapitre 1. Section 2. Sous-section 1. § 1 -Les traces personnelles
[1606] Code de procédure pénale, livre IV titre XXV chapitre II Section 6 bis « *De la captation des données informatiques*
« Art. 706-102-1. − Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent

Les personnes visées par cette surveillance sont les terroristes présumés, mais aussi toutes les personnes suspectées de crimes en « bande organisée », qu'il s'agisse de vols, de trafic de drogue, de proxénétisme ou encore d'aide à l'immigration clandestine.

Pour installer les dispositifs de captation des données et des échanges, la police peut discrètement s'introduire au domicile du suspect, dans sa voiture ou dans n'importe quel autre local, et à toute heure (sans les limites imposées aux perquisitions qui ne sont autorisées, hors affaires de terrorisme, qu'entre 6 heures et 21 heures)[1607]. La loi ne précise pas les outils informatiques utilisés (« cheval de Troie », surveillance en amont au niveau du fournisseur d'accès, boîtes noires ...). La surveillance peut durer quatre mois, mais elle peut être renouvelée pour les besoins de l'enquête. L'opération ne peut être menée que par des officiers de police judiciaire, elle doit être autorisée par un juge d'instruction et dûment motivée. Si elle est menée au domicile du suspect, une autorisation d'un juge des libertés et de la détention est également nécessaire. Les informations sur la vie privée qui ne concernent pas l'enquête ne peuvent pas être conservées. Comme pour les écoutes téléphoniques, les avocats, les magistrats et les parlementaires sont protégés[1608]. La loi prévoit ainsi des garde-fous autour de cette surveillance

sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction ».

[1607] Code de procédure pénale, livre IV titre XXV chapitre II Section 6 bis « *De la captation des données informatiques*

« Art. 706-102-5. − En vue de mettre en place le dispositif technique mentionné à l'article 706-102-1, le juge d'instruction peut autoriser l'introduction dans un véhicule ou dans un lieu privé, y compris hors des heures prévues à l'article 59, à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur celui-ci. S'il s'agit d'un lieu d'habitation et que l'opération doit intervenir hors des heures prévues à l'article 59, cette autorisation est délivrée par le juge des libertés et de la détention, saisi à cette fin par le juge d'instruction. Ces opérations, qui ne peuvent avoir d'autre fin que la mise en place du dispositif technique, sont effectuées sous l'autorité et le contrôle du juge d'instruction ».

[1608] Code de la sécurité intérieure, « *Art. L.821-7. – Un parlementaire, un magistrat, un avocat ou un journaliste ne peut être l'objet d'une demande de mise en œuvre, sur le territoire national, d'une technique de recueil de renseignement mentionnée au titre V du présent livre à raison de l'exercice de son mandat ou de sa profession* ».

légale, la loi sur le renseignement[1609] précise les limites légales du recueil d'informations[1610], mais les contrôles peuvent s'avérer insuffisants[1611].

L'interception peut aussi se faire en amont, au niveau des fournisseurs d'accès Internet. Tout comme en matière d'écoute téléphonique, il était possible d'installer un microémetteur dans le téléphone ou une « jarretière » au niveau du central téléphonique, en matière numérique, la pose de logiciels espions au niveau des nœuds d'accès du fournisseur d'accès Internet est possible[1612]. Dans ce cas, le domicile de la personne à surveiller n'a pas à être investi et il ne devient plus nécessaire de faire une demande à un juge des libertés et de la détention. Il reste à la personne surveillée la possibilité dans ce cas de se connecter à un point d'accès Wi-Fi d'un voisin pour que les communications ne soient pas interceptées, tout comme une personne mise sous écoute téléphonique pouvait aller téléphoner dans une cabine téléphonique publique ou utiliser un téléphone portable à carte prépayée.

Tout opérateur de services de télécommunications est tenu de mettre en place les moyens nécessaires pour intercepter les communications échangées sur un réseau public[1613]. Une interception légale peut être mise en place pour collecter deux grandes catégories d'informations. La première catégorie concerne le « quoi », c'est-à-dire le contenu des communications (une conversation entre deux personnes, le contenu de mails, d'une session de messagerie instantanée ou encore des fichiers). La seconde catégorie concerne plus le « qui », c'est-à-dire les numéros appelés, les appels ayant abouti et ceux n'ayant pas débouché sur une

---

[1609] Loi nº 2015-912 du 24 juillet 2015 *relative au renseignement*, publiée au JORF du 26 juillet 2015.

[1610] « *L'autorisation et la mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres Ier à III du titre V du présent livre [Code de la sécurité intérieure, livre VIII intitulé : « Du renseignement »] ne peuvent être décidées que si :*
« 1º Elles procèdent d'une autorité ayant légalement compétence pour le faire ;
« 2º Elles résultent d'une procédure conforme au titre II du même livre ;
« 3º Elles respectent les missions confiées aux services mentionnés à l'article L.811-2 ou aux services désignés par le décret en Conseil d'Etat prévu à l'article L.811-4 ;
« 4º Elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L.811-3 ;
« 5º Les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués.
« La Commission nationale de contrôle des techniques de renseignement s'assure, dans les conditions prévues au présent livre, du respect de ces principes. Le Conseil d'Etat statue sur les recours formés contre les décisions relatives à l'autorisation et à la mise en œuvre de ces techniques et ceux portant sur la conservation des renseignements collectés ».

[1611] Jean-Claude Paye, « Lutte antiterroriste et contrôle de la vie privée », *Multitudes*, 2003/1 (nº 11), pp. 91-105. URL : https://www.cairn.info/revue-multitudes-2003-1-page-91.htm consulté le 9 janvier 2018.

[1612] Andro Milanović, Siniša Srbljić, Ivo Ražnjević, Darryl Sladden, Ivan Matošević, and Daniel Skrobo, *Methods for Lawful Interception in IP Telephony Networks Based on H.323,* EUROCON 2003 Ljubljana, Slovenia

[1613] Jean-François Audenard, « Interceptions légales : Retour aux bases » in *Les blogs Orange Business* à http://blogs.orange-business.com/securite/2010/11/interceptions-legales-retour-aux-bases.html consulté le 30 avril 2012

conversation, ce sont des informations dites de « signalisation » ou métadonnées. Ces interceptions d'échanges dans le cas d'enquêtes concernant le terrorisme, la pédophilie, la cybercriminalité, l'espionnage, sont autorisées au niveau européen et en particulier par les articles 20 et 21 de la convention sur la cybercriminalité de Budapest[1614], ratifiée par la France le 10 janvier 2006.

L'interception des échanges permet de collecter les données donc des informations qui peuvent avoir un caractère personnel[1615]. La technique du cheval de Troie permet aussi de scanner le contenu des disques et de le transférer vers un site extérieur[1616]. Ainsi, une fois posé et installé, le logiciel de captation peut retrouver des informations passées et stockées dans la mémoire de l'ordinateur, mais aussi surveiller tous les nouveaux échanges à venir. La découverte de données concernant un acte délictuel, non en rapport avec l'enquête pour laquelle le dispositif a été posé, peut être retenue contre le propriétaire de l'ordinateur et provoquer une incrimination nouvelle, découverte par le dispositif[1617].

Mais, ces techniques légales peuvent être détournées et utilisées pour des usages illégaux ou frauduleux. La technique utilisée n'est de fait que celle utilisée par les pirates pour attaquer des ordinateurs. Seule la technique de pose peut différer. Dans le cadre légal de la loi LOPPSI 2[1618], les forces de l'ordre, officiers de police judiciaire ou gendarmes, peuvent s'introduire dans les locaux privés pour installer le logiciel, sans que cela ne soit une violation de domicile, alors que la pose de tels dispositifs par des pirates est réalisée par envoi de messages d'amorce qui, lors de leur ouverture par l'utilisateur de l'ordinateur, vont activer la mise en place du logiciel *spyware*. La loi ne précise pas le moyen utilisé par les forces de police ou de gendarmerie pour mettre en place le dispositif de captation : installation après intrusion au domicile ou via le réseau par les techniques utilisées par les hackers. Ainsi, ce sont bien des techniques utilisées par les cybercriminels qui sont mises à la disposition légale des forces de l'ordre, protégées des incriminations pénales par l'immunité que leur confère la loi.

[1614] Conseil de l'Europe*, Convention sur la cybercriminalité, STCE n° 185* Budapest, 23 novembre 2001.

[1615] Sylvia Preuss-Laussinotte, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *Cultures & Conflits* [En ligne], 64 | hiver 2006, mis en ligne le 06 mars 2007, consulté le 11 avril 2018. URL : http://journals.openedition.org/conflits/2133.

[1616] Internet dispose de nombreux sites décrivant la technique pour espionner un ordinateur, à titre d'exemple : Julien Paignau, « Comment espionner un ordinateur connecté au Web à distance », 26 mai 2014, *Guide comparatif : logiciel espion Pc / Mac et keylogger*, Master Keylogger, URL : http://www.masterkeylogger.com/comment-espionner-ordinateur-a-distance/ consulté le 9 janvier 2018.

[1617] Code procédure pénale, Art. 76 « […] *le fait que ces opérations révèlent des infractions autres que celles visées dans la décision ne constitue pas une cause de nullité des procédures incidentes* ».

[1618] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation *pour la performance de la sécurité intérieure* publiée au JORF n°0062 du 15 mars 2011 page 4582

Les écoutes téléphoniques restent un moyen de surveillance des individus suspectés d'activité criminelle ou terroriste. La numérisation de la technique téléphonique, GSM ou VOiP, met en œuvre des techniques analogues à la captation des données informatiques : captation des métadonnées permettant de savoir qui appelle ou qui est appelé, ou captation des données échangées permettant de connaître le contenu des informations échangées.

§ 2 - L'infiltration et l'immunité de la faute pénale

La loi LOPPSI 2 permet également aux forces de sécurité d'usurper l'identité d'une personne ou d'utiliser une identité fictive, un alias, pour infiltrer un réseau terroriste ou criminel, ces agissements pénalement répréhensibles font alors également l'objet d'une immunité pénale[1619]. Un service spécialisé sous le contrôle du ministère de l'Intérieur peut donc infiltrer un groupe soupçonné de terrorisme, d'apologie du terrorisme ou d'atteinte à la sécurité de l'État, afin de capter des informations ou des données permettant d'obtenir des preuves des agissements supposés. Les officiers de police judiciaire ayant ainsi infiltré un groupe de suspects peuvent participer à leur activité pénalement répréhensible pour collecter des preuves, tout en bénéficiant pour leurs actes propres de l'immunité conférée par la loi.

La seule restriction apportée par le texte est que ces actes ne doivent pas constituer une incitation à commettre lesdites infractions[1620], restriction qui n'existe pas dans la loi américaine.

[1619] Code de procédure pénale, Article 706-25-2 : « *Dans le but de constater les infractions mentionnées au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsable :*
« 1º Participer sous un pseudonyme aux échanges électroniques ;
« 2º Être en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ;
« 3º Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions.
« A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions. »

[1620] Code de procédure pénale, livre IV titre XV section 2 « *Art. 706-25-2. − Dans le but de constater les infractions mentionnées au sixième alinéa de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves et d'en rechercher les auteurs, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, s'ils sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin, procéder aux actes suivants sans en être pénalement responsables :*
« 1º Participer sous un pseudonyme aux échanges électroniques ;
« 2º Être en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions ;
« 3º Extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions.
« A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions ».

Un cyberpédophile a été dénoncé par la police new-yorkaise à la police française comme ayant consulté un site pédopornographique mis en place par cette unité de police, la preuve n'a pas été recevable en France, car elle provenait d'une incitation au délit, incitation constituée par l'existence du site lui-même[1621].

A) La difficulté de contrôler les moyens utilisés

Comment différencier un logiciel posé légalement par un officier de police judiciaire sous le contrôle d'un juge, d'un logiciel légal posé par un service de renseignements sans autorisation légale ou un malware posé par un pirate en toute illégalité ? Par ailleurs, la sophistication de ces dispositifs les rend de plus en plus difficiles à détecter, et peut inciter à leur pose en dehors de tout cadre légal, l'immunité étant alors due au « pas vu, pas pris »[1622].

Les logiciels de captation des données qui peuvent légalement être installés dans un ordinateur ne diffèrent pas réellement des logiciels Spyware utilisés illégalement par les cyberdélinquants. Les logiciels légaux ne seront vraisemblablement pas estampillés « *legal spyware* » et leur signature électronique ne les différenciera pas des « *malware* » ou logiciels illégaux. Quand un tel logiciel sera découvert sur un ordinateur par son propriétaire, il cherchera à l'effacer ou à le neutraliser. Compte tenu des diverses formes de ces logiciels malins, quelle autorité pourra vérifier que le logiciel malin trouvé sur un ordinateur est un logiciel déposé dans le cadre d'une procédure légale et non un logiciel autre ? La suppression d'un tel logiciel, légalement installé, sera-t-elle considérée comme un délit pour entrave à l'enquête ?

Le 28 mai 2012, Symantec[1623] a publié une analyse concernant une menace appelée *Flamer*. Il s'agit d'une menace extrêmement sophistiquée, utilisant plusieurs composants, qui dissimule habilement sa nature malveillante. L'architecture de *W32.Flamer* permet aux auteurs de modifier le fonctionnement et le comportement d'un composant individuel sans avoir à remanier ou même à connaître les autres modules utilisés par les contrôleurs du logiciel malveillant. Les modifications peuvent être introduites sous la forme de mises à niveau de la

[1621] Cité par Romain Darriere, « Sweetie, l'avatar virtuel fait condamner un pédophile : en France aussi, c'est possible », *L'Obs Le Plus,* 23 juin 2014, URL : http://leplus.nouvelobs.com/contribution/1253201-sweetie-l-avatar-virtuel-fait-condamner-un-pedophile-en-france-aussi-c-est-possible.html consulté le 9 janvier 2018.

[1622] Refrain des bataillons d'Afrique. Location employée quand on fait en secret quelque chose qui serait condamné si c'était vu, formule moqueuse pour dire que quelque chose peut être fait dès lors qu'on ne se fait pas prendre (source URL : http://www.languefrancaise.net/Bob/69627).

[1623] « *Menace Flamer* » sur le site de SYMANTEC, http://www.symantec.com/fr/fr/outbreak/?id=flamer&inid=fr_ghp_hero1_flamer consulté le 6 juin 2012

fonctionnalité, de correctifs ou simplement pour déjouer les produits de sécurité. *Flamer* vise principalement à obtenir des informations et des données. D'une façon générale, elle procure la capacité de voler des documents, de réaliser des captures d'écran des bureaux des utilisateurs, de se propager par le biais des lecteurs amovibles et de désactiver certains produits de sécurité. Ce logiciel malveillant *Flamer* dispose des fonctions de captation des données tel que prévu par la loi LOPPSI 2. Ce logiciel peut être mis à niveau à distance et semble difficile à déceler de par cette capacité à évoluer après son installation sur un ordinateur. De plus, selon Symantec, des serveurs ont transmis à des ordinateurs infectés par ce logiciel *Flamer* des ordres de destruction complète. Ainsi, un logiciel espion sophistiqué peut-il une fois installé, se voir mis à jour pour déjouer les logiciels de protection, et en cas de détection se saborder pour disparaître et supprimer ses traces ? Si le logiciel utilisé légalement dispose des mêmes fonctionnalités, ce qui semble tout à fait vraisemblable, il devient difficile de détecter sa présence et dans une telle situation, son autodestruction ne permet plus de recueillir des informations sur son origine et les informations transmises.

En septembre 2017, un logiciel espion utilisé par la NSA est révélé sur Internet[1624]. Le logiciel décrit est une plateforme très sophistiquée baptisée *UnitedRake* que la NSA utilise pour espionner les ordinateurs Windows. *UnitedRake* se présente comme un outil véritablement professionnel. Il est totalement adaptable et composé de cinq types d'éléments : un logiciel serveur, une interface graphique, une base de données, des modules de plugins et de logiciels client. Ces derniers sont déployés sur les ordinateurs ciblés sous la forme de chevaux de Troie. L'un de ces plugins est détaillé dans les documents d'Edward Snowden, à savoir « *Wistfultoll* ». Il permet de récolter des informations techniques et forensiques des ordinateurs infectés.

La lutte entre les logiciels de protection, tels ceux fournis par Symantec, et les logiciels malveillants est telle que ces derniers se retrouvent vulnérables peu après leur diffusion et donc potentiellement destructibles par les logiciels de protection. Il semble difficile de différencier les logiciels légaux des logiciels de protection. Les principaux fournisseurs de logiciels de protection sont américains (Symantec-Norton, McAfee Inc.), israéliens, roumains (*BitDefender*) ou russes (Kapersky). Il semble difficile dans ce contexte international de prévoir une signature qui permettrait à ces logiciels de reconnaître, en France, les logiciels installés légalement. De plus, une telle signature serait vite utilisée par les pirates et deviendrait une

[1624] Gilbert Kallenborn, « Un logiciel d'espionnage très sophistiqué de la NSA fuite sur le Web », 11 septembre 2017, *01net.com,* URL : http://www.01net.com/actualites/un-logiciel-d-espionnage-tres-sophistique-de-la-nsa-fuite-sur-le-web-1252292.html consulté le 9 janvier 2018.

faille de sécurité rédhibitoire. En conséquence, ces logiciels légaux seront détectés et détruits par les logiciels de protection des ordinateurs et il semble difficile de pouvoir incriminer le propriétaire d'un ordinateur correctement protégé (cette protection est requise par l'HADOPI et un manque de protection d'un ordinateur est répréhensible), d'avoir fait disparaître un logiciel de captation légale.

Les données captées par interception ou collectées lors des enquêtes ou des plaintes restent des données à caractère personnel, leur traitement reste soumis à la législation. Ces traitements doivent être contrôlés pour vérifier leur adéquation à la réglementation.

B) Des contrôles inadaptés ou inefficaces face à une législation sécuritaire

Le traitement des données personnelles est encadré par la loi n° 78-17 dite « informatique et liberté ». Tout traitement automatique de données personnelles doit être déclaré à la CNIL préalablement à sa création ou être autorisé par un décret. L'administration a créé des fichiers contenant des informations personnelles répertoriant toute personne objet d'une procédure judiciaire. Ces fichiers ont été créés sans déclaration préalable à la CNIL ni décret d'autorisation, et régularisés par une loi ou un décret plusieurs années après leur création[1625].

La loi LOPPSI 2 a prévu un regroupement des fichiers de police et de gendarmerie existant, en un seul fichier dit traitement de données à caractère personnel relatif aux « antécédents judiciaires »[1626] ainsi que des logiciels de rapprochement judiciaire à des fins d'analyse criminelle et des fichiers d'analyse sérielle. Mais ce regroupement des fichiers est réalisé avec les données existantes dans le STIC et JUDEX, alors que de nombreuses remarques ont été formulées sur le caractère erroné ou trop intrusif de certaines de ces données tant par la CNIL[1627] que par certaines commissions parlementaires. Ainsi le 13 juin 2013, la Commission de l'informatique et des libertés écrit[1628] : « *Le fonctionnement du STIC n'a pas connu d'évolution*

[1625] Bauer Alain, Soullez Christophe, « État des lieux », dans *Les fichiers de police et de gendarmerie.* Paris, Presses Universitaires de France, « Que sais-je ? », 2011, pp. 30-73. URL : https://www.cairn.info/les-fichiers-de-police-et-de-gendarmerie--9782130591160-page-30.htm consulté le 9 janvier 2018.

[1626] Décret n° 2013-1268 du 27 décembre 2013 *portant modification du décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires* publié au JORF n°0302 du 29 décembre 2013 page 21796.

[1627] Commission nationale de l'informatique et des libertés, Délibération n° 2011-204 du 7 juillet 2011 *portant avis sur un projet de décret en Conseil d'État relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé « traitement de procédures judiciaires » (TPJ) (demande d'avis n° 1484843)* publiée au JORF n°0107 du 6 mai 2012

[1628] Commission nationale de l'informatique et des libertés , « Contrôle des fichiers d'antécédents : conclusions et propositions de la CNIL », 13 juin 2013 accessible à

réelle et les défaillances relevées en 2009 persistent, en dépit d'avancées législatives pourtant conformes aux demandes de la CNIL » et « *il n'a pas été prévu de mettre à jour les millions de fiches issues du STIC et de JUDEX, qui comportent de nombreuses données inexactes […]Ainsi, des personnes continueront à se voir refuser l'accès à certains emplois, à un titre de séjour ou à la nationalité française sur le fondement de données d'antécédents erronées ».* Ainsi, les données collectées ne sont pas ou mal contrôlées lors de leur enregistrement et leur mise à jour, destruction ou effacement par les parquets ou l'autorité judiciaire n'est que partielle faute de personnel[1629].

Sous-section 2. Des textes rendus obsolètes par l'évolution des techniques

Comme le dit Mars Rees, Jean-Marie Delarue, le dernier président de la Commission nationale de contrôle des interceptions de sécurité doute, estimant le texte de la loi relative au renseignement trop centré sur les techniques : « *Nous nous trouvons désormais en porte à faux, car les techniques qui ne sont pas mentionnées dans la loi sont réputées illégales. Or l'évolution technologique dans ce domaine est galopante. La loi ne mentionne pas les drones. La préfecture de police en a déjà un. Le survol de propriétés privées risque de poser problème, car il me paraît difficile d'assimiler le drone à une technique existante* »[1630]. Cette distance nécessaire entre loi et technique était relevée dans l'étude d'impact accompagnant le projet de loi sur le renseignement[1631] : « *La législation (Intelligence Service Act 1994, British Security Service Act et RIPA 2000) ne réglemente pas en tant que tel l'usage de telle ou telle technique, mais raisonne davantage par rapport à la nature de l'atteinte à la vie privée qu'elle représente (ex : accès au domicile, filature, interceptions des communications). Un warrant peut ainsi intervenir dans n'importe quel domaine de la vie privée. Cette approche a permis à la*

http://www.cnil.fr/linstitution/actualite/article/article/controle-des-fichiers-dantecedents-conclusions-et-propositions-de-la-cnil/ consulté le 7 décembre 2015.

[1629] Commission nationale de l'informatique et des libertés, « Conclusions du contrôle du système de traitement des infractions constatées (STIC) », *Rapport remis au Premier ministre* le 20 janvier 2009, disponible à l'URL : https://www.cnil.fr/sites/default/files/typo/document/Conclusions%20des%20controles%20STIC%20CNIL%202009.pdf.

[1630] Cité par Marc Rees, « Loi Renseignement : l'actuel président de la CNCIS réitère ses doutes et critiques », *NextImpact* du 21 septembre 2015, disponible en ligne à https://www.nextinpact.com/news/96585-loi-renseignement-actuel-president-cncis-reitere-ses-doutes-et-critiques.htm, consulté le 18 juillet 2017.

[1631] *Projet de loi relative au renseignement*, Étude d'impact, 18 mars 2015, en ligne à http://www.assemblee-nationale.fr/14/projets/pl2669-ei.asp#P534_78127, consulté le 18 juillet 2017.

législation anglaise de s'adapter aux évolutions technologiques, sans qu'il soit nécessaire de mettre à jour les textes trop fréquemment ».

Ainsi, il est reconnu que l'imbrication de la technique avec la législation est une source d'inflation des textes et d'insuffisance législative. Cette difficulté de légiférer dans un domaine technique est due au délai législatif long, mais aussi à l'évolution rapide de la technique.

§ 1 - Des délais d'élaboration des textes réglementaires trop longs

Internet a mondialisé les échanges numériques. La technique évolue rapidement, chaque année apparaît un nouveau service ou un ancien service évolue. En 2016, Twitter qui limite les échanges à cent quatre-vingts caractères a étendu la longueur des messages échangés, ouvrant ainsi de nouvelles possibilités de communication instantanées. Facebook ouvre de nouveaux services chaque année et les mises à jour d'Android sont effectives tous les trimestres environ, tant pour optimiser et fiabiliser le système que pour y inclure de nouveaux services. Certaines techniques utilisées massivement disparaissent au profit de nouvelles techniques, comme le ftp face au streaming par exemple.

Face à l'évolution rapide de la technique, les délais d'élaboration des lois deviennent prohibitifs même si ces délais sont nécessaires pour éviter l'écueil de lois inadaptées ou non applicables. En France, le délai normal d'élaboration et de promulgation d'une loi est de plusieurs mois, voire plusieurs années. Le projet de loi est élaboré dans les cabinets ministériels, étudié pour avis par le Conseil d'État, adopté en conseil des ministres puis déposé à la Présidence de l'Assemblée nationale ou du Sénat. Il est alors étudié en commission, amendé puis inscrit à l'ordre du jour de cette assemblée. Il fait alors l'objet de discussions publiques avant son vote par l'assemblée. Une fois voté, il est transmis à la Présidence de l'autre chambre ou le même cycle se reproduit. En règle générale, il n'est pas voté dans les mêmes termes par les deux chambres et donc retourne devant la première chambre pour une nouvelle analyse des articles modifiés en commission, nouvelle discussion publique et nouveau vote. Après deux passages devant les chambres, si un texte commun n'est pas voté, une commission mixte va élaborer un texte commun qui sera présenté aux deux assemblées et finalement si ce texte n'est pas voté dans les mêmes termes par les deux assemblées, il revient à l'Assemblée nationale de voter le texte définitif. À partir de ce vote, il peut être soumis au Conseil constitutionnel pour valider sa

conformité à la Constitution. Après analyse, le projet de loi voit ses article déclarés conformes ou partiellement conformes, la loi pourra alors être promulguée et publiée au Journal officiel en totalité ou partiellement dans le respect des décisions du Conseil constitutionnel[1632]. Après ces navettes entre les assemblées et la décision du Conseil constitutionnel, il devra dans la plupart des cas attendre la publication des décrets d'application élaborés par les ministères concernés pour être pleinement opérationnel.

Une procédure d'urgence peut être adoptée par le gouvernement, dans ce cas, le projet est soumis à chaque chambre une seule fois, en cas de désaccord la commission mixte élabore un texte commun qui est soumis à l'Assemblée nationale, puis éventuellement au Conseil constitutionnel qui dispose alors d'un délai réduit pour se prononcer. L'une des lois promulguées rapidement en France est la loi d'orientation et de programmation pour la sécurité intérieure[1633]. Présentée en conseil des ministres le 10 juillet 2002, elle est défendue par Nicolas Sarkozy, ministre d'État, ministre de l'Intérieur. Examiné en urgence en juillet à l'Assemblée nationale, le projet de loi est adopté conforme par le Sénat, et déclaré conforme à la Constitution par le Conseil constitutionnel le 22 août. Promulguer une loi en moins de 6 semaines reste un exploit en France où certaines lois demandent plusieurs années avant leur promulgation. Toutefois, il est à noter que certaines dispositions de la loi, comme le blocage administratif de certains sites, n'ont jamais été mises en œuvre faute de décret d'application. La directive européenne 95/46/CE qui harmonise les législations sur la protection des données personnelles au niveau européen et qui devait être transposée en droit français en octobre 1998 au plus tard, ne l'a été qu'en 2004, soit plus de cinq ans après, en dépit des pressions de la Commission européenne.

Ainsi, face au délai long et nécessaire pour l'élaboration d'une loi, la situation technique, entre les débuts de l'élaboration du projet de loi concernant la société numérique et sa promulgation, a souvent évolué et la loi nécessiterait une révision avant d'avoir été promulguée. Ainsi après avoir adopté la loi HADOPI 2 qui ne concernait que les copies d'œuvres illicites réalisées en pair à pair, la technique du streaming, non prévue par la loi, était utilisée par les internautes. Le gouvernement de l'époque avait alors annoncé la préparation d'une loi HADOPI 3 intégrant la technique du streaming.

[1632] Olivier Gohin, « La formation de la loi », *Droit constitutionnel,* 3e édition, LexisNexis, 2016, pp.992-1026.
[1633] Loi no 2002-1 094 du 29 août 2002 *d'orientation et de programmation pour la sécurité intérieure (LOPSI).*

§ 2 - Des moyens techniques en croissance exponentielle

Outre le délai nécessaire à son élaboration, la loi est confrontée à l'apparition de nouvelles techniques. Internet n'existait pas en 1978 lors de la promulgation de la loi Informatique et Libertés. L'apparition rapide de nouvelles techniques peut rendre inopérantes certaines règles.
La protection des données à caractère personnel est efficace sur un territoire dont la législation est homogène. Ainsi, l'Union européenne a-t-elle une protection efficace pour les données gérées sur le territoire de l'Union, et interdit, en conséquence, tout transfert de données vers un pays ou État qui n'a pas une protection adéquate, c'est-à-dire équivalente. Or, le stockage des données est assuré dans des data centres répartis dans plusieurs pays, via la technique du cloud[1634] et il n'est pas aisé de s'assurer que les données collectées en Europe restent bien stockées sur le territoire européen.
L'anonymisation des données prévue par la législation pour conserver des données à caractère personnel sur une longue période à usage statistique n'est plus un moyen de garantir l'anonymat des personnes concernées. La base constituée par Netflix[1635] entre 2006 et 2009 démontre que face aux outils modernes, l'anonymisation des données est quasi-impossible à garantir.
D'autres règles, même observées correctement, peuvent se révéler inopérantes. L'anonymisation des données personnelles en est un exemple. Entre 2006 et 2009, Netflix a mis en place un concours public dont le but était de prévoir quels films ses utilisateurs allaient aimer. En se basant sur les notes qu'attribuent les clients aux films et étant donné la liste de ce qu'ils ont vu, Netflix peut-il faire des propositions ciblées de films qui conviennent au goût de ses clients pour de futurs achats ? Pour cela, Netflix a publié une base de données contenant les appréciations de 500 000 de ses clients sur son catalogue de films. La base était anonymisée en ce que le nom des clients était remplacé par un chiffre aléatoire. La base contenait autour de 100 millions de notes. Le but du concours était de produire un algorithme qui, étant donné la base publiée et étant donné un ensemble de 2,8 millions de couples utilisateur-film, s'approchait le plus près des notes réellement mises par ces utilisateurs.

[1634] Gustavo Gomez Mejia, « De quoi le "nuage" est-il le nom ? Le statut des supports face aux régimes du *cloud computing* », *Communication & langages*, 2014/4 (N° 182), pp. 77-93. URL : https://www.cairn.info/revue-communication-et-langages1-2014-4-page-77.htm consulté le 9 janvier 2018.
[1635] Neflix est une entreprise proposant des films en flux continu sur Internet.

À partir de cette base, Arvind Naranayan et Vitaly Shmatikov[1636] sont arrivés à retrouver jusqu'à 99 % d'exactitude, l'identité des utilisateurs ayant plus de 8 notes, et même 66 % d'exactitude dans le cas où seulement deux notes sont disponibles. Le biais par lequel les chercheurs sont arrivés à infiltrer la base de données est qu'en plus des simples notes pour chaque film, Netflix publiait également la date à laquelle ces notes avaient été attribuées. Naranayan et Shmatikov ont utilisé les informations de notations d'un autre site Internet Movie Database[1637]. Sur ce site, les internautes peuvent laisser des commentaires et leurs notes sur les films qu'ils ont vus. Ils ont alors fait le rapprochement entre la date à laquelle étaient notés les films sur la base de données de Netflix et celle à laquelle le même film était noté de manière similaire sur IMDB. Ainsi en faisant varier les intervalles de notes et de dates, et suivant le nombre de films associés à un numéro dans la base de Netflix (plus il y a de films notés qui correspondent entre les deux bases, plus il est facile d'établir l'identité d'une personne), ils sont arrivés à retrouver les noms des consommateurs anonymisés jusqu'à des niveaux de précision incroyable.

Ils ont également montré que même si on ne tient pas compte des dates (c'est-à-dire si on suppose que la base publiée ne contenait pas ces informations) il est toujours possible de désanonymiser une partie importante de la base publiée. Pour cela, ils ont utilisé les films « marginaux », c'est-à-dire ceux qui sont vus par peu de personnes (dans leur expérience, un film était classé marginal s'il n'était pas dans le top 500 des films les plus vus). Ils sont arrivés à retrouver les identités de 84 % des utilisateurs ayant 8 notes dont au moins 6 ne font pas partie du top 500.

Est-il possible de compromettre la vie privée d'un abonné de Netflix en utilisant la base de données publiée pour le concours Netflix ? La réponse à cette dernière question est oui. En effet, il est possible de connaître la liste des films qu'il a empruntés, voire celle qu'il aurait pu probablement emprunter (en utilisant par exemple un algorithme du concours Netflix justement) pour en déduire ses préférences politiques ou bien sexuelles, par exemple en connaissant (par un autre moyen) les préférences d'autres personnes ayant un schéma d'emprunt équivalent. Rien n'empêche également d'utiliser d'autres sources d'informations publiques dans lesquelles apparaissent certaines personnes identifiées dans Netflix et par rapprochement d'en déduire des informations sur d'autres utilisateurs de Netflix.

[1636] Arvind Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset,* The University of Texas at Austin, February 5, 2008

[1637] http://www.imdb.com/.

La perte de confidentialité est un phénomène de type contagieux. Les réseaux sociaux se font mutuellement la courte-échelle, le premier sert de base, et le second fournit des informations qui ne sont pas dans le premier, mais qui permettent à leur tour en réutilisant le premier réseau, de déduire des informations qui ne sont pas dans le second, et ainsi de suite. La puissance de calcul, la capacité de stockage des informations et le développement de nouveaux algorithmes toujours plus performants rendent pratiquement caduque la technique de l'anonymisation et donc l'obligation légale de l'utiliser. Le Règlement général sur la protection des données[1638] prend en compte cette particularité en ne parlant que de « pseudonymisation », et en le définissant comme étant « *le traitement de données à caractère personnel [réalisé] 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 et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

L'exemple de Netflix montre que des données personnelles d'identification, typiquement les données de type démographique comme le nom, l'âge, le sexe, le numéro de sécurité sociale, etc., ne sont qu'une illusion. Toute donnée particulière suffit pour identifier un individu. Plus il est possible d'accéder à des informations sur quelqu'un, plus il devient facile de l'identifier.

D'autres techniques, encore plus perfectionnées, permettent de sortir des corrélations en observant des masses gigantesques de données. C'est l'objectif de groupes de recherche comme celui de l'équipe *Human Dynamics* au *MIT Media Lab*[1639]. Leurs derniers résultats vont de la détection précoce de la maladie de Parkinson en cherchant des motifs dans la tonalité de la voix, les mouvements, les endroits (toutes des informations qui peuvent être récupérées par un téléphone portable) jusqu'à la prédiction du comportement économique des personnes en observant les schémas émergents relatifs aux utilisations de cartes bancaires.

Les techniques d'intrusion sur le réseau ou à l'intérieur d'un ordinateur évoluent également et deviennent de plus en plus difficiles à détecter. Les logiciels spéciaux de lutte contre ces intrusions évoluent également rapidement, des mises à jour en ligne sont proposées plusieurs fois par jour. La législation tente de protéger les individus contre ses intrusions qui peuvent

[1638] 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).*
[1639] http://hd.media.mit.edu/.

avoir des conséquences sur la vie privée des personnes et sur leur libre-arbitre. Mais, la législation, si elle est trop techniquement précise ne peut que devenir inopérante à plus ou moins long terme.

De plus, les États utilisent des techniques intrusives pour surveiller les individus suspectés de préparer des actes criminels ou des actes de terrorisme, en toute légalité ou non. La NSA qui utilisait des failles de sécurité pour s'introduire dans les serveurs, ne les a pas publiées, permettant ainsi la propagation de rançongiciel. Des moyens techniques peuvent ainsi être utilisées par des organisations criminelles pour préparer des crimes ou des attentats, et par les forces de sécurité pour défendre les États et la sécurité publique.

Partie 2. La société numérique confrontée aux libertés

Les débuts de l'informatique remontent à la fin de la Seconde Guerre mondiale, quand en 1946, le premier calculateur reprogrammable a été dévoilé au public[1640]. Sa programmation nécessitait une semaine de travail de câblage et il pesait trente tonnes. Depuis cette période, avec le progrès des techniques de l'électronique et de la miniaturisation des composants, l'informatique a, dans les années 1960 et 1970, commencé par investir les services comptables des sociétés, comptabilité générale, paie, etc. Cet outil mal contrôlé et mal accepté, a déresponsabilisé certaines fonctions de l'entreprise, voire certains services de l'administration, qui se retranchaient derrière des erreurs informatiques pour justifier leur propre erreur[1641].

Après les sociétés commerciales et industrielles, l'informatique a progressivement investi l'administration et la société civile. En 1975, l'INSEE s'est doté d'un ordinateur puissant, l'IRIS 80 de la CII[1642], et a développé plusieurs logiciels de traitement de données : COLIBRI pour les données issues du recensement ; LÉDA, CASTOR et POLUX pour le dépouillement des enquêtes statistiques[1643]. La France, dès 1978, a pris conscience du danger potentiel lié à la puissance et à la rapidité de calcul de ces nouveaux calculateurs électroniques ou ordinateurs. Cette prise de conscience aboutira en janvier 1978 à la promulgation de la loi relative à l'informatique, aux fichiers et aux libertés[1644]. Cette loi sera le premier texte mariant libertés, informatique et fichiers. En juillet de cette même année, sera promulguée la loi portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal[1645], appelée loi CADA du nom de la commission d'accès aux documents administratifs chargée de veiller au respect de la liberté d'accès aux données administratives. Ce texte encadre la mise à disposition des informations administratives et leur réutilisation. Ainsi, dès 1978, la France se dote de deux lois spécifiques et crée deux autorités administratives indépendantes : la Commission nationale de l'informatique et des libertés ou

[1640] Le 14 février 1946, l'ENIAC (acronyme de l'expression anglaise *Electronic Numerical Integrator Analyser and Computer*), est dévoilé au public à l'Université de Pennsylvanie à Philadelphie.

[1641] « C'est la faute de l'ordinateur », *La Nouvelle République,* 2 septembre 2011, URL : https://www.lanouvellerepublique.fr/actu/c-est-la-faute-de-l-ordinateur consulté le 26 mars 2018.

[1642] La Compagnie internationale pour l'informatique (CII) est une société privée française créée en décembre 1966, dans le cadre du plan Calcul, lancé par le gouvernement du général de Gaulle. Absorbée par Honeywell-Bull en 1975, elle devint partie de CII Honeywell-Bull, rebaptisé Bull en 1982.

[1643] Source personnelle de l'auteur qui a participé au développement de ces outils d'aide au dépouillement des enquêtes.

[1644] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* publiée au JORF du 7 janvier 1978 p. 227.

[1645] Loi nº 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*, publiée au JORF du 18 juillet 1978 p. 2851.

CNIL, pour la protection des données personnelles, et la Commission d'accès aux données administratives ou CADA, pour la liberté d'accès aux données administratives, dont certaines sont des données à caractère personnel (état civil, impôts et taxes, scolarité, etc.). Une concertation entre la CNIL et la CADA sur des sujets d'intérêt commun, par exemple les données administratives à caractère personnel, n'est instituée qu'en 2016 avec la loi pour une République numérique[1646].

Après les années 1980, l'informatique et la digitalisation[1647] des données ont continué leur progression, quittant le monde des entreprises et de l'administration pour entrer dans tous les foyers : téléphone, télévision, courrier personnel, santé et imagerie médicale, domotique, etc. En mai 1985, la Direction générale des Télécommunications, devenue depuis ORANGE[1648], inaugurait la première base de données nationale accessible à l'ensemble des abonnés au téléphone, l'Annuaire électronique et sa base de données contenant alors les noms et l'adresse des vingt-trois millions d'abonnés de l'époque, et développait le premier réseau numérique de services télématiques : Télétel. Aujourd'hui, les réseaux de transmissions transportent des séries de nombres et non plus des signaux analogiques. En ce début de XXI^{e} siècle, la société connaît une mutation rapide et plus profonde que les révolutions industrielles du XIX^{e} siècle associées à la mise à disposition de sources d'énergie nombreuses et autonomes. Cette nouvelle mutation, voire révolution, est associée aux données et à leur surabondance[1649], ainsi qu'au développement de nouveaux algorithmes de plus en plus performants. La puissance des algorithmes et leur capacité a s'autoadapter a permis le développement d'une nouvelle branche de l'informatique : l'Intelligence Artificielle[1650]. Ces algorithmes rivalisent avec l'homme dans les capacités de diagnostics et de décisions.

Le déploiement, dans notre vie quotidienne et dans notre environnement, des technologies numériques et des usages associés est en passe de modifier notre relation à la société, d'altérer notre liberté et de modifier nos comportements humains. Le numérique change les rapports que nous entretenons avec notre mémoire et notre histoire, ainsi que le transfert des connaissances. Notre appréhension de la sphère privée et nos relations avec les autres se trouvent modifiées

[1646] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, art. 26 et 28.
[1647] Terme dérivé de l'anglais *digit* qui signifie chiffre. Ce terme sera abandonné et remplacé par le verbe numériser.
[1648] Pour l'historique des changements concernant ORANGE, Cf. note 11.
[1649] Rémy Rieffel, *Révolution numérique, révolution culturelle ?* Gallimard, 2014.
[1650] Bertrand Braunschweig (coordination), *Intelligence Artificielle, les défis actuels et l'action d'Inria,* 16 septembre 2016, INRIA, en ligne à l'URL : https://www.inria.fr/medias/inria/documents/livre-blanc-ia consulté le 12 avril 2018.

dans la société numérique. Nos rapports avec le travail et la libre entreprise évoluent, faisant naître de nouveaux métiers et en faisant disparaître d'autres[1651], sans garantir une équivalence entre les créations et les suppressions, dérégularisant ainsi nos protections sociales.

Le *big data* associé aux nouveaux algorithmes permettent de prévoir la survenue d'une épidémie[1652] ou de calculer la probabilité de réalisation d'un délit dans un quartier urbain[1653]. Les méthodes statistiques prédictives anticipent les crises[1654], changent nos rapports avec nos envies, notre santé[1655]. Demain, une demande d'êtres humains complétés et augmentés peut apparaître, rendant certains handicaps inacceptables et rejetés. L'homme augmenté fait place au transhumanisme[1656], les prothèses réparatrices, pompes à insuline commandées électroniquement selon le taux de glucose du sang, font place aux prothèses augmentant les capacités d'un individu, voire prolongeant son espérance de vie. Enfin, il change nos rapports avec les objets, les rendant « intelligents » et autonomes et nous en faisant perdre le contrôle[1657], annihilant notre liberté de les utiliser ou non.

Ces transformations affectent également les sphères de l'État, de l'administration, de l'économie, de l'urbanisme[1658], en fait, cette révolution affecte notre environnement quotidien. Devant ces modifications de la société et l'accélération des techniques, l'appréhension du droit et de la protection de nos libertés doit évoluer. La proclamation universelle des droits de l'homme[1659] a été effective deux siècles après la Révolution française et la Déclaration des droits de l'homme et du citoyen[1660]. Elle est la conséquence du traumatisme causé par le

---

[1651] Mellet Kevin, « L'Internet et le marché du travail. Cadrage des interactions et pluralité des formats d'information », *Réseaux*, 2004/3 (n° 125), pp. 113-142. URL : https://www.cairn.info/revue-reseaux1-2004-3-page-113.htm consulté le 6 décembre 2017.

[1652] Science et Avenir avec AFP, « Les "big data", nouvel outil contre les épidémies comme Ebola ? », *Sciences et Avenir* 27 octobre 2014, en ligne URL : https://www.sciencesetavenir.fr/sante/les-big-data-nouvel-outil-contre-les-epidemies-comme-ebola_28006, consulté le 4 décembre 2017.

[1653] Sender Elena, « Californie : la police connaît déjà l'heure du crime », *Sciences et Avenir n°782*, avril 2012, pp. 68-73.

[1654] José Gaydu, « Réflexions sur l'analyse prédictive pour l'administration des collectivités territoriales », Irène Bouhadana, William Gilles (sous la direction), *Vis privée, vie publique à l'ère du numérique, Revue de l'Institut du Monde et du Développement*, mai 2011, les éditions IMODEV, pp. 113-114.

[1655] Richard Boyre, « Predictive Analytics and the Internet of Things », *Predictive Analytics Times,* 30 janvier 2016, URL: http://www.predictiveanalyticsworld.com/patimes/predictive-analytics-and-the-internet-of-things/7282/, consulté le 4 janvier 2017.

[1656] François Berger, « Le transhumanisme est un charlatanisme dangereux », *Sciences et Avenir*, Août 2016.

[1657] Laurence Allard, « Dans quel monde voulons-nous être connectés ? Transhumanisme vs companionism », *Nectart*, 2016/2 (N° 3), pp. 125-132. URL : https://www.cairn.info/revue-nectart-2016-2-page-125.htm consulté le 6 décembre 2017.

[1658] Maryse Carmes, Yanita Andonova, « Les politiques numériques internes à l'heure de "l'e-administration" : une analyse des programmes d'action des collectivités territoriales », *Communication & organisation* n°41, 2012, pp.87-100, URL : http://communicationorganisation.revues.org/3747 consulté le 6 décembre 2017.

[1659] Organisation des Nations Unies, *Déclaration des droits de l'homme*, 10 décembre 1948.

[1660] *Déclarations des droits de l'homme et du citoyen*, 1789.

nazisme qui a foulé ces droits fondamentaux. L'invasion du numérique n'a pris que quelques décennies et les bouleversements de notre société ne sont pas encore tous perceptibles, le droit doit anticiper autant que faire se peut les atteintes à nos libertés et à notre vie privée, atteintes étatiques, administratives, sociétales ou atteintes mercantiles.

Titre 1. La société numérique comme vecteur de mutation

Historiquement, toute innovation technologique importante a eu des conséquences sur la société de son époque. L'imprimerie de Gutenberg a permis la diffusion des livres qui étaient auparavant manuscrits et restaient l'apanage des moines et des clercs. La diffusion des écrits imprimés a permis la diffusion du savoir et a aboli le monopole de l'église dans l'enseignement et la transmission des savoirs[1661]. La Sorbonne était une institution religieuse et ses étudiants étaient des clercs. La première matière enseignée y était la théologie. L'imprimerie a permis la diffusion de la Bible et sa lecture par des laïcs lettrés, et annonce la Réforme[1662] basée sur la lecture de la Bible et non plus sur la parole de l'église[1663]. La liberté de religion est une conséquence indirecte de l'invention de l'imprimerie. L'imprimerie a permis également de libérer les connaissances en permettant la diffusion du savoir autrement qu'oralement par des clercs. La diffusion des connaissances par un maître entouré de ses disciples est révolue, et cette révolution marque la fin de l'obscurantisme, le début de la diffusion des connaissances modernes et le développement de la liberté intellectuelle et de la recherche scientifique. L'imprimerie a également permis la création et la propagation de la littérature romanesque issue des chansons de geste du Moyen-Âge qui étaient récitées ou chantées.

Comme l'imprimerie a influencé la société de la Renaissance[1664], la révolution numérique a aussi transformé la société actuelle et a contribué à des modifications du comportement des individus qui se retrouvent en permanence surveillés. Pour Gilles Babinet[1665], cinq mutations liées à l'ère numérique vont avoir des conséquences sur notre vie : l'accélération de la diffusion de la connaissance, l'éducation, la santé, la révolution des robots et les gouvernements ouverts. Ces mutations vont concerner nos libertés et modifier nos paradigmes sociétaux.

Cette mutation est visible avec l'apparition de la génération Y ou « digital natives » qui désigne les individus nés entre 1978 et 1994, suffisamment jeunes lors de l'introduction massive de

[1661] Russell L. Weaver, « *From Gutenberg to the Internet: Free speech, advancing technology, and the implications for democracy* », Carolina Academic Press 2013.

[1662] Jean Quéniart, « 4 - Livre et réformes religieuses », dans *Les Français et l'écrit (XIII^e-XIX^e siècle).* Quéniart Jean (dir.). Hachette Éducation (programme ReLIRE), « Carré Histoire », 1998, pp. 54-74. URL : https://www.cairn.info/les-francais-et-l-ecrit-xiiie-xixe-siecle--9782011450098-page-54.htm consulté le 6 décembre 2017.

[1663] Laurence Villoz, « Quand l'imprimerie bouleversa la religion », *Imprimer la Réforme - Protestinfo,* 24 août 2017, URL : https://www.reformes.ch/culture/2017/08/quand-limprimerie-bouleversa-la-religion-histoire-reforme-protestantisme-imprimerie, consulté le 4 décembre 2017.

[1664] Jean Quéniart, « 3 - Livre et culture au début du XVI^e siècle », dans *Les Français et l'écrit (XIII^e-XIX^e siècle).* Jean Quéniart (dir.). Hachette Éducation (programme ReLIRE), « Carré Histoire », 1998, pp. 37-53. URL : https://www.cairn.info/les-francais-et-l-ecrit-xiiie-xixe-siecle--9782011450098-page-37.htm consulté le 6 décembre 2017.

[1665] Gilles Babinet, *L'ère numérique, un nouvel âge de l'humanité. Cinq mutations qui vont bouleverser notre vie*. Le Passeur, 2014.

l'informatique grand public et de l'électronique portable (téléphonie mobile, photo numérique, GPS) pour en avoir acquis une maîtrise intuitive et des comportements de communication reposant sur l'utilisation des techniques associées aux réseaux sociaux[1666]. Internet permet à cette génération de consommer de l'information, d'accéder à la culture, mais elle expose sa vie privée sur les réseaux sociaux et met ainsi à disposition des informations intimes qui restaient auparavant dans la sphère familiale.

L'utilisation des techniques numériques provoque des mutations dans la société du XXI^{e} siècle. Ces mutations touchent l'accès au savoir, l'éducation, la culture, l'information, la médecine, la vie privée et professionnelle, mais aussi par contagion la vie politique. Dans une première partie, la mutation de la notion de vie privée est analysée pour étudier dans une seconde partie l'émergence progressive d'une participation citoyenne à la vie de la cité et à la politique. Ces deux évolutions ont des conséquences sur les libertés des individus et révèlent les enjeux liés à la numérisation en cours.

[1666] David Moriez, Catherine Voynnet Fourboul, « Les valeurs de la génération Y et ses implications pour la gestion. Etude des valeurs individuelles, organisationnelles et de bien être d'une population étudiante en École Supérieure de Commerce », *Revue internationale de psychosociologie et de gestion des comportements organisationnels*, 2016/53 (Vol. XXII), pp. 37-64. URL : https://www.cairn.info/revue-internationale-de-psychosociologie-de-gestion-des-comportements-organisationnels-2016-53-page-37.htm, consulté le 4 décembre 2017.

Chapitre 1. La mutation insidieuse de la vie privée liée aux usages des individus

Avec les capacités de stockage et de calcul des ordinateurs modernes et la construction des fermes de calcul ou de stockage[1667], il est possible de collationner et de recouper une quantité importante d'informations concernant un individu ou un groupe d'individus. Avec les techniques existantes et l'amélioration continuelle des algorithmes, il devient aisé de localiser un individu à partir de certains de ses actes (paiement par carte bancaire, utilisation des transports en commun avec utilisation de cartes RFID, utilisation de téléphone portable, caméra de vidéosurveillance…), mais également de capter sa correspondance privée, de connaître ses relations, ses tendances sexuelles, d'être informé sur sa santé et de collecter d'autres informations qui restaient, jusqu'alors, propres à la sphère privée. Ces algorithmes d'analyse des données permettent de détecter l'apparition des épidémies avant que l'OMS n'en soit alertée[1668]. Avec des techniques différentes de celles pensées par George Orwell[1669], Big Brother[1670], ou sa surveillance omniprésente, s'immisce dans notre monde moderne et numérique. Les caméras de vidéoprotection situées dans les centres commerciaux et les centres-villes, dans les transports en commun, dans les rues et places des villes et villages surveillent les passants, les utilisateurs et les chalands. Les achats sont enregistrés lors des passages en caisse dans les magasins et l'information collectée est immédiatement utilisée pour assurer une promotion commerciale ciblée. Les revenus et dépenses sont enregistrés par la banque qui

[1667] La ferme (ou *cluster* en anglais) est un procédé de mise en réseau de plusieurs ordinateurs qui vont apparaître, vus de l'extérieur, comme un seul ordinateur surpuissant, tant en vitesse de calcul (utilisé pour effectuer des calculs parallèles) qu'en capacité de stockage avec ou sans redondance.
[1668] Science et Avenir avec AFP, « Les "big data", nouvel outil contre les épidémies comme Ebola ? », *Sciences et Avenir* 27 octobre 2014, en ligne URL : https://www.sciencesetavenir.fr/sante/les-big-data-nouvel-outil-contre-les-epidemies-comme-ebola_28006, consulté le 4 décembre 2017.
[1669] George Orwell, *1984*, version française Éditions Gallimard, 1950
[1670] Big Brother surveille tout le monde à travers le télécran installé dans les appartements et des rondes effectuées en hélicoptère pour regarder par les fenêtres. Mais Big Brother prévient de cette surveillance et annonce à travers des affiches : « Big Brother vous surveille » (en anglais : *" Big Brother is watching you").*

connaît également, grâce aux paiements effectués avec la carte bancaire, les modes de vie et les centres d'intérêt de son détenteur[1671]. Nul besoin d'être confesseur pour connaître la vie privée d'un individu, Google dispose de plus d'informations sur les individus que tout confident ou confesseur, sans que la personne concernée en soit consciente[1672].

En cas de disparition d'un individu ou lors d'une enquête, le téléphone portable est géolocalisé et les messages ou conversations sont interceptés, l'ordinateur est fouillé, les paiements et les retraits effectués avec une carte bancaire surveillés, tous ces moyens permettent à l'enquête de progresser, mais ces moyens peuvent aussi être utilisés pour surveiller un individu à son insu et attenter à sa liberté et sa vie privée. La surveillance de l'individu peut également être effectuée par les forces de police et de gendarmerie dans le cadre des lois pour la sécurité et contre le terrorisme[1673] sur décision réglementaire, sans intervention d'un juge judiciaire[1674]. La sûreté des individus n'est plus légalement garantie[1675] puisque si les indices convergent, un individu peut être arrêté ou assigné à résidence avant d'avoir commis une infraction liée au terrorisme[1676].

Les données individuelles peuvent aujourd'hui être fournies par des objets avec la venue de l'Internet des objets[1677]. L'émergence de ces nouveaux objets connectés multiplie les sources d'information privée et constitue une immixtion dans la sphère intime de l'individu[1678]. La sécurité de ces objets n'est pas garantie, favorisant ainsi le vol de données personnelles intimes[1679].

[1671] Olivier Ertzscheid, « L'homme, un document comme les autres », *Hermès, La Revue*, 2009/1 (n° 53), pp. 33-40. URL : https://www.cairn.info/revue-hermes-la-revue-2009-1-page-33.htm consulté le 11 décembre 2018.

[1672] Gary Assouline, « Google sait tout de vous, vous le montre désormais et vous dit comment faire pour reprendre le contrôle », *Huffpost,* 5 octobre 2016, en ligne URL : http://www.huffingtonpost.fr/2016/06/30/google-mon-compte-vie-privee-_n_10750178.html, consulté le 4 décembre 2017.

[1673] David Lyon, « 6. Le 11 septembre, la "guerre au terrorisme" et la surveillance généralisée », dans *Au nom du 11 septembre...Les démocraties à l'épreuve de l'antiterrorisme.* Paris, La Découverte, « Cahiers libres », 2008, pp. 90-103. URL : https://www.cairn.info/au-nom-du--9782707153296-page-90.htm, consulté le 6 décembre 2017.

[1674] Code de la sécurité intérieure, Livre II, Titre IV – Interceptions de sécurité, art. L.241-1 à L.242-9.

[1675] Didier Bigo, Laurent Bonelli, Thomas Deltombe, « Introduction. Les libertés sacrifiées au nom de la sécurité ? », dans *Au nom du 11 septembre...Les démocraties à l'épreuve de l'antiterrorisme*. Paris, La Découverte, « Cahiers libres », 2008, pp. 5-10. URL : https://www.cairn.info/au-nom-du--9782707153296-page-5.htm, consulté le 6 décembre 2017.

[1676] Conseil d'État, Ordonnance du 23 décembre 2015, N° 395229, *M. B.*

[1677] « Le corps, Nouvel Objet Connecté – Du *quantified self* à la M-santé. Les nouveaux territoires de la mise en données du monde ». – *Cahiers IP (Innovation & Prospective)* n° 2, CNIL, Mai 2014.

[1678] François-André Allaert, Noël-Jean Mazen, Louis Legrand *et al.*, « Les enjeux de la sécurité des objets connectés et applications de santé », *Journal de gestion et d'économie médicales*, 2016/5 (Vol. 34), pp. 311-319. DOI : 10.3917/jgem.165.0311. URL : https://www.cairn.info/revue-journal-de-gestion-et-d-economie-medicales-2016-5-page-311.htm consulté le 6 décembre 2017.

[1679] Julian Rioche, « L'enjeu de la sécurité des objets connectés », *I2D – Information, données & documents*, 2017/3 (Volume 54), pp. 64-65. URL : https://www.cairn.info/revue-i2d-information-donnees-et-documents-2017-3-page-64.htm consulté le 11 janvier 2018.

Avec les techniques numériques, le régime hitlérien aurait pu contrôler les déplacements des individus et aurait vu sa puissance de nuisance décuplée. L'étoile jaune, bien que visible, n'a pas la capacité de localisation d'une puce RFID utilisée aujourd'hui pour suivre et assurer la traçabilité des bovins, ovins et autres porcins. Cette technologie est déjà utilisée par certaines entreprises pour identifier rapidement des employés et gérer l'accès à certains espaces particulièrement protégés en lieu et place de badges. Certains lieux de loisirs utilisent ces puces RFID pour autoriser l'accès de leurs membres[1680], aujourd'hui sur la base du volontariat. Nul besoin de marquage visible, un lecteur sans contact suffit pour savoir qu'une personne est passée à un endroit donné. Dès 2013, la CNIL préconise la réalisation d'une étude d'impact lors de l'utilisation de ces dispositifs[1681], anticipant ainsi l'obligation de ces études d'impact prévues par le Règlement général sur la protection des données [1682].

Dans son livre, Alex Türk[1683] fait état d'un projet européen de géolocalisation des passagers dans les aéroports, le projet « Op Tag » dévoilé au public en 2006[1684]. Ce projet a été testé dans l'aéroport de Copenhague[1685] sur fonds de la Commission européenne. Couplée au réseau de vidéosurveillance, une puce RFID présente sur la carte d'embarquement doit permettre de repérer les voyageurs qui flânent dans l'aéroport et retardent d'autant la procédure d'embarquement[1686]. Cet outil peut être facilement détourné de son usage primaire et devenir un outil policier très contraignant si aucun texte n'encadre son utilisation, tout voyageur muni

[1680] La Vanguardia – Barcelone, « Une puce électronique sous la peau pour entrer en discothèque », *Courrier international,* 2 juin 2004, URL : https://www.courrierinternational.com/article/2004/06/03/une-puce-electronique-sous-la-peau-pour-entrer-en-discotheque consulté le 6 décembre 2017.

[1681] Commission nationale de l'informatique et des libertés, *Comment réaliser une évaluation d'impact sur la vie privée (EIVP) pour les dispositifs RFID ?* Septembre 2013, disponible en ligne à l'URL : https://www.cnil.fr/sites/default/files/typo/document/Methodologie-etude_impact_RFID.pdf, consulté le 31 juillet 2017.

[1682] Considérant n[os] 84, 90 à 95, et section 3, articles 35 et 36 du 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).*

[1683] Alex Türk, sénateur français, président de la CNIL de 2004 à 2011.

[1684] Alex Türk, *La vie privée en péril*, Éditions Odile Jacob, 2011.

[1685] Cécile Blanchard, « Localisation des passagers par RFID ou bluetooth testée à l'aéroport de Copenhague », 4 juin 2008, in *ReseauxTelecom.net* à http://www.reseaux-telecoms.net/actualites/lire-localisation-des-passagers-par-rfid-ou-bluetooth-testee-a-l-aeroport-de-copenhague-18282.html consulté le 5 mai 2012.

[1686] Ce projet européen a fait l'objet d'un rapport : « *Project no. AST3-CT-2004 502858_OpTag, Op Tag Improving Airport Efficiency, Security and Passenger Flow by Enhanced Passenger Monitoring Executive Summary* » concernant son expérimentation du 1[er] février 2004 au 31 janvier 2007, rapport disponible à http://cordis.europa.eu/docs/publications/1239/123991301-6_en.pdf, consulté le 2 aout 2017.

d'un tel billet se retrouve sous surveillance permanente dès son entrée dans l'aéroport. L'expérience ne semble pas s'être conclue par une mise en service permanente du dispositif[1687]. Les régimes démocratiques peuvent également connaître des dérives sécuritaires en utilisant des moyens puissants et furtifs mis à disposition grâce à la technologie numérique, technologie utilisée également par les cybercriminels[1688] qui affaiblissent ainsi nos démocraties.

[1687] Alors que le projet était financé par l'Europe, critiqué par le G29, il est impossible sur Internet de trouver une information sur ce projet après 2012.
[1688] Voir Partie 1. Titre 2. Chapitre 1. Section 1. Sous-section 1. § 2 -Des attaques facilitées par les techniques numériques : Cyberterrorisme et cyberguerre.

Section 1. L'évolution de la notion de vie privée

La notion de vie privée a évolué au cours de l'histoire. La vie privée et la vie publique de Louis XIV sont intimement liées, tous les actes de sa vie privée, du lever au coucher, sont donnés en spectacle à la cour. Les maîtresses ou favorites du roi sont connues et courtisées. Toutefois, le mariage de Louis XIV et madame de Maintenon n'a pas été divulgué par le Roi, sans doute plus pour des raisons de bienséance que pour des raisons de protection de la vie privée[1689]. Les révolutionnaires français ont défini des droits naturels et individuels : la liberté, la propriété et la sûreté[1690], mais n'ont pas évoqué explicitement la vie privée. La vie privée telle que nous la connaissons aujourd'hui est apparue au XIX^{e} siècle dans les milieux bourgeois. La vie publique et la vie privée deviennent deux notions divergentes, l'une est connue et montrée, l'autre est confinée et non révélée. Avec Internet, la frontière entre vie privée et vie publique bouge à nouveau, il faut distinguer deux notions nouvelles, fortement imbriquées l'une dans l'autre : la vie privée et l'intimité de la vie privée. Le Code civil, dans son article 9[1691], s'il protège la vie privée des individus, ne définit le rôle du juge que pour une atteinte à l'intimité de la vie privée. Le Code pénal ne définit une infraction pénale que pour la violation de l'intimité de la vie privée[1692]. Sont pénalement répréhensibles l'enregistrement ou la captation de conversations privées ou confidentielles ou d'images de la personne sans autorisation dans

[1689] « *Dans la nuit du 9 au 10 octobre 1683, le roi Louis XIV épouse en grand secret l'ancienne gouvernante de ses bâtards, […] la marquise de Maintenon, née Françoise d'Aubigné, fille d'un voyou et veuve du poète paralytique Scarron* » (« 9 octobre 1683 - Le mariage secret de Louis XIV », *herodote.net*, URL : https://www.herodote.net/9_octobre_1683-evenement-16831009.php consulté le 26 mars 2018).

[1690] Article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

[1691] Code civil, article 9, « *Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé* ».

[1692] Code pénal, Section 1 : De l'atteinte à la vie privée. Article 226-1, « *Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :*
« 1º En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
« 2º En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.
« Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé ».

un lieu privé. L'interception de correspondances privées est elle aussi répréhensible et prévue dans le Code des postes et des communications électroniques[1693].

La Déclaration universelle des droits de l'homme[1694] proclame dans son article 12 que l'immixtion dans la vie privée[1695] est prohibée et doit être protégée par la loi. Cet article 12 associe vie privée, famille, domicile, correspondance ainsi que réputation et honneur. Au niveau européen, la Convention européenne des droits de l'homme[1696] proclame le droit à la vie privée dans son article 8[1697] en associant également vie privée, vie familiale, domicile et correspondance. La Convention n° 108[1698] rappelle dans son article 1er la nécessité de garantir le droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel. La Charte des droits fondamentaux de l'Union européenne[1699], dans son article 7[1700], proclame le droit au respect de la vie privée et familiale, de son domicile, de sa correspondance.

Ainsi, sans avoir été définie, la vie privée est protégée par plusieurs sources internationales et nationales, mais dans une société numérique où la collecte de données à caractère personnel est difficilement contrôlée, et où la diffusion de telles données peut être le fait de la personne concernée elle-même, la notion de vie privée évolue avec les usages.

[1693] Code des postes et des communications électroniques, LIVRE II : Les communications électroniques. TITRE Ier : Dispositions générales. Chapitre II : Régime juridique. Section 3 : Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques. (Articles L.34-1 à L.34-6).

[1694] Le 10 décembre 1948, les 58 États Membres qui constituaient alors l'Assemblée générale de l'Organisation des Nations Unies ont adopté la Déclaration universelle des droits de l'homme à Paris au Palais de Chaillot (résolution 217 A (III)).

[1695] Déclaration universelle des droits de l'homme, Article 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* ».

[1696] Conseil de l'Europe, *Convention de sauvegarde des droits de l'homme et des libertés fondamentales,* Rome, 4 novembre 1950.

[1697] Convention européenne des droits de l'homme, Article 8 « *Droit au respect de la vie privée et familiale*
« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
« 2. 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 ».

[1698] Conseil de l'Europe, traité n° 108, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 janvier 1981.

[1699] *Charte des droits fondamentaux de l'Union européenne (2000/C 364/01)* publiée au Journal officiel des Communautés européennes du 18 décembre 2000.

[1700] Charte des droits fondamentaux de l'Union européenne, Article 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* ».

Sous-section 1. De la vie privée à l'intimité de la vie privée

La société reconnaît à l'individu le droit de disposer d'un espace privé, distinct de la vie collective de la communauté[1701]. Dès l'époque franque, un domaine privé existe, il est l'objet d'un droit de possession, marqué de signes distinctifs : bornes, perches, barrières. Les objets qui sont dans l'enclos, dans la cour, ne relèvent pas de la loi, mais du maître de la « *domus* », du « domestique », de la maison. « *Ce fut dans les formes de la vie privée que la féodalisation émietta le pouvoir public* »[1702].

Plus tard, à la cour du roi, on parle de privé, de « *privance* », de « *priveté* »[1703] pour qualifier les gens du cercle de famille, par rapport aux étrangers : « *Estrayns o privats*. » La notion de privé s'affirme en contrepoint de la notion de public. Au XIIe siècle, le « *privatus* » correspond à l'idée qu'existent des actes, des êtres, des objets échappant de droit à l'autorité collective. Mais, pour Georges Duby, la bourgeoisie anglo-saxonne a, depuis le XIXe siècle, organisé, socialement et juridiquement, les défenses de la « *privacy* » qui est vue comme un savoir-être et un savoir-vivre[1704]. Au cours du XX^{e} siècle, des régimes totalitaires ont remis en cause le caractère central de la sphère privée en niant l'existence et la légitimité de cette sphère privée et en soumettant l'individu à la réalisation d'une unité basée sur la race, l'histoire ou l'idéologie. Les réseaux sociaux ont modifié la vision de la vie privée avec les habitudes de mettre sur les réseaux sociaux des pans de cette vie privée : photos d'événements familiaux, photos de voyage, annonce d'événements familiaux, etc. La date de naissance d'un individu est ainsi devenue par le biais des réseaux sociaux une information publique, information rappelée chaque année par émission d'un message vers les « amis » pour les inciter à l'envoi d'une carte virtuelle de bon anniversaire ou à tout autre signe d'amitié. Au travers des réseaux sociaux, des pans de la vie privée des individus négligents transitent également [1705] et sont stockés sur le réseau Internet, rendant ces informations disponibles et quasiment ineffaçables. La vie privée et l'image d'un individu se retrouvent ainsi l'otage des réseaux sociaux pour qui l'exposition de ces informations est vitale pour leur existence.

[1701] Yves Détraigne et Anne-Marie Escoffier, Rapport n^{o} 441 du 27 mai 2009 *relatif au Respect de la vie privée à l'heure des mémoires numériques,* Sénat, p. 11.

[1702] Philippe Ariès, Georges Duby, *Histoire de la vie privée, Tome 2 De l'Europe féodale à la Renaissance*, Collection L'Univers historique, Éditions du Seuil, 1 988

[1703] Terme cité par Littré.

[1704] Cité par Pierre Tabatoni, « Vie privée : une notion et des pratiques complexes » in *La protection de la vie privée dans la société d'information*, Presses Universitaires de France (Cahiers des Sciences morales et politiques).

[1705] Caroline Vallet, « Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs », *Droit et société* 2012/1 (n^{o} 80), pp. 163-188.

Si la protection de la vie privée est devenue vitale en réaction à l'époque nazie, cette protection est liée également à la crainte de voir des informations accessibles à des entités, institutions ou individus, utilisées pour porter atteinte aux libertés individuelles et à la capacité d'autodétermination de chaque individu. Comme l'écrit Yves Poullet, *« l'information représente pour ceux qui la détiennent un pouvoir vis-à-vis de ceux sur lesquels l'information est détenue. Celui qui détient l'information sur autrui peut adapter sa décision en fonction de la connaissance que l'information collectée et traitée lui donne d'autrui. Il prévoit son attitude et peut donc répondre à sa demande ou influencer celle-ci* »[1706].

Dans des pays comme l'Allemagne, l'Espagne ou l'Italie, ainsi que la France où l'histoire a marqué directement les populations, la protection de la vie privée est ainsi plus ancrée dans les réactions individuelles que dans les pays anglo-saxons où l'effet direct des régimes totalitaires ne s'est pas fait ressentir, bien que dans ces pays, existe aussi une vigilance concernant l'intrusion des gouvernements dans la sphère privée. La tradition puritaine pose que la vie privée est une garantie des qualités de la vie publique[1707]. Ainsi, l'exposition de la vie privée d'un homme politique est une forme de critique, alors qu'en France, tradition royale oblige, cette exposition serait de faire aimer les autorités, non les juger.

Pour un individu privé, il y a deux approches en matière de vie privée : la protection de la vie privée qui vise à assurer à toute personne le respect de sa vie privée, de son intimité, et à sanctionner, le cas échéant, la divulgation illégale de renseignements le concernant, et la reconnaissance aux individus d'une sphère de vie privée[1708] à l'intérieur de laquelle nul ne peut s'immiscer sans autorisation judiciaire[1709]. Les frontières de la vie privée sont variables, subjectives[1710] et dépendent des circonstances, des personnes impliquées et des valeurs de la société. La divulgation de faits privés liés à une personne publique peut être considérée comme une intrusion à leur intimité, mais elle peut aussi être considérée comme une information

[1706] Yves Poullet, Jean-François Henrotte, « La protection des données (à caractère personnel) à l'heure de l'Internet », in *Protection du consommateur, pratiques commerciales et T.I.C.*, collection Commission Université-Palais, volume 109, pp. 197-245 (cité dans le rapport nº 441).

[1707] Bernard Beignier, *Vie privée et vie publique*, septembre 1995, Légipresse pp. 67-74.

[1708] *La « sphère de la vie privée a un caractère éminemment subjectif qui se rapporte à l'identité de la personne, à son rôle social, à la nature des actes qu'elle accomplit »* ; France Allard, « Les droits de la personnalité », in Barreau du Québec, *Personnes, famille et successions*, Collection de droit 1997-1998, volume 3, Cowansville, Éditions Yvon Blais, 55-75.

[1709] Pierre Trudel, *La protection de la vie privée*, cours, Chaire L. R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, Faculté de droit, Université de Montréal.

[1710] Pierre-Brice Lebrun, « La vie privée », *Empan* 2015/4 (nº 100), pp. 168-172.

légitime[1711]. La Cour européenne des droits de l'homme considère que les personnalités publiques bénéficient d'une vie privée amoindrie par rapport aux personnes privées, la liberté d'expression serait supérieure à la protection de la vie privée de la personne publique si l'information en question contribue à un débat d'intérêt général, et si le journaliste respecte les principes européens de déontologie de l'information[1712]. Le 9 décembre 1992, le Tribunal de grande instance de Nanterre avait formulé cette dualité vie privée c/ vie publique en formulant : « *le domaine de la vie privée d'un personnage connu, célèbre, peut, en certaines circonstances et à la condition que n'ait été manifestée aucune volonté contraire, être plus restreint que celui de la vie privée d'un citoyen anonyme* »[1713].

En Europe, sont considérés comme inclus dans la vie privée, la vie sentimentale ou sexuelle, l'état de santé, la vie familiale, le domicile, les opinions religieuses, politiques ou philosophiques, mais aussi l'orientation sexuelle d'une personne, son anatomie ou son intimité corporelle[1714]. Avec les réseaux sociaux, tous ces éléments peuvent se retrouver disponibles[1715] et consultés par des personnes non autorisées et malveillantes. Les réseaux sociaux étant principalement d'origine nord-américaine, la protection de la vie privée sur ces réseaux reste d'inspiration anglo-saxonne, c'est-à-dire liée à une autorégulation[1716].

[1711] Anne Pigeon-Bormans, *Vie privée et personnalités publiques à propos de deux arrêts de la CEDH*, Publié le 1er septembre 2014 à http://pigeon-bormans.com/Vie-privee-et-personnalites.html, consulté le 2 aout 2017.
[1712] Cour européenne des droits de l'homme, 7 févr. 2012, Affaire nº 40660/08; 60641/08. Lire en ligne : https://www.doctrine.fr/d/CEDH/CLINF/CLIN/2012/CEDH002-99, consulté le 2 aout 2017.
[1713] Cité par Bernard Beignier, Vie privée et vie publique, Archives de *philosophie du droit*, tome 41 (1997), pp. 163-180 en ligne à http://www.philosophie-droit.asso.fr/APDpourweb/19.pdf, consulté le 3 aout 2017.
[1714] Le droit au respect de la vie privée et familiale est garanti par l'article 8 de la Convention européenne des droits de l'homme et interprété par la Cour européenne des droits de l'homme. Ce droit a été complété et renforcé par la convention nº 108.
[1715] Caroline Vallet, « Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs », *Droit et société* 2012/1 (n° 80), pp. 163-188.
[1716] Elise Vuillième, « Peut-on parler d'un droit à l'image en Grande-Bretagne ? », *LEGICOM*, 1995/4 (n° 10), pp. 41-44. URL : https://www.cairn.info/revue-legicom-1995-4-page-41.htm consulté le 11 décembre 2018.

Sous-section 2. Privacy right c/ protection de la vie privée

Entre l'ancien continent et l'Amérique, la protection de la vie privée et le *Privacy right* semblent issus de deux traditions juridiques différentes[1717], voire de parcours historiques différents. En France, l'article 17 de la Constitution de 1791 limitait les délits de presse à la provocation aux crimes et délits, à la calomnie volontaire contre les fonctionnaires publics et aux « calomnies et injures contre quelques personnes que ce soit relatif aux actions de leur vie privée »[1718]. Mais la vie privée n'est pas citée dans les lois sur la presse de la III[e] République et il faudra attendre 1970 pour qu'une loi protège la vie privée[1719].

Le parcours du droit américain apparaît très différent et n'a pas abouti à une loi (qu'elle soit fédérale ou d'État) protégeant la vie privée[1720]. Le « *right to privacy* » apparaît comme un droit constitutionnel, rattaché au IV[e] Amendement[1721], suite à deux décisions de la Cour Suprême : *Griswold c/ Connecticut*[1722] sur l'emploi de moyens contraceptifs par des personnes mariées, un raisonnement analogue est utilisé en 1973 dans la décision *Roe c/ Wade*[1723] sur l'avortement et *Katz v. USA*[1724], sur les écoutes téléphoniques qui ont fait également l'objet de la décision *Berger v. New York*[1725].

Le professeur William Prosser[1726] a recensé quatre infractions pouvant porter atteinte à la protection de la vie privée : l'intrusion physique dans un lieu ; la divulgation publique de faits privés ; la présentation d'une personne sous un jour trompeur ou défavorable ; et l'appropriation

---

[1717] Jean-Louis Halpérin, « Protection de la vie privée et *privacy* : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015/3 (n° 48), pp. 59-68.

[1718] Jean-Louis Halpérin, « Diffamation, vie publique et vie privée en France de 1 789 à 1 944 », *Droit et Cultures*, 2013/1, 65, p. 149.

[1719] Par la création d'un article 9 dans le Code civil instaurant un droit au respect de la vie privée (Article 22 de la loi n°70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens).*

[1720] Jean-Louis Halpérin, « Protection de la vie privée et *privacy* : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015/3 (n° 48), pp. 59-68.

[1721] Texte du IV[e] amendement : "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

Traduction française : « Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir ».

[1722] US Supreme Court, 381 U.S. 479, *Griswold v. Connecticut* (n°. 496), June 7, 1965.

[1723] US Supreme Court, 410 U.S. 113, *Roe v. Wade* (n°. 70-18), January 22, 1973.

[1724] US Supreme Court, 389 U.S. 347, *Katz v. United States* (n°. 35), December 18, 1967.

[1725] US Supreme Court, 388 U.S. 41, *Berger v. New York* (n°. 615), June 12, 1967.

[1726] Cité par David Korzenik, « La protection des droits de la personnalité aux États-Unis et en Grande-Bretagne : aspects de droit comparé », *LEGICOM* 2009/2 (n° 43), pp. 51-55.

du nom ou de l'image d'une personne à des fins commerciales. L'article 8 de la Convention européenne des droits de l'homme englobe d'autres notions : la confidentialité et toutes les atteintes à la vie privée réalisées par un gouvernement ou les forces de police.

Aux États-Unis d'Amérique, la *privacy* est protégée par la Constitution pour les atteintes par l'État, pas pour les atteintes par les particuliers. Les citoyens sont protégés contre les intrusions de la police et du gouvernement, mais la Constitution ne dit rien des atteintes par les particuliers. Les recours contre les intrusions privées et les atteintes à la *privacy* se trouveront dans la Common Law des États-Unis. La *privacy law* n'a pas valeur constitutionnelle concernant la conduite des citoyens[1727]. En Europe, la protection de la vie privée est assurée tant contre les atteintes des citoyens que de l'État par l'article 8 de la Convention européenne des droits de l'homme.

Au XIX[e] siècle, Samuel D. Warren et Louis D. Brandeis[1728] décrivent la nature du droit à la vie privée dans la Common Law par analogie avec la protection contre la diffamation ou la calomnie, ou avec le droit de propriété et une rupture du contrat de confiance. Ils enracinent cette protection dans la tradition. Aux États-Unis, sa consécration par les tribunaux ne date que de 1905[1729]. Les termes *privacy*, *intimacy*, *self*, concernent l'existence d'une personne, sa liberté, son « *droit d'être laissé tranquille* »[1730], il s'agit d'un droit personnel dont les limites sont fixées par des normes sociales, droit protégé par le IV[e] amendement. La protection de la vie privée et des données personnelles relève, quant à elle, d'un contrat privé plus que de lois générales comme elles peuvent exister en Europe. Dans un rapport américain de 1 977[1731], quatre mesures de protection étaient recommandées : *notice* (information) : informer les individus des pratiques et des finalités de la collecte et du traitement de données permettant d'identifier des personnes ; *access* (accès) : l'individu doit avoir accès aux banques de données qui le concernent, et pouvoir corriger ou éliminer certaines données ; *consent and choice*

[1727] Ibid.

[1728] Louis D. Brandeis, Samuel D. Warren, "The right to privacy", in *Harvard Law Review,* 4, 1890, pp. 193-220, (traduction en Français par Françoise Michaut disponible à l'URL : http://www.cliothemis.com/Louis-D-Brandeis-Samuel-D-Warren consulté le 26 mars 2018).

[1729] Jean-Louis Halpérin, « L'essor de la *"privacy"* et l'usage des concepts juridiques », *Droit et société*, 2005/3 (n° 61), pp. 765-782. URL : https://www.cairn.info/revue-droit-et-societe-2005-3-page-765.htm consulté le 26 mars 2018.

[1730] "*It has been recognized that this freedom not to be compelled to share our confidence with others is the very hallmark of free society*". US Supreme Court of Justice, Gérard La Forest, *R. v. Duarte*, 1990.
Traduction : « On a reconnu que cette liberté de ne pas être forcé à partager nos affaires confidentielles avec d'autres est le véritable symbole d'une société libre ».

[1731] *Personal Privacy in an Information Society,* The Report of the Privacy Protection Study Commission, July, 1977.

(consentement et choix) : l'individu doit pouvoir exprimer son accord ou désaccord sur la collecte et la diffusion, à des tiers notamment, de données personnelles, et sur la durée de leur conservation ; *security* (sécurité); l'information doit être exacte, protégée efficacement contre toute entreprise frauduleuse, le vol, la disparition. La *Federal Trade Commission* a ajouté, dans son rapport de 1998[1732], le principe de sanction effective des infractions à ces principes (*enforcement*). Ces critères reviennent à affirmer que toute organisation qui collecte des données personnelles en est responsable, et qu'elle doit clairement définir les procédures de correction et de compensation. Ces recommandations ne se traduisent pas dans une loi, mais dans des clauses générales d'utilisation présentées par les sociétés collectant des données personnelles, donc dans un contrat d'adhésion. Dans la présentation de son rapport, la commission précise : « *La Commission a été impliquée dans les problèmes de confidentialité en ligne pratiquement depuis qu'il existe une place de marché en ligne et a organisé une série d'ateliers et d'audiences sur ces questions. À chaque fois, l'objectif de la Commission a été d'encourager et de faciliter une autorégulation efficace comme approche privilégiée pour protéger la vie privée des consommateurs en ligne. Ces efforts sont basés sur la conviction qu'une plus grande protection de la vie privée sur le WEB permet non seulement de protéger les consommateurs, mais aussi d'augmenter la confiance des consommateurs et, finalement, leur participation dans le commerce en ligne* »[1733].

Aux États-Unis d'Amérique, la protection des données personnelles reste donc du domaine contractuel, même si les litiges en résultant peuvent faire l'objet de procès et donc créer des précédents dans un pays de *common law*. De façon similaire, au Royaume-Uni, il n'existe pas de droit général à la vie privée[1734]. Le « *right to privacy* », lorsqu'aucune des parties ne peut être assimilée à l'État, est régi par les règles de responsabilité civile ou le régime des « *torts* » de common law. Le « tort » exige un comportement fautif et un dommage et le dommage doit découler du comportement fautif. Le « *right to privacy* » s'est principalement articulé autour de quatre comportements fautifs : l'intrusion dans la vie privée (cueillette d'informations par la presse) ; la publication de faits privés ; la présentation d'une personne sous un jour défavorable

[1732] *Privacy online: a Report to Congress*, Federal Trade Commission, June 1998.
[1733] "*The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace and has held a series of workshops and hearings on such issues. Throughout, the Commission's goal has been to encourage and facilitate effective selfregulation as the preferred approach to protecting consumer privacy online. These efforts have been based on the belief that greater protection of personal privacy on the WEB will not only protect consumers, but also increase consumer confidence and ultimately their participation in the online marketplace*." Traduit en français par l'auteur.
[1734] Éric Barendt, « La protection de la vie privée en Angleterre », *LEGICOM* 1999/4 (nº 20), pp. 115-120.

(« *false light* », apparenté à la diffamation) et ; l'appropriation du nom ou de l'image d'une personne[1735].

Aux États-Unis, la liberté d'expression, protégée par le premier amendement, prime sur la protection de la vie privée. Dès que la Cour suprême constate qu'un écrit ou un discours est d'intérêt général, les protections constitutionnelles rendent caduques les poursuites pour atteintes à la vie privée. En Europe, dans une telle situation, la Cour européenne des droits de l'homme va rechercher un équilibre entre l'atteinte à la vie privée et la liberté d'expression si l'information divulguée est considérée d'intérêt général[1736].

La tradition britannique, comme d'ailleurs la tradition scandinave, reconnaît aux citoyens des droits spécifiques, plutôt que des droits de caractère général. L'incorporation de la Convention européenne des droits de l'homme dans le *Human Rights Act* de 1998[1737] a défini dans le droit britannique une charte des droits fondamentaux. La vie privée reste plutôt protégée par des textes ponctuels. Il existe une tradition de protection non juridique des libertés individuelles. La tradition juridique britannique fait face aux problèmes de la vie privée dans la société d'information de manière fragmentée. La réglementation spécifique à l'égard des nouveaux moyens de communication est confrontée à chaque situation, tel qu'elle évolue. L'autoréglementation des acteurs qui pourraient s'ingérer dans la vie privée des particuliers, est privilégiée au vote de lois. Cette solution est moins contraignante pour l'administration et est plus flexible. Le droit mou (*soft law*) ainsi mis en place (codes de déontologie, chartes d'éthique) peut être justifié davantage par des intérêts commerciaux que par le souci de protéger la vie privée, ainsi que le démontre les modifications nombreuses et fréquentes apportées aux conditions générales d'utilisation proposées tant par Facebook que Google, grands collecteurs de données personnelles.

[1735] Pierre Trudel, « La protection de la vie privée et de l'image aux États-Unis », dans *Institut de formation continue du Barreau de Paris, Liberté de presse, respect de la vie privée et de l'image en droit comparé*, Supplément de la Gazette du Palais, 1992, pp. 14-24.

[1736] François Saint-Pierre, « Respect de la vie privée versus droit à l'information : un point utile sur la jurisprudence de la Cour européenne des droits de l'homme », 27 février 2015, *Dalloz actualité,* URL : https://www.dalloz-actualite.fr/chronique/respect-de-vie-privee-versus-droit-l-information-un-point-utile-sur-jurisprudence-de-cour- consulté le 12 avril 2018.

[1737] *Human Rights Act* 1998 Chapter 42, *An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes*.

En Europe, la protection de la vie privée est garantie par l'article 8 de la Convention européenne de sauvegarde des droits et libertés fondamentales[1738]. La Convention n° 108[1739] définissait, avant la directive 95/46/CE, des règles de protection des données à caractère personnel proches des règles de la loi n° 78-17 informatique et libertés. Le Règlement général sur la protection des données entrant en application le 25 mai 2018 redéfinit cette protection en y intégrant la notion de consentement, de droit à l'oubli et de la nécessité de sécurité des centres stockant ces informations. Mais au-delà des convergences attestées, les spécificités nationales des visions des droits et libertés doivent nécessairement être prises en compte, à peine d'aboutir à des généralisations périlleuses. Ainsi, la France n'a ratifié la convention européenne des droits de l'homme qu'en 1974, lors de la présidence intérimaire de M. Alain Poher suite au décès du Président Georges Pompidou, avec des déclarations et réserves portant sur les articles 5, 6, 10 et 15[1740]. La République d'Autriche, le gouvernement du Royaume de Grèce ainsi que le gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord ont également adhéré à cette convention avec des réserves territoriales pour le Royaume-Uni, réserves levées pour certains territoires, mais depuis le gouvernement de David Cameron, la prédominance de la Convention sur les lois du Royaume-Uni semble poser des problèmes aux gouvernements.

Avec la signature du traité de Lisbonne, l'Union européenne « adhère à la Convention » et se place ainsi sous la juridiction de la Cour européenne des droits de l'homme. Mais alors que tous les États membres ont adhéré individuellement à la convention, cette adhésion de l'Union européenne est retardée par un avis de la Cour de justice de l'Union européenne[1741]. La Cour estime que le projet d'adhésion de l'Union européenne à la Convention européenne des droits de l'homme ne respecte ni les caractéristiques essentielles et spécifiques de l'Union européenne, en particulier son autonomie, ni les conditions posées par le Traité pour l'adhésion[1742].

[1738] Art. 8, § 1er de la Convention européenne de sauvegarde des droits et libertés fondamentales « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

[1739] Conseil de l'Europe, Série des traités européens – n° 108, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981.

[1740] Voire annexe 1, le fac-similé de la ratification publiée au Journal officiel du 14 mai 1974.

[1741] Avis 2/13 de la Cour de justice de l'Union européenne (assemblée plénière) du 18 décembre 2014. « *Avis rendu en vertu de l'article 218, paragraphe 11, TFUE – Projet d'accord international – Adhésion de l'Union européenne à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales – Compatibilité dudit projet avec les traités UE et FUE* ». Dans la procédure d'avis 2/13, ayant pour objet une demande d'avis au titre de l'article 218, paragraphe 11, TFUE, introduite le 4 juillet 2013 par la Commission européenne.

[1742] « *À la lumière de l'ensemble des considérations qui précèdent, il convient de constater que l'accord envisagé, en tant que :*

« – il est susceptible de porter atteinte aux caractéristiques spécifiques et à l'autonomie du droit de l'Union, dans la mesure où il n'assure pas la coordination entre l'article 53 de la CEDH et l'article 53 de la Charte, ne prévient

Le traité de Lisbonne a par ailleurs rendu contraignante la Charte des Droits fondamentaux de l'Union européenne, adoptée en décembre 2000. Deux États membres, la Pologne et le Royaume-Uni ont restreint pour leur part la contrainte de cette charte[1743] en refusant à la Cour de justice de l'Union européenne le pouvoir de juger la compatibilité des lois nationales et des pratiques administratives de ces pays au regard des obligations de la charte. Avec le Brexit, le problème ne se posera plus pour le Royaume-Uni qui ne reconnaîtra plus la compétence ni la suprématie de la Cour de justice de l'Union européenne[1744]. Il appartiendra à la Commission européenne de vérifier l'adéquation du Royaume-Uni post-Brexit.

La Charte des Droits fondamentaux de l'Union européenne différencie dans ses articles 7 et 8, le respect de la vie privée et familiale de la protection des données personnelles[1745]. La notion de vie privée et familiale n'est pas clairement définie dans les textes, et permet une large interprétation par les tribunaux, alors que la notion de données personnelles est clairement

---

pas le risque d'atteinte au principe de la confiance mutuelle entre les États membres dans le droit de l'Union et ne prévoit aucune articulation entre le mécanisme institué par le protocole no 16 et la procédure de renvoi préjudiciel prévue à l'article 267 TFUE ;

« – il est susceptible d'affecter l'article 344 TFUE, dans la mesure où il n'exclut pas la possibilité que des litiges entre les États membres ou entre ces derniers et l'Union, relatifs à l'application de la CEDH dans le champ d'application matériel du droit de l'Union, soient portés devant la Cour EDH ;

« – il ne prévoit pas des modalités de fonctionnement du mécanisme du codéfendeur et de la procédure de l'implication préalable de la Cour qui permettent de préserver les caractéristiques spécifiques de l'Union et de son droit, et

« – il méconnaît les caractéristiques spécifiques du droit de l'Union concernant le contrôle juridictionnel des actes, actions ou omissions de l'Union en matière de PESC, dans la mesure où il confie le contrôle juridictionnel de certains de ces actes, actions ou omissions exclusivement à un organe externe à l'Union,

n'est pas compatible avec l'article 6, paragraphe 2, TUE ni avec le protocole no 8 UE ».

[1743] Protocole sur l'application de la Charte des droits fondamentaux de l'Union européenne à la Pologne et du Royaume-Uni, « *Article premier :*

« *1. La Charte n'étend pas la faculté de la Cour de justice de l'Union européenne, ou de toute juridiction de la Pologne ou du Royaume-Uni, d'estimer que les lois, règlements ou dispositions, pratiques ou actions administratives de la Pologne ou du Royaume-Uni sont incompatibles avec les droits, les libertés et les principes fondamentaux qu'elle réaffirme.*

« 2. En particulier, et pour dissiper tout doute, rien dans le titre IV de la Charte ne crée des droits justiciables applicables à la Pologne ou au Royaume-Uni, sauf dans la mesure où la Pologne ou le Royaume-Uni a prévu de tels droits dans sa législation nationale.

« Article 2 :

« Lorsqu'une disposition de la Charte fait référence aux législations et pratiques nationales, elle ne s'applique à la Pologne ou au Royaume-Uni que dans la mesure où les droits et principes qu'elle contient sont reconnus dans la législation ou les pratiques de la Pologne ou du Royaume-Uni ».

[1744] Discours de Theresa May, Premier ministre, du 17 janvier 2017.

[1745] Charte des droits fondamentaux de l'Union européenne, « *Article 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.*

« Article 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 ».

définie par les textes européens ou locaux. Dans la directive 95/46/CE, la définition en est la suivante : « *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* ». Le nouveau Règlement général sur la protection des données [1746] a modifié et complété cette définition par : « *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* » prenant en compte les modifications techniques apparues depuis la directive. Le règlement a étendu la notion de fichier de données à caractère personnel à « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* ». Ainsi, des fichiers liés entre eux contenant des parties de données seront considérés comme fichier de données à caractère personnel dès lors que le rapprochement des données desdits fichiers permettra d'identifier une personne physique. Le règlement ne considère pas un fichier isolé, mais un ensemble de fichiers pour déterminer si ces fichiers contiennent des données à caractère personnel permettant d'identifier une personne physique, que ces fichiers soient gérés par une seule entité ou par plusieurs entités indépendantes.

Cette possibilité répond à la préoccupation de la Commission de l'informatique et des libertés qui dans son 14e rapport annuel publié en 1994. Elle se disait « préoccupée » par la toile qui se tissait peu à peu autour de chaque individu et par l'utilisation des systèmes d'information guidée par le seul souci de l'efficacité qui conduisait à conserver un très grand nombre « de traces » informatiques[1747].

En effet, la société numérique est un creuset favorisant certaines libertés, mais elle reste un défi pour d'autres libertés, notamment individuelles. En1978, le législateur avait identifié ce défi et

[1746] 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).*

[1747] Cité par Michèle Voisset, « Droit au respect de la vie privée et société de l'information », pp. 249-254, in *La protection de la vie privée dans la société d'information*, Presses Universitaires de France, http://asmp.fr/travaux/gpw/Internetvieprivee/rapport3/chapitr16.pdf consulté le 1 juillet 2016.

l'avait adressé au travers de la loi « Informatique, fichiers et libertés »[1748] et créé la CNIL, chargée de veiller à l'équilibre entre développement technologique et protection des libertés individuelles. Le rejet de l'interconnexion des fichiers administratifs par utilisation du NIR avait anticipé certains dangers potentiels pour les libertés, dangers liés au développement, à l'époque, des technologies de l'information. Dans les années 1970, l'informatique était une technique de traitement de l'information, d'où son nom en français dérivé de « information » et « automatique ». Il est à remarquer que pour les Anglo-saxons, l'informatique est restée un « traitement de données » ou « *data processing* », voire une science des ordinateurs ou « *computer science* ». Le législateur français avait bien perçu le risque de l'emprise de la technique sur les libertés au travers de l'article 1er de la loi : « *L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Depuis sa promulgation, la loi s'est adaptée aux progrès des technologies, mais aussi aux besoins des administrations et des entreprises. Quelques lois, décrets ou arrêtés sont venus assouplir la loi originelle[1749] et malgré des mises en garde de la CNIL[1750], l'efficacité administrative a prévalu sur la protection des libertés et le respect de la vie privée. Alors que l'interconnexion des fichiers administratifs par utilisation du NIR est à l'origine de la loi de 1978, l'utilisation du NIR par les administrations des Finances (Direction générale des Impôts, Comptabilité Publique, Douanes et droits indirects) est autorisée par l'article 107 de la loi de Finances pour 1999. Le Conseil constitutionnel[1751] a rejeté les griefs des députés et des

[1748] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, publiée au JORF du 7 janvier 1978 p. 227.

[1749] Les articles 26 et 27 de la loi n° 78-17 concernant les autorisations de certains traitements administratifs ont été modifiés par la loi n° 2004-801 du 6 août 2004 (Cf. Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 1. § 1 -B)1) L'assouplissement de la loi informatique et libertés).

[1750] Avant les modifications apportées par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, les avis de la CNIL portant sur un projet de loi ne pouvaient être rendus publics que si le Président de la Commission permanente de l'une des deux assemblées en faisait la demande (article 11-4°)-a) de la loi "informatique et libertés"). L'article 59 de la loi n° 2016-1321 avait ajouté la phrase « *L'avis de la commission sur un projet de loi est rendu public* », cette phrase a été supprimée par l'article 40 de la loi n° 2017-55 du 20 janvier 2017 *portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes.* Par contre, il a été maintenu : « *lorsqu'une loi prévoit qu'un décret ou un arrêté est pris après avis de la commission, cet avis est publié avec le décret ou l'arrêté* ».
Sur le site de la CNIL, il est possible de trouver :
Délibération n°2015-078 du 5 mars 2015 *portant avis sur un projet de loi relatif au renseignement* ;
Commission nationale de l'informatique et des libertés, Délibération n° 2016-292 du 29 septembre 2016 *portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité* (saisine n° 1979541).
Mais pas sur le projet de loi de finances pour 1999 et son article 107 qui autorise l'administratin fiscale à utiliser le NIR.

[1751] Conseil constitutionnel, Décision nº 98-405 DC du 29 décembre 1998 *Loi de finances pour 1999*.

sénateurs concernant cet article, car il a estimé que les garanties énoncées dans la loi étaient suffisantes[1752].

Le décret du 14 décembre 1999[1753] précise que ce NIR n'est communiqué par l'employeur ou les organismes de prestations sociales que lors de la transmission des données légalement obligatoires, comme le sont le salaire annuel de tout employé ou les indemnités versées par les organismes sociaux. Le décret du 4 janvier 2000[1754] pris pour l'application de cette disposition de la loi de Finances pour 1999, traite des « mesures de sécurité » pour l'application de tout ce dispositif, surveillées par le Haut Fonctionnaire de Défense du Ministère de l'Économie, des Finances et de l'Industrie. Ces décrets renforcent, en apparence, les pouvoirs de la CNIL, qui

---

[1752] Conseil constitutionnel, Décision n° 98-405 DC du 22 décembre 1998, considérants n^os 60 et suivants : « - *SUR L'ARTICLE 107 :*
60. Considérant que l'article 107 se borne à permettre à la direction générale de la comptabilité publique, à la direction générale des impôts et à la direction générale des douanes et des droits indirects d'utiliser, en vue d'éviter les erreurs d'identité et de vérifier les adresses des personnes, le numéro d'inscription au répertoire national d'identification des personnes physiques, dans le cadre des missions respectives de ces directions, ainsi qu'à l'occasion des transferts de données opérés en application des articles L.81.A et L.152 du livre des procédures fiscales ; que les trois directions précitées ne peuvent collecter, conserver ou échanger entre elles les numéros d'inscription au répertoire national d'identification des personnes physiques que pour mettre en œuvre des traitements de données relatifs à l'assiette, au contrôle et au recouvrement de tous impôts, droits, taxes, redevances ou amendes ; que toutes les informations recueillies à l'occasion de ces opérations sont soumises à l'obligation de secret professionnel prescrite par l'article L.103 du livre des procédures fiscales ; que la Commission nationale de l'informatique et des libertés a la faculté d'intervenir "lorsque la mise en œuvre du droit de communication prévu aux articles L.81.A et L.152 s'avère susceptible de porter une atteinte grave et immédiate aux droits et libertés visés à l'article 1er de la loi n° 78-17 du 6 janvier 1978..." ; qu'en outre, le législateur n'a pu entendre déroger aux dispositions protectrices de la liberté individuelle et de la vie privée établies par la législation relative à l'informatique, aux fichiers et aux libertés ; que si, en vertu des nouvelles dispositions, les directions précitées du ministère de l'économie et des finances mentionnent le numéro d'identification des personnes physiques lorsqu'elles communiquent, en application des dispositions de l'article L.152 du livre des procédures fiscales, des informations nominatives aux organismes et services chargés de la gestion d'un régime obligatoire de base de sécurité sociale et aux institutions mentionnées au chapitre 1er du II du livre IX du code de la sécurité sociale, ces communications doivent être strictement nécessaires et exclusivement destinées à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de l'assiette et du montant des cotisations et contributions, ainsi qu'à leur recouvrement ; que la méconnaissance de ces dispositions sera réprimée dans les conditions prévues par le V de l'article 107 ;
« 61. Considérant, enfin, que l'utilisation du numéro d'inscription au répertoire national d'immatriculation des personnes physiques a pour finalité d'éviter les erreurs d'identité, lors de la mise en œuvre des traitements de données en vigueur, et ne conduit pas à la constitution de fichiers nominatifs sans rapport direct avec les opérations incombant aux administrations fiscales et sociales ;
62. Considérant qu'eu égard à l'objet de l'article 107 et sous réserve des garanties dont est assortie sa mise en œuvre, il y a lieu de rejeter le grief tiré dans les deux requêtes de la méconnaissance des exigences constitutionnelles relatives à la protection de la vie privée et de la liberté individuelle ».

[1753] Décret n° 99-1047 du 14 décembre 1999 *pris pour l'application de l'article 107 de la loi de finances pour 1999 (n° 98-1266 du 30 décembre 1998) relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects,* publié au JORF n° 290 du 15 décembre 1999 p. 18665.

[1754] Décret n° 2000-8 du 4 janvier 2000 *pris pour l'application de l'article L.288 du livre des procédures fiscales*, publié au JORF n° 5 du 7 janvier 2000 p. 294.

dispose de la possibilité d'obtenir la destruction immédiate de données par voie d'injonction, et qui peut, en cas de refus, saisir par voie de référé, le Président du Tribunal de Grande Instance de Paris et d'une manière plus générale, se voit reconnaître des pouvoirs de surveillance renforcés.

L'article 107 de la loi de finances pour 1999 s'inscrit dans les glissements progressifs vers l'efficacité des procédures de contrôles administratives et l'intrusion dans la vie privée des personnes physiques, restreignant ainsi le champ de la sphère privée. Il en est ainsi de la loi du 1er juillet 1994[1755] qui permet, à des fins de recherche, la collecte et le traitement automatique des données de santé et qui relativise ainsi le secret médical, secret reconnu comme faisant partie de l'intimité de la vie privée.

La protection de la vie privée apparaît implicitement en 1977 dans la décision du Conseil constitutionnel concernant la fouille des véhicules[1756], sur le fondement de la liberté individuelle dont l'article 66 de la Constitution confie la garde à l'autorité judiciaire. Le Conseil constitutionnel admet le droit au respect de la vie privée en 1995[1757]. En 1999, avec la décision relative à la loi portant création d'une couverture maladie universelle[1758], le Conseil constitutionnel rattache la protection de la vie privée à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789. En 2010, le Conseil constitutionnel admet que ce droit relève des droits et libertés que la Constitution garantit[1759].

Ainsi, la protection de la vie privée se voit restreinte de par la lutte contre la fraude fiscale, l'administration fiscale devenant destinatrice de nombreuses informations considérées comme du domaine privé : le patrimoine, les revenus du travail ou les revenus mobiliers. Depuis 1982, l'article L.111 du Livre des Procédures fiscales permet d'accéder à certains renseignements sur les revenus et l'impôt sur le revenu d'autres contribuables qui dépendent de la même direction départementale. Pour des raisons de transparence, le patrimoine, les revenus des députés et

[1755] Loi nº 94-548 du 1er juillet 1994 *relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libert*és, publiée au JORF nº 152 du 2 juillet 1994 p. 9559.

[1756] Conseil constitutionnel, Décision n° 76-75 DC du 12 janvier 1977, *Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales.*

[1757] Conseil constitutionnel, Décision n° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, considérant n° 3 : « *la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* ».

[1758] Conseil constitutionnel, Décision nº 99-416 du 23 juillet 1999, *Loi portant création d'une couverture médicale universelle*.

[1759] Conseil constitutionnel, Décision n° 2010-25 QPC du 16 septembre 2010, *M. Jean-Victor C. [Fichier empreintes génétiques]*, considérants nºs 6 et 16.

sénateurs sont publics et peuvent être consultés dans la préfecture de leur circonscription élective.

Compte tenu des localisations des principales sociétés de l'Internet dans des pays de droit anglo-saxon (Royaume-Uni, Irlande ou États-Unis d'Amérique), la protection légale de la vie privée prévue dans l'Union européenne peut se trouver amoindrie par des sociétés pratiquant une protection contractuelle plutôt que législative. Le consentement préalable prévu par le Règlement général sur la protection des données, relevant du droit contractuel, donc du droit privé civil, plutôt que du droit administratif associé au pouvoir de redressement et d'effacement, est un début de réponse à cette problématique. Mais la vigilance des utilisateurs reste le moyen le plus efficace de protéger la vie privée dans une société où le mur de cette vie privée devient transparent. Comme le souhaitaient deux sénateurs[1760] dès 2009, « *la première réponse réside, à l'évidence, dans l'implication pleine et entière des individus dans leur propre protection* ». Ils souhaitent la transformation de l'« *Homo Sapiens* » en un « *Homo Numericus* » libre et éclairé, protecteur de ses propres données, et préconisent de « *renforcer la place accordée à la sensibilisation aux questions de protection de la vie privée et des données personnelles dans les programmes scolaires* ». La protection de la vie privée et des données à caractère personnel et individuel passe par l'éducation dès le plus jeune âge des internautes afin d'éviter l'exposition de cette vie privée sur Internet.

[1760] Yves Détraigne et Anne-Marie Escoffier, *proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique*, enregistrée à la Présidence du Sénat le 6 novembre 2009.

Section 2. L'exposition de la vie privée au travers de l'activité sur Internet

Toute activité d'une personne physique est enregistrée, soit par des traces laissées lors des accès à l'Internet, soit par les enregistrements liés aux moyens de paiement électronique, soit par les images captées par les caméras de surveillance déployées dans de nombreux lieux publics, soit par la collecte et le traitement des données fournies par les objets connectés, mais aussi par les informations « données » volontairement sur les réseaux sociaux[1761]. Toute donnée collectée peut devenir une donnée à caractère personnel[1762]. Face à cette surveillance multiforme, l'anonymisation de certaines actions peut sembler un moyen d'échapper à « *Big Brother* ». Comme l'écrivait en 1997, Timothy O'Hagan[1763], relatant un article de Warren et Brandeis, paru en 1890[1764] : « *Plus d'un siècle plus tard, "les inventions récentes et les méthodes du marché", notamment la surveillance électronique ainsi que la collecte et la diffusion de données électroniques représentent une menace plus grande encore pour l'intimité de l'individu dans toutes les sociétés développées* ». Ainsi, si la menace concernant la violation de la vie privée n'est pas récente ni apparue avec les techniques numériques, cette menace se trouve renforcée dans la société numérique de par les moyens disponibles pour la surveillance des individus et la collecte massive des données à caractère personnel.

Sous-section 1. Le dévoilement de la vie privée

La protection de la vie privée et des données à caractère personnel, primordiale dans une société de l'information, est fragilisée par le développement des réseaux sociaux et des traces laissées sur le réseau Internet par les internautes, volontairement ou non. Le problème n'est plus principalement celui d'un État qui accumule des données et croise des fichiers, mais aussi celui d'informations sensibles émanant des individus eux-mêmes en contrepartie de services volatils.

[1761] Caroline Vallet, « Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs », *Droit et société* 2012/1 (nº 80), pp. 163-188.
[1762] Thomas Bizet, « Vers une inflation des données personnelles ? », 13 août 2014, *Village de la justice,* URL : https://www.village-justice.com/articles/Vers-une-inflation-des-donnees,17539.html consulté le 6 décembre 2017.
[1763] Timothy O'Hagan, « Public et privé, hommes et femmes » in *Archives de Philosophie du droit*, tome 41 (1997), pp. 43-51, en ligne à http://www.philosophie-droit.asso.fr/APDpourweb/173.pdf, consulté le 3 aout 2017.
[1764] Samuel D. Warren et Louis D. Brandeis, 1890, « Le droit à la vie privée » réimprimé in *The Philosophical Dimension of Privacy*, Schoeman, 1984.

Ces informations une fois collectées se retrouvent stockées et dotées d'une résilience quasi-infinie[1765]. C'est ainsi qu'AMAZON qui collecte les informations de paiement pour un achat en ligne, conserve au-delà du besoin de la transaction, les différents moyens de paiement utilisés, que leur date de validité soit expirée ou non[1766].

§ 1 - Les traces personnelles

A) Les traces liées à une activité sur Internet

Depuis le développement de l'informatique, pour des raisons techniques de sécurité, tous les programmes informatiques ou une majorité d'entre eux, enregistrent les événements importants pour leur fonctionnement. Ces enregistrements sont consignés dans un journal, en anglais « *log* ». Ces enregistrements permettent de connaître l'origine d'une modification dans les bases de données, de revenir à un état stable en cas d'erreur de programme ou de s'assurer et garantir la cohérence des données en cas de modifications conjointes[1767]. Ainsi toute installation d'un programme particulier sur un PC fait l'objet d'un log, d'une journalisation, ce fichier étant utilisé lors de la désinstallation dudit programme pour effacer les éléments devenus non utiles. Ces journaux d'origine technique peuvent être lus, collectés et ils permettent de connaître l'activité dudit PC, et donc, statistiquement son profil d'utilisation.

Avec le développement d'Internet et des moteurs de recherche, toute activité sur Internet fait l'objet d'enregistrements contenant, a minima, l'adresse IP du dispositif utilisé pour accéder au réseau. Pour la Commission de l'informatique et des libertés[1768], cette adresse IP constitue une

[1765] Fabien Granjon, « De quelques pathologies sociales de l'individualité numérique. Exposition de soi et autoréification sur les sites de réseaux sociaux », *Réseaux*, 2011/3 (n° 167), pp. 75-103. URL : https://www.cairn.info/revue-reseaux-2011-3-page-75.htm consulté le 6 décembre 2017.

[1766] Voir Annexe 4 Liste des cartes de crédit par AMAZON.

[1767] Ce fichier journal permet aux systèmes de base de données relationnels d'assurer une cohérence des bases en cas de modifications complexes au cours d'une transaction, les modifications demandées ne sont pas réellement effectuées, mais seulement consignées et ne sont effectives que lorsque l'utilisateur en ayant terminé avec la transaction en demande la réalisation par un ordre COMMIT.
Ce fichier est également utilisé lors d'une opération de maintenance pour revenir à un état stable de la base en annulant toutes les transactions effectuées depuis un précédent état stable.

[1768] Commission Nationale de l'Informatique et des Libertés, Délibération n°2006-294 du 21 décembre 2006 *autorisant la mise en œuvre par l'Association de Lutte contre la Piraterie Audiovisuelle (LPA) d'un traitement de données à caractère personnel ayant pour finalité principale la recherche des auteurs de contrefaçons audiovisuelles* : « *la Commission observe qu'en tant que telle, l'utilisation d'un logiciel de "peer to peer" aux fins de procéder à la constatation d'un acte de contrefaçon constitue un traitement de données à caractère personnel notamment dans la mesure où les agents assermentés procèdent à la collecte, la consultation, la conservation et*

donnée à caractère personnel[1769], et à ce titre doit être protégée par la loi nº 78-17 relative à l'informatique et aux libertés et son article 2. Pour les juges, cette interprétation n'est pas évidente[1770]. En 2009, dans un rapport d'information[1771], des sénateurs recommandent que soit affirmé sans ambiguïté que l'adresse IP constitue une donnée à caractère personnel. En 2014, le Tribunal de Grande Instance de Paris a confirmé dans un jugement en référé[1772] que l'adresse IP est bien une donnée à caractère personnel infirmant les arrêts de 2007[1773] de la Cour d'appel de Paris. En 2016, la Cour de cassation[1774] a également estimé que l'adresse IP qui permet d'identifier indirectement une personne physique, est une donnée à caractère personnel, de sorte que sa collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la CNIL. Dès 2008, la Cour de justice de l'Union européenne avait confirmé le statut de donnée personnelle de l'adresse IP[1775]. En l'occurrence, si l'adresse IP est une donnée à caractère personnel, son possesseur doit pouvoir demander l'application du droit d'accès prévu par l'article 39.I.4 de la loi nº 78-17 et donc avoir accès aux enregistrements de cette adresse ayant fait l'objet d'un traitement automatique[1776]. C'est

l'enregistrement de l'adresse IP des internaute qui constitue une donnée à caractère personnel puisqu'elle permet d'identifier indirectement la personne physique titulaire d'un abonnement à Internet ».

[1769] Pour la CNIL et l'ensemble des autorités de protection des données personnelles de l'Union européenne, l'adresse IP est une donnée à caractère personnel (https://www.cnil.fr/fr/ladresse-ip-est-une-donnee-caractere-personnel-pour-lensemble-des-cnil-europeennes 2 août 2007, consulté le 24 mars 2016).

[1770] En 2007, la cour d'appel de Paris a estimé que « *cette série de chiffres ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur* » (Cité par Viviane Gelles, « Adresse IP : donnée à caractère personnel ? », 28 août 2014, *Jurisexpert*, http://www.jurisexpert.net/adresse-ip-donnee-caractere-personnel/ consulté le 24 mars 2016 ; Cour d'Appel de Paris, arrêt du 27 avril 2007, 13e chambre, Section B, *Anthony G. c/SCPP* et arrêt du 15 mai 2007, 13e chambre, Section A, *Henri S. c/HCPP*). La Cour de cassation a, quant à elle, considéré que l'adresse IP est une donnée parmi d'autres insuffisante pour être qualifiée de donnée personnelle (Cour de Cassation, Chambre criminelle, du 5 septembre 2007, nº de pourvoi 07-81.031). En 2009, la troisième chambre du Tribunal de grande instance de Paris a affirmé sans ambiguïté que l'adresse IP est une donnée personnelle qui permet de retrouver la personne qui a mis en ligne un contenu (Tribunal de grande instance de Paris 3e chambre, 3e section, Jugement du 24 juin 2009 *Jean-Yves Lafesse et autres/Google et autres*).

[1771] *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information nº 441 (2008-2009) de M. Yves Détraigne et Mme Anne-Marie Escoffier, fait au nom de la commission des lois, déposé le 27 mai 2009.

[1772] Tribunal de grande instance de Paris, Ordonnance de référé 17 juillet 2014 *Chantal M./Crédit Lyonnais.*

[1773] Cour d'Appel de Paris, arrêt du 27 avril 2007, 13e chambre, Section B, *Anthony G. c/SCPP* et arrêt du 15 mai 2007, 13e chambre, Section A, *Henri S. c/HCPP*, Op. cit.

[1774] Cour de cassation, 1ère chambre civile, arrêt du 3 novembre 2016, *Cabinet Peterson / Groupe Logisneuf et autres : « les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la CNIL ».*

[1775] Cour de Justice de l'Union européenne (Grande chambre), arrêt du 29 janvier 2008, Affaire C-275/06 *Productores de Música de España (Promusicae) c/Telefónica de España SAU,* confirmé par CJUE (2e ch.) arrêt du 19 octobre 2016 affaire n° 582/14 *Patrick Breyer c/ Bundesrepublik Deutschland* .

[1776] Ibrahim Coulibaly, « Le puissant droit d'accès aux données à caractère personnel », 18 août 2014, *Village de la Justice*, URL : http://www.village-justice.com/articles/puissant-droit-acces-aux-donnees, 17541.html consulté le 24 mai 2016.

bien ce que confirme l'arrêt du Conseil d'État du 12 mars 2014, relatif à la sanction prononcée par la CNIL contre la société Pages Jaunes[1777]. Le Conseil d'État a jugé que la collecte par Pages Jaunes des adresses IP contenues dans les requêtes traitées par le site n'était pas légitime. Le Règlement général sur la protection des données [1778] clôt le débat sur le statut de l'adresse IP. En effet, il définit les données à caractère personnel[1779] comme « *toute information se rapportant à une personne physique identifiée ou identifiable ; 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* ». Aux termes du considérant n° 30 de ce règlement[1780], les adresses IP tout comme les *cookies* peuvent être utilisés par les serveurs pour créer des profils de personnes physiques et les identifier. En conséquence, puisque l'adresse IP est un des identifiants laissant des traces pouvant servir à identifier des personnes, il est une donnée à caractère personnel protégée par ce Règlement général sur la protection des données [1781].
Si l'adresse IP est une donnée systématiquement traçable de par la construction du réseau Internet et de son mode d'adressage, il existe d'autres données à caractère personnel qui transitent sur le réseau. Une partie de ces données est accessible de par la négligence ou l'inconscience des utilisateurs d'Internet.

B) Les traces dues à une attitude irresponsable des individus

Internet permet la connaissance de tout, par tout le monde, de manière quasi instantanée. Toute notre vie ou presque est consignée sur la toile, notre identité via les réseaux sociaux, nos

[1777] Conseil d'État, Arrêt du 12 mars 2014, Affaire N° 353193, *Pages Jaunes Groupe*.
[1778] Règlement UE 2016/679 du 27 avril 2016, applicable à compter du 25 mai 2018.
[1779] Règlement UE 2016/679 du 27 avril 2016, Art. 4 Définitions.
[1780] Règlement UE 2016/679 du 27 avril 2016, considérant n° 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. 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* »
[1781] Dominique Loyer-Bouez, « Fichiers informatisés : une adresse IP peut être une donnée à caractère personnel », 24 novembre 2016, *Au cœur du droit,* Éditions Francis Lefebvre – La Quotidienne, URL : https://www.efl.fr/droit/affaires/details.html?ref=ui-0fb53028-f6a9-4e70-be88-ce7b50bfe0dc consulté le 13 janvier 2018.

données de santé, nos résultats scolaires et universitaires, nos impôts, nos factures[1782]. En France, l'administration propose d'accéder aux informations administratives via un seul portail[1783]. Même si nous sommes allergiques aux réseaux sociaux et refusons de nous y inscrire, d'autres se chargent à notre place de nous y référencer : le commerçant en ligne qui nous enregistre dans sa base de données ; ENEDIS, anciennement ERDF, qui déploie des compteurs électriques intelligents, bientôt généralisés au nom des économies d'énergie, recensant tout ce que nous faisons (du point de vue électrique) et quand nous le faisons, et pouvant potentiellement agir sur certains de nos appareils électriques[1784] ou envoyer ces informations sur le réseau[1785] ; sans oublier l'ami qui nous prend en photo et nous identifie sur celle-ci quand il la dépose sur son mur.

En fait, nous sommes tous démunis face à cet outil de communication « impudique » et insidieux qu'est Internet. Compte tenu de l'effet parcellaire et morcelé immédiatement visible, nous n'avons pas encore pris conscience de l'emprise de ces technologies sur notre vie privée et de l'évolution induite de la notion de confidentialité. L'illusion d'anonymat qu'offrent Internet et la profusion de données disponibles est d'autant plus paradoxale que c'est exactement l'inverse qui se passe actuellement : la sphère privée devient de plus en plus difficile à maîtriser et à protéger de par la masse d'informations disponibles et collectées.

Le problème est de plus en plus complexe du fait de la technologie qui nous apporte cette connaissance globale. Les ordinateurs de plus en plus puissants permettent de traiter une masse quasi incommensurable et humainement inimaginable d'informations et peuvent trouver, dans ces informations, des structures qui sont tout, sauf apparentes ou évidentes. Le projet SAFARI avec son identifiant unique n'a plus de raison d'être, le traitement de milliers de données et leur corrélation devenue possible, renvoient l'identifiant unique au rang des accessoires surannés.

Devant cette technologie de traitement des données, certains comportements des individus semblent dangereux, inconséquents et inadaptés. Certaines applications, disponibles sur

---

[1782] Bénédicte Rey, « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique*, 2014/1 (Vol. 10), pp. 9-18. URL : https://www.cairn.info/revue-les-cahiers-du-numerique-2014-1-page-9.htm consulté le 15 janvier 2018.

[1783] https://franceconnect.gouv.fr/ .

[1784] Voire à ce sujet la page de présentation du compteur communiquant sur le site de ENEDIS à l'URL http://www.enedis.fr/compteur-communicant, consultée le 2 aout 2017.

[1785] Commission nationale de l'informatique et des libertés, Délibération n° 2012-404 du 15 novembre 2012 *portant recommandation relative aux traitements des données de consommation détaillées collectées par les compteurs communicants.*

Commission nationale de l'informatique et des libertés, Décision MED n° 2018- 007 du 5 mars 2018 *mettant en demeure la société DIRECT ENERGIE.*

Smartphone, Apple ou Android, nécessitent pour activer l'ensemble de leurs fonctionnalités, d'accéder à tout ou partie des données personnelles présentes sur ces Smartphones : données de localisation, carnet d'adresses, liste de contacts, ainsi que des données plus intimes telles que pression artérielle, activité physique, périodes de sommeil, etc. Ces données peuvent être soit déterminées par les applications installées et activées sur le Smartphone, soit produites via des objets connectés, *SmartWatch* par exemple, soit fournies directement par le propriétaire du Smartphone. Dans un rapport de 2012 de l'Assemblée nationale, les rapporteurs constataient une exposition inconsciente de la vie privée[1786], réalisée au travers des données fournies par les internautes eux-mêmes. Les réseaux sociaux, mais également de manière croissante tout un ensemble de services, reposent aujourd'hui sur l'exploitation d'informations personnelles, très largement volontairement fournies, et sur leur restitution partiellement enrichie. Cette restitution confère à ces services sens et valeur pour les individus eux-mêmes[1787]. Les individus ne sont plus seulement de possibles victimes d'intrusions, émanant d'institutions extérieures face auxquelles ils ne sauraient se défendre sans un arsenal juridique et réglementaire, mais ils deviennent des acteurs de premier plan de la production, de la diffusion et de la consommation d'informations[1788].

Ces applications ou services sont, en règle générale, mis à disposition gratuitement auprès des utilisateurs, la rémunération des sociétés éditrices de ces services provenant de la vente de données validées, calibrées et à fort potentiel marchand. Les sociétés fournissant ces services sont souvent, à l'origine, des start-up créées avec peu de moyens autour d'une idée originale. Une fois l'application réalisée, diffusée et validée par les utilisateurs, ces start-up sont rachetées pour plusieurs millions d'euros par des sociétés ou des investisseurs[1789]. La valeur de ces sociétés est liée à la valeur marchande des données collectées et au potentiel économique des profils de ses utilisateurs qui seront alors ciblés pour certaines offres. Le 13 juin 2016, Microsoft

[1786] « *Lors de ses travaux, la mission d'information a été frappée à plusieurs reprises par le fait que, de plus en plus, les citoyens exposent leur vie privée sur Internet, notamment les plus jeunes, et qu'ils le font sans en avoir toujours conscience. Quand ils en prennent conscience et souhaitent mieux protéger leurs droits, ces internautes sont confrontés à des difficultés techniques et juridiques et se retrouvent alors relativement isolés face aux grands groupes de l'Internet, que sont Google, Facebook ou Twitter* » (Patrick Bloche, Patrick Verchère, *Rapport d'information* déposé par la mission d'information commune sur les droits de l'individu dans la révolution numérique, enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011).

[1787] Grazia Cecere, Fabrice Le Guel, Fabrice Rochelandet, « Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique », *Réseaux*, 2015/1 (n° 189), pp. 77-101. URL : https://www.cairn.info/revue-reseaux-2015-1-page-77.htm consulté le 15 janvier 2018.

[1788] Bénédicte Rey, « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique* 2014 (Vol. 10), pp. 9-18.

[1789] Ulrich Hege, « L'évaluation et le financement des start-up Internet », *Revue économique*, 2001/7 (Vol. 52), pp. 291-312. URL : https://www.cairn.info/revue-economique-2001-7-page-291.htm consulté le 6 décembre 2017.

annonçait qu'il allait mettre 26,2 milliards de dollars pour prendre le contrôle de LinkedIn, créé en 2003, revendiquant 433 millions de membres dans le monde[1790], base riche de profils et de compétences professionnels.

Face à cette exposition de la vie privée via la fourniture volontaire ou la collecte insidieuse des données à caractère personnel, de nombreux organismes, dont la CNIL, fournissent des conseils et des manuels de bonne conduite[1791] à respecter pour éviter l'exposition involontaire de la vie privée, mais comme pour la protection contre les vers, virus ou chevaux de Troie, ces conseils sont peu ou prou respectés, voire mal connus. Par exemple, la CNIL a publié en 2014[1792], une fiche pratique concernant la publication de photos sur le réseau[1793]. Ces recommandations adressent l'attitude des individus face à un moyen de publication puissant et mal contrôlé. La Commission nationale de l'informatique et des libertés prévient les utilisateurs contre la possibilité de propagation des identifications sur une photo à l'ensemble des photos où l'individu apparaît, ainsi qu'à la possibilité de rapprochement des photos entre plusieurs sites ou prestataires. Dans sa lettre innovation et perspective n° 4[1794], la CNIL analyse le comportement des individus face au partage d'informations par tranche d'âge[1795]. Concernant

---

[1790] « *Microsoft rachète LinkedIn qui décolle en Bourse* », Challenges, publié le 13 juin 2016 à 14 h 46, à http://www.challenges.fr/Internet/20160613.CHA0490/microsoft-racheterait-linkedin.html, consulté le 2 juillet 2016.

[1791] Xavier Tannier, *Se protéger sur Internet, Conseils pour la vie en ligne,* 26 août 2010, Eyrolles.
Assistance Orange, « Menaces sur Internet : se protéger efficacement », URL : https://assistance.orange.fr/ordinateurs-peripheriques/installer-et-utiliser/la-securite/risques-et-prevention/virus/menaces-sur-internet-se-proteger-efficacement_41287-42102 consulté le 15 janvier 2018.
Le Monde.fr, « Comment protéger sa vie privée sur Internet ? », 12 novembre 2009, *LeMonde.fr,* URL : http://www.lemonde.fr/technologies/article/2009/11/12/comment-proteger-sa-vie-privee-sur-internet_1266460_651865.html consulté le 15 janvier 2018.

[1792] CNIL, *Les conseils de la CNIL pour mieux maîtriser la publication de photos*, 13 octobre 2014, à https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mieux-maitriser-la-publication-de-photos-0, consulté le 7 juillet 2016.

[1793] Les conseils formulés sont : adapter le type de photos au site sur lequel elles seront publiées ; éviter d'utiliser la même photo de profil sur des sites ayant des finalités différentes (Facebook, Viadeo ou LinkedIn, Meetic), la photo pouvant être utilisée via des moteurs de recherche d'images pour faire le lien entre les différents profils ; limiter l'accès aux photos publiées sur les réseaux sociaux ; réfléchir avant de publier une photo, car il n'est pas anodin de publier une photo gênante de ses amis ou de soi-même sur un réseau social ; demander l'autorisation avant de publier une photo de quelqu'un ; demander la suppression des photos dérangeantes à la personne les ayant publiées ou en cas de refus à la CNIL ; utiliser avec modération les outils de « tags » (identification) de personnes et la reconnaissance faciale, car cela expose davantage la personne concernée ; contrôler la manière d'être identifié (« taggué ») sur les photos publiées sur les réseaux sociaux ; faire régulièrement le tri dans les photos publiées, des photos anciennes, anodines dans un certain contexte peuvent devenir gênantes dans un autre contexte ; faire attention à la synchronisation automatique des photos, sur smartphone, tablette ou sur les nouveaux appareils photos numériques connectés ; ne pas partager de photos intimes sur un smartphone.

[1794] Accessible à http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/Lettre_IP_N4.pdf, consultée le 4 juillet 2016.

[1795] Si les jeunes de 13 à 17 ans sont les plus actifs à partager des données sur les réseaux sociaux, ils utilisent les paramètres de visibilité pour limiter l'accès des parents et donner une image sage d'eux-mêmes, les 18 à 24 ans reconnaissent que l'envie de partager comporte des risques, et environ 60 % reconnaissent avoir été gênés par des

le partage des photos, l'attitude des individus reste majoritairement une attitude irresponsable même si les risques potentiels sont parfois connus. La volonté de partage l'emporte sur la sécurité et la protection de la vie privée même si pour certaines activités, une recherche d'anonymisation est effectuée. La Gendarmerie Nationale conseille aux parents de ne pas diffuser de photos de jeunes enfants sur Internet[1796].

Conscient de l'importance de protéger les mineurs contre la diffusion volontaire ou non de certaines informations, un certain droit à l'oubli ou à l'effacement d'informations existe aujourd'hui. La loi pour une République numérique a prévu cette possibilité[1797]. Le Règlement général sur la protection des données [1798] a introduit un droit plus large pour l'effacement ou la rectification des données, droit lié au consentement.

Ces données personnelles permettent tant aux gouvernements qu'aux sociétés mercantiles de ficher les individus et d'établir leur profil soit en termes de risques pour la société, soit en termes de cibles marchandes ou publicitaires.

§ 2 - Le fichage et le profilage des individus

À chaque attentat terroriste, en réaction, les États attaqués ont modifié leur législation. La législation contre le terrorisme a toujours été votée en réaction à des attentats, par des gouvernements qui ont réagi à chaud aux événements. Cette législation peut être considérée comme une législation de crise. Devant la difficulté d'anticiper les actes de terrorisme, les gouvernements édictent des lois de surveillance qui limitent les libertés fondamentales et même la sûreté des individus puisque les individus suspectés de préparer ou d'aider à la préparation d'un acte de terrorisme peuvent être arrêtés et privés de liberté avant d'avoir perpétré leur

photos publiées par des tiers, et environ un tiers de cette tranche d'âge affirme qu'une photo a déjà eu des effets négatifs. Les adultes de plus de 51 ans n'utilisent le partage de photos que comme un album classique et la majorité reconnaît ne pas connaître le paramétrage d'accès à ces albums, paramétrage qui permet d'éviter une diffusion générale.

[1796] Relaté par Big Browser, « À quel point publier des photos de ses enfants sur Facebook est-il dangereux ? », *Le Monde,* 18 avril 2017, en ligne à http://www.lemonde.fr/big-browser/article/2017/04/18/a-quel-point-publier-des-photos-de-ses-enfants-sur-facebook-est-il-dangereux_5113202_4832693.html, consulté le 6 décembre 2017.

[1797] Article 63 de la Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique.*

[1798] Section 3, Articles 16 à 20 du Règlement (UE) 2016/679 du Parlement 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).*

acte[1799]. Ces lois peuvent rappeler le film « *minority report* »[1800] et sa prévention du crime. Dans ce film, grâce aux visions du futur fournies par trois individus exceptionnels doués de précognition, les agents de Précrime peuvent arrêter les criminels avant qu'ils n'aient commis leur méfait.

Disposer des forces de police ou de l'armée pour prévenir des attentats sur certains sites n'est pas une mesure suffisante pour lutter contre le terrorisme. Il est nécessaire de donner aux services de sécurité des moyens d'investigation pour rechercher les individus qui pourraient préparer un attentat et les empêcher de passer à l'acte. Mais, comme l'écrivaient les sénateurs dans la saisine du 23 décembre 2005 contre la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles des frontières[1801] : « *L'indispensable volonté de prévenir et punir les actes de terrorismes ne saurait, en revanche, légitimer le glissement insidieux vers un état d'urgence permanent* ». Dans un État de droit, le droit à la sécurité doit toujours être concilié avec le droit à la sûreté, c'est-à-dire le droit de n'être ni surveillé, ni poursuivi, ni arrêté, ni détenu, ni condamné arbitrairement[1802]. Les sénateurs précisent que « *la plus grande victoire des terroristes serait que nous renoncions à l'État de droit* ».

La tentation sécuritaire, tout comme le marketing, nécessite pour être efficace de mettre en fiche les individus remarquables.

A) Les traitements administratifs

En France, tout individu ayant provoqué l'attention des services de sécurité fait l'objet d'une fiche « S ». Cette fiche S fait partie du fichier des personnes recherchées, elle signale une personne pour « atteinte à la sûreté de l'État ». Ce fichier est décrit par la Commission nationale de l'informatique et des libertés en ces termes : « *En recensant toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique, le FPR sert à*

[1799] Conseil constitutionnel, Décision nº 2015-527 QPC du 22 décembre 2015 *M. Cédric D. [Assignations à résidence dans le cadre de l'état d'urgence]*.
Conseil d'État, Ordonnance du 23 décembre 2015*, M. B...,* Nº 395229.
[1800] Stéphane Spielberg, *Minority report*, sorti en 2002, d'après la nouvelle de Philip K. Dick.
[1801] Saisine par 60 sénateurs de la *loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* (Conseil constitutionnel, Décision n° 2005-532 DC du 19 janvier 2006).
[1802] Alex Türk, Pierre Piazza, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Cultures & Conflits,* 76 hiver 2009, pp. 115-134, URL : http://journals.openedition.org/conflits/17806 consulté le 15 janvier 2018.

faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives »[1803]. À titre d'exemple, la CNIL précise quelques catégories de fiches présentes dans ce fichier : « E » police générale des étrangers, « IT » interdiction du territoire, « R » opposition à résidence en France, « TE » opposition à l'entrée en France, « AL » aliénés, « M » mineurs fugueurs, « V » évadés, « S » Sûreté de l'État, « PJ » recherches de police judiciaire, « T » débiteurs envers le Trésor…[1804].

L'inscription au Fichier des personnes recherchées intervient pour plusieurs motifs : judiciaires (exécution de mandats, de condamnation, d'un contrôle judiciaire, enquête de police judiciaire, etc.) ; administratifs (application de réglementations spécifiques de police administrative) ; d'ordre public (prévention de menaces contre la sécurité publique ou la sûreté de l'État). De plus, sans donner lieu à inscription, le Fichier des personnes recherchées est également consulté lors de l'instruction des demandes de carte nationale d'identité, de passeport, de titre de séjour ou de visa.

La création de ce fichier a été autorisée par décret en 2010[1805]. Le décret précise : « *Pour chaque personne inscrite dans le traitement, donnent lieu à enregistrement les données à caractère personnel et informations suivantes : 1º l'état civil (nom, prénom [s], date et lieu de naissance, filiation), l'alias, le sexe, la nationalité ; 2º le signalement et la photographie ; 3º les motifs de la recherche ; 4º la conduite à tenir en cas de découverte* »[1806] ; « *Les données contenues dans le fichier peuvent, dans le respect des conditions prévues à l'article 24 de la loi du 18 mars 2003 susvisée, être transférées à des organismes de coopération internationale en matière de police judiciaire ou à des services de police étrangers* »[1807], et « *Les droits d'information et d'opposition prévus aux articles 32 et 38 de la loi du 6 janvier 1978 susvisée ne sont pas applicables au présent traitement* »[1808]. Ainsi, ce fichier est bien un traitement automatique de données à caractère personnel, qui peut être transmis hors du territoire national, voire européen[1809], mais qui ne donne pas un droit d'information ni d'opposition aux personnes

[1803] FPR : Fichier des personnes recherchées, CNIL à https://www.cnil.fr/fr/fpr-fichier-des-personnes-recherchees consulté le 5 juillet 2016.
[1804] Ibid.
[1805] Décret nº 2010-569 du 28 mai 2010 *relatif au fichier des personnes recherchées* publié au JORF nº 0123 du 30 mai 2010 p. 9765.
[1806] Ibid. article 3.
[1807] Ibid. article 6.
[1808] Ibid. article 10.
[1809] Cf. Commission nationale de l'informatique et des libertés, Délibération nº 2009-587 du 12 novembre 2009 *portant avis sur un projet de décret en Conseil d'État relatif au fichier des personnes recherchées (FPR)*

faisant l'objet d'une inscription dans ce fichier[1810]. Dès 1988, la CNIL demandait au gouvernement que : « *en application des dispositions de l'article 31 de la loi du 6 janvier 1978, que le ministère de l'Intérieur et le ministère de la Défense saisissent la commission d'un projet de décret en conseil d'État autorisant la collecte de ces informations ; que devra en outre être mentionnée l'application de l'article 31 dans le projet d'arrêté portant création du traitement* »[1811], mais émettait un avis favorable à la création de ce fichier. Suite à des réorganisations administratives de la police et de la gendarmerie nationale, ou à des extensions des raisons de l'inscription dans le fichier, la commission a été amenée à se prononcer sur plusieurs projets de décrets[1812].

Ainsi, une personne physique dont le comportement aurait été jugé dangereux pour l'ordre public, soit qu'il se soit rendu en territoire djihadiste, soit qu'il ait consulté des sites Internet djihadistes, soit qu'il ait fréquenté régulièrement des mosquées réputées djihadistes ou salafistes, sera considéré comme potentiellement dangereux et pourra faire l'objet d'une inscription en fiche « S », sans en avoir connaissance ni sans pouvoir bénéficier d'un recours contradictoire[1813]. Ce fichier n'est que l'un des traitements administratifs existants[1814] avec les fichiers de police et le fichier des antécédents judiciaires[1815].

Hormis les fichiers d'état civil, tout citoyen français majeur est fiché dans un ou plusieurs traitements administratifs : fichier du permis de conduire, fichier des cartes grises, fichiers fiscaux, fichier des données biométriques, etc. Tous ces fichiers ne sont pas interconnectés,

---

[1810] Décret nº 2010-569 du 28 mai 2010 *relatif au fichier des personnes recherchées*, Article 10 : « *Les droits d'information et d'opposition prévus aux articles 32 et 38 de la loi du 6 janvier 1978 susvisée ne sont pas applicables au présent traitement* ».

[1811] Commission nationale de l'informatique et des libertés, Délibération n º 88-120 du 08 novembre 1988 *Délibération portant avis sur la mise en œuvre conjointe par le Ministère de l'Intérieur et le Ministère de la Défense du traitement automatisé d'informations nominatives relatif au fichier des personnes recherchées (F.P.R.).*

[1812] Commission nationale de l'informatique et des libertés, Délibération nº 92-056 du 09 juin 1992, *Délibération portant avis sur le projet d'arrêté relatif au fichier des personnes recherchées géré par le Ministère de l'Intérieur et le Ministère de la Défense ;* Délibération nº 95-051 du 25 avril 1995, *Délibération portant avis conforme sur le projet de décret portant application au fichier des personnes recherchées des dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;* Délibération n º 2006-292 du 21 décembre 2006 *portant avis sur le projet d'arrêté portant modification de l'arrêté du 15 mai 1996 modifié relatif au fichier des personnes recherchées (FPR) ;* Délibération nº 2009-587 du 12 novembre 2009 *portant avis sur un projet de décret en Conseil d'Etat relatif au fichier des personnes recherchées (FPR).*

[1813] Décret nº 2010-569 du 28 mai 2010 *relatif au fichier des personnes recherchées,* Articles 2-I et II, 9 et 10. L'article 9 prévoit un droit d'accès indirect et de rectification auprès de la Commission nationale de l'informatique et des libertés.

[1814] Jean-Claude Vitran, « Vous êtes étiquetés ? », *Revue Projet*, 2010/6 (n° 319), pp. 55-61. URL : https://www.cairn.info/revue-projet-2010-6-page-55.htm consulté le 15 janvier 2018.

[1815] Cf. Partie 1. Titre 2. Chapitre 1. Section 1. Sous-section 2. § 2 -La dérive sécuritaire de la loi en matière de données personnelles

mais à l'exemple des fichiers fiscaux, ils pourraient l'être dans le cas d'un gouvernement autoritaire d'autant plus, que dans son rapport 2014, le Conseil d'État préconise l'étude de la mise en place d'un identifiant national, non signifiant[1816].

En 2012, lors de la création de la carte d'identité biométrique, le Parlement avait souhaité la création d'un registre national recensant l'ensemble des informations biométriques qui revenait à mettre en fiche la quasi-totalité de la population française. Le ministre de l'Intérieur souhaitait permettre que cette base de données puisse être exploitée à des fins de police judiciaire et non réservée à la seule détection d'une usurpation d'identité. Le Conseil constitutionnel[1817] a déclaré non conforme à la Constitution le traitement automatique souhaité pour atteinte au droit au respect de la vie privée disproportionnée au vu de l'intérêt général recherché : la lutte contre la fraude. La Commission de l'informatique et des libertés avait émis un avis défavorable[1818] concernant la création de ce traitement, les données biométriques étant des données à caractère personnel particulièrement sensibles. Mais le 28 octobre 2016, le gouvernement a autorisé par décret la création d'un fichier « titres électroniques sécurisés » (TES)[1819] pour recenser et stocker les informations relatives aux demandeurs de cartes nationales d'identité et de passeport, permettant ainsi progressivement le fichage de tous les citoyens français, malgré un nouvel avis défavorable de la CNIL[1820]. La Commission demandait au Gouvernement de saisir le Parlement du projet et considérait qu'un tel fichier est d'une ampleur et d'une nature inégalées, puisqu'il constitue le premier fichier quasi exhaustif des citoyens français contenant des données biométriques, et présente un risque de détournement de finalité[1821]. Cette base de données peut devenir une cible privilégiée pour les cybercriminels au détriment des citoyens, d'autant plus que la sécurité de ce traitement peut poser problème.

[1816] Conseil d'État, *Le numérique et les droits fondamentaux*, Proposition nº 21.
[1817] Conseil constitutionnel, Décision nº 2012-652 DC du 22 mars 2012 *Loi relative à la protection de l'identité*.
[1818] Commission nationale de l'informatique et des libertés, *Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité,* Examinée en séance plénière le 25 octobre 2011.
[1819] Décret nº 2016-1 460 du 28 octobre 2016 *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*, publié au JORF nº0254 du 30 octobre 2016.
[1820] Commission nationale de l'informatique et des libertés, Délibération n° 2016-292 du 29 septembre 2016 *portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité* (saisine n° 1979541)
[1821] Thèmes retrouvés dans le rapport conjoint de l'Agence nationale de la sécurité des systèmes d'information et de la Direction interministérielle du numérique et du système d'information et de communication de l'État, *Audit de système « Titres Électroniques Sécurisés »,* du 13 janvier 2017.

B) Les traitements commerciaux

Mais, les traitements automatiques des données personnelles ne sont pas l'apanage de l'administration, ils peuvent être réalisés par des entreprises mercantiles pour des raisons économiques. Comme l'indique le Conseil d'État dans son étude 2014, « *la publicité joue […] un rôle particulier : plus le nombre d'informations détenues sur le "profil" d'une personne est grand, plus les publicités qui lui seront adressées seront pertinentes* »[1822]. De ce fait, les données collectées ont une valeur marchande d'autant plus élevée que ces données sont fiables et corrélées à des profils précis d'acheteurs potentiels. Certaines sociétés collectent elles-mêmes des données à caractère personnel, soit de par leur activité, moteurs de recherche, sites marchands, banques en ligne, etc., certaines de par leur relation avec l'utilisateur, réseaux sociaux. Ces sociétés cherchent par divers moyens à accroître leur capacité de collectes de données : prise de contrôle par Google de *Linkedlin* pour accéder aux cursus professionnels ; rachat par Facebook du site de partage des photos *Instagram* ou de la messagerie *Whatsapp* pour obtenir plus d'informations. Google a reconnu, en déclarant ne plus utiliser cette source d'information, qu'il scannait les messages transitant dans la messagerie GMAIL pour cibler la publicité vers les internautes[1823].

D'autres sociétés spécialisées dans l'achat et la revente de ces données[1824], les *data brokers*, interviennent sur ce marché en toute illégalité puisqu'elles traitent des données collectées par d'autres entités pour un usage différent, et ce à l'insu complet des personnes physiques concernées. Ces marchands vendent ces données sur le marché mondial sans tenir compte des législations nationales ou européennes qui limitent ces transferts. L'État français, lui-même, s'est autorisé par un décret[1825] à commercialiser les données collectées pour l'établissement des

[1822] Conseil d'État, *Le numérique et les droits fondamentaux*, p. 17.

[1823] « Gmail : Google renonce à scanner les courriels pour cibler les pubs », *ZDNet*, 26 juin 2017, en ligne à http://www.zdnet.fr/actualites/gmail-google-renonce-a-scanner-les-courriels-pour-cibler-les-pubs-39854144.htm, consulté le 7 aout 2017.

[1824] Slim Turki, Muriel Foulonneau, « Valorisation des données ouvertes : acteurs, enjeux et modèles d'affaires », dans *Big Data - Open Data : Quelles valeurs ? Quels enjeux ? Actes du colloque « Document numérique et société », Rabat, 2015.* Louvain-la-Neuve, De Boeck Supérieur, « Information et stratégie », 2015, pp. 113-125. URL : https://www.cairn.info/big-data-open-data-quelles-valeurs--9782807300316-page-113.htm consulté le 15 janvier 2018.

[1825] Arrêté du 1er septembre 2009 *portant création d'un traitement automatisé de données à caractère personnel dénommé « Système d'information décisionnel du système d'immatriculation des véhicules »* publié au JORF du 22 septembre 2009.

cartes grises, devenues certificats d'immatriculation[1826], « *à des fins d'enquêtes et de prospection commerciale dès lors que le droit d'opposition des personnes concernées est respecté* »[1827]. L'État français a choisi le refus explicite, *opt-out*, en cochant une case sur le formulaire de demande de certificat d'immatriculation d'un véhicule[1828]. Par ailleurs, ce fichier est accessible aux professionnels de l'automobile au travers d'une licence d'utilisation.

La prolifération des données à caractère personnel et l'utilisation d'algorithmes puissants et confidentiels tendent à la segmentation des populations : population pauvre, proie facile des établissements de crédit personnels ; envies des acheteurs potentiels permettant de proposer des prix ciblés que l'utilisateur ne pourra pas évaluer, car ne connaissant pas le prix proposé à d'autres acheteurs éventuels, etc. Le résultat de ces algorithmes est de rompre l'égalité entre le vendeur et l'acheteur, le premier ayant une connaissance du profil du second lui donnant un avantage dans la négociation. Ainsi que le relate l'étude du Conseil d'État[1829], Google a déposé un brevet pour son projet de « *dynamic pricing* » dont la description démontre l'objectif de permettre une différenciation des prix en fonction des envies et propensions supposées ou estimées de l'acheteur potentiel. Ce qui pose la question des algorithmes et de leur neutralité. Comme le constate le Conseil d'État[1830], la législation actuelle ne permet pas de contrôler les algorithmes prédictifs ni leur potentielle discrimination. Une information sur ces algorithmes et leur paramétrage semble à minima nécessaire.

Le règlement général sur la protection des données[1831] décrit le profilage comme étant : « *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* »[1832]. Le

[1826] Simon Caqué, « La réutilisation des données issues du système d'immatriculation des véhicules (SIV) », Irène Bouhadana, William Gilles (dir.), *Revue internationale des Gouvernements Ouverts,* Vol. 5, 2017, IMODEV, pp. 105-116.
[1827] Arrêté du 1er septembre 2009, Op. cit. article 4.
[1828] Voir formulaire Cerfa n° 13750*05. Le Règlement général sur la protection des données demande à ce que ce soit une acceptation expresse que doivent demander les responsables de traitement, privilégiant ainsi l'opt-in et le consentement explicite (mis en application dans l'Union européenne le 25 mai 2018). Une modification du formulaire sera nécessaire pou se conformer au règlement.
[1829] Conseil d'État, *Le numérique et les droits fondamentaux*, p. 161.
[1830] Ibid. pp. 22-23, 233 et suivantes.
[1831] 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).*
[1832] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, Article 4-4).

responsable d'un traitement doit fournir à la personne concernée toute information concernant « *l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, 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* », la personne concernée ayant alors la possibilité de s'y opposer[1833]. De plus, la personne concernée 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[1834]. Ainsi, si le profilage permet de penser qu'une personne prépare un acte de terrorisme, par exemple, d'autres constatations seront nécessaires pour produire des effets juridiques comme la privation de liberté.

Un exemple d'utilisation d'un algorithme de décision est le traitement Admission post-bac ou APB, utilisé par le ministère de l'Éducation nationale. Les futurs bacheliers doivent s'y inscrire en fournissant plusieurs choix possibles pour leur futur cursus universitaire. Le traitement propose, après l'obtention du baccalauréat, une inscription dans une université pouvant accepter l'étudiant en respectant ses choix. Lors de la rentrée universitaire 2017-2018, plusieurs centaines d'étudiants se sont retrouvés sans affectation ni proposition d'inscription et de nombreux autres ont reçu des propositions ne correspondant pas à leurs premiers choix malgré des mentions TB au baccalauréat. Suite à la réception d'une plainte, la Commission nationale de l'informatique et des libertés a rappelé qu'une décision concernant une personne physique ne pouvait pas dépendre d'un seul algorithme sans intervention humaine et donc que le choix d'une inscription en université ne pouvait être délégué à un algorithme[1835]. Le système APB a

[1833] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, Article 21, Droit d'opposition.

[1834] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, art.10 2nd paragraphe : « *Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, Article 22, Décision individuelle automatisée, y compris le profilage, 1er paragraphe : « *1. La personne concernée 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* ».

[1835] Commission nationale de l'informatique et des libertés, *Admission Post-Bac (APB) : mise en demeure pour plusieurs manquements,* 28 septembre 2017 ; Décision no MED-2017-053 du 30 août 2017 *mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation ;* Délibération du bureau de la Commission nationale de l'informatique et des libertés no 2017-233 du 7 septembre 2017 *décidant de rendre publique la mise en demeure no 2017-053 du 30 août 2017 prise à l'encontre le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation.*

été abandonné[1836] et remplacé par le système Parcoursup qui intègre une « fiche avenir » contenant l'appréciation des professeurs sur ces vœux. Le Conseil d'État a rejeté les demandes de suspension de cette plateforme[1837].

Bien que n'étant pas l'objet de la loi n° 78-17 ni du règlement général sur la protection des données, mais de la lutte contre le terrorisme, le Conseil constitutionnel[1838] a considéré que la seule visite d'un site djihadiste, même régulière, ne suffisait pas à définir un délit, même si cette décision a été motivée par la seule atteinte à la liberté de communication. La présomption du délit de terrorisme doit être confirmée par plusieurs faits, l'administration ou la police disposant d'autres moyens d'investigation que la surveillance des accès aux sites incriminés.

Compte-tenu de la captation des données à caractère personnel implicite ou explicite sur Internet, un besoin des utilisateurs de rester anonyme existe.

Sous-section 2. Le besoin d'anonymisation dans les sociétés numériques

Liberté ou liberté surveillée ? À l'ère du numérique, cette question revêt toujours un intérêt majeur, consubstantiel à la société de l'information[1839]. Internet a été créé dès l'origine comme un espace de liberté qui a rapidement fait l'objet de restrictions à la faveur de la prise de conscience des enjeux potentiels réels qu'ils présentaient, notamment au regard de la sécurité. L'arbitrage entre liberté et sécurité auquel l'Internet nous confronte aujourd'hui redonne un éclairage particulier aux propos de Benjamin Franklin, selon lequel : « Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre »[1840].

Face à la traçabilité des activités numériques et à la surveillance liée à la lutte contre la criminalité et le terrorisme, voire au mercantilisme des principaux acteurs de l'Internet, nombre d'individus cherchent à conserver l'anonymat lors des accès à Internet. Cet anonymat a été

[1836] Clôturant ainsi la mise en demeure de la CNIL (Décision du 22 janvier 2018 *Clôture de la décision n° MED-2017- 053 du 30 août 2017 mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation*)

[1837] Conseil d'État, ordonnance n° 417905 du 20 février 2018, *Groupe communiste, républicain, citoyen et écologiste et autres* et Conseil d'État, ordonnance n° 418029 du 20 février 2018, *Solidaires Etudiant-e-s, Syndicats de luttes et l'Union nationale lycéenne - syndicale et démocratique*.

[1838] Conseil constitutionnel, Décision nº 2016-611 QPC du 10 février 2017, *M. David P. [Délit de consultation habituelle de sites Internet terroristes]*.

[1839] Emmanuel Valjavec, « Internet, un nouvel espace de liberté sous surveillance », *Études*, 2013/3 (Tome 418), pp. 317-327. URL : https://www.cairn.info/revue-etudes-2013-3-page-317.htm consulté le 15 janvier 2018.

[1840] "*They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety*". Benjamin Franklin, Contributions to the Conference on February 17, 1775.

facilité par les démocraties occidentales dans un premier temps pour permettre à certains dissidents de pays sous régime totalitaire de pouvoir communiquer et s'exprimer. Depuis les attentats du 11 septembre 2001 à New York, il semblerait que nos démocraties modernes aient décidé de limiter les libertés individuelles et de lutter contre l'anonymat afin de pouvoir combattre le terrorisme et la cybercriminalité.

La société numérique favorise la communication rapide entre les individus ainsi que l'échange d'informations. Cette communication laissant des traces, la recherche de communication sans trace ou avec impossibilité de lire les informations échangées s'est développée. Paradoxalement, la liberté et la vie privée se nourrissent d'anonymat, voire d'obscurité, qui eux-mêmes peuvent parfois être source d'insécurité. Ainsi, l'internaute anonyme bénéficie d'une plus grande liberté qui lui permet d'agir plus librement en bien ou en mal. Par exemple, le cybercriminel peut « *voler sans rien prendre, entrer sans frapper, [voir] sans être vu* »[1841]. Pour l'utilisateur à la recherche d'anonymat, il existe deux solutions : l'utilisation de messagerie cryptée garantissant la non-conservation des messages comme *Telegram Messenger*[1842] ou l'utilisation de logiciel d'accès aux réseaux parallèles du Darknet comme TOR ou FreeNet.

§ 1 - L'anonymisation relative des données collectées

Des textes existent pour assurer la protection des données à caractère personnel[1843] et sont relayés par la CNIL en France. Mais, cette protection souffre de la prolifération de ces données sur Internet, prolifération volontaire ou non, de l'attitude des individus eux-mêmes, ainsi que de la mondialisation des acteurs de l'Internet. Elle souffre également, des moyens techniques invasifs mis à disposition des enquêteurs, officiellement ou non.

[1841] Cf. Pierre Joxe, « La cybercriminalité, résurgence du furtum noctu à l'ère du numérique », in Irène Bouhadana, William Gilles (sous la direction de), *Cybercriminalité, cybermenaces et cyberfraudes*, Les éditions Imodev, 2012.
[1842] *Telegram Messenger* est une application de messagerie sécurisée hébergée sur le cloud. L'application gratuite est disponible sur Android, iOS, Windows Phone ainsi que sur ordinateur (Windows, OS X et Linux). Les utilisateurs peuvent échanger des messages, photos, vidéos et documents d'une taille allant jusqu'à 1,5 Go. Il est aussi possible d'envoyer des messages chiffrés de bout en bout qui ne sont pas stockés sur les serveurs de *Telegram*.
[1843] Cf. Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 1. § 1 - La protection de la vie privée en France.

A) La chute du mur de l'intimité sur Internet

Sur Internet, toute action laisse des traces qui permettent de surveiller les individus et leur activité sur le réseau. Une recherche d'information sur un produit ou un type de produit va provoquer l'apparition, dans les encarts publicitaires des écrans consultés, de promotions pour ces mêmes produits. La bulle ou le mur de l'intimité n'existe pas sur Internet. Au travers des accès à Internet, des messages échangés, une personne peut être surveillée ou retrouvée au cours d'une enquête policière. En 2012, l'affaire Petraeus[1844] en est un exemple significatif et montre la porosité du mur de l'intimité aux investigations policières sur Internet[1845]. Le général David Petraeus, Directeur de la CIA, a été contraint à la démission suite à la mise au jour d'une relation extra-conjugale, dévoilée par connectivité d'une enquête du FBI concernant une agression par mails. L'affaire est inquiétante pour la protection des libertés individuelles, Internet et la vie privée semblant devenus incompatibles. L'affaire Petraeus est d'autant plus préoccupante qu'elle implique une personnalité, censée être protégée, qui n'arrive pas à protéger sa propre vie privée de faits collatéraux.

En France, en mars 2012, avec une technique de recoupement d'adresse IP ayant consulté une annonce sur Internet, Mohammed Merah[1846] fut présumé être le tueur de Toulouse et de Montauban[1847].

[1844] David Petraeus, général, directeur de la CIA.

[1845] La maîtresse du général a envoyé des e-mails menaçants à une autre femme qu'elle considérait comme une rivale, provoquant ainsi une enquête du FBI, suite à un dépôt de plainte. La maîtresse du général, Paula Broadwell, spécialisée dans la stratégie et l'antiterrorisme, écrit une biographie du général David Petraeus alors qu'il est commandant en chef des armées américaines en Afghanistan. Ils deviennent amants courant 2011. Durant le mois de mai 2012, Jill Kelley, une autre amie de David Petraeus, porte plainte pour harcèlement au moyen de mails menaçants qui l'accusent d'avoir une relation avec le général Petraeus. Une enquête du FBI est ouverte, elle remonte à l'origine de ces mails. Paula Broadwell est interrogée, reconnaît les faits et révèle à cette occasion la liaison qu'elle a entretenue avec le général Petraeus.
L'enquête du FBI a permis de remonter à Paula Broadwell en utilisant le fait que Google, Yahoo et consorts enregistrent les adresses IP à partir desquelles les mails sont envoyés, et en croisant les informations sur les différents comptes utilisés depuis une même adresse. Les enquêteurs ont ensuite vérifié que les lieux liés à ces adresses correspondaient bien à l'emploi du temps de Mme Broadwell, utilisant pour ce faire les données de géolocalisation fournies par son opérateur de téléphonie, les services Wi-Fi dans les hôtels qu'elle avait utilisés, etc. À chaque nouvel hôtel où elle séjournait, le nombre de suspects partageant la même adresse IP diminuait : il suffit de trois ou quatre hôtels pour qu'un seul nom apparaisse.

[1846] Mohammed Merah est un terroriste islamiste franco-algérien ayant en mars 2012, à Toulouse et Montauban, assassiné sept personnes et fait six blessés, lors de trois expéditions.

[1847] Le Monde.fr, « Tuerie de Toulouse : retour sur les événements », 23 mars 2012, *Le Monde.fr,* URL : http://www.lemonde.fr/societe/article/2012/03/23/tuerie-de-toulouse-retour-sur-les-evenements_1674320_3224.html consulté le 15 janvier 2018.

En surveillant des échanges sur le réseau TOR, le FBI a aussi pu appréhender Ross Ulbricht et fermer le site « *the silk road* »[1848]. Les enquêteurs ont passé de longs mois à retrouver les premières occurrences du site en ligne, traquer des pseudonymes, déterrer des *posts* de blog, passer des forums au scanner, de fait chercher l'erreur humaine, la faille involontaire[1849], car dans ce cas, l'utilisation de TOR rend invisible l'adresse IP de l'intervenant.

Avec les traces techniques, les métadonnées stockées par les opérateurs, tout écrit, explicite ou implicite, toute chose qui transite sur Internet, peut être traité et récupéré par les agences gouvernementales[1850]. Même s'il existe des techniques cryptographiques à l'épreuve des curieux, la moindre erreur, le moindre faux pas peuvent permettre de dérouler le fil et de remonter les pistes[1851]. La seule véritable limite reste la motivation des enquêteurs et les moyens techniques mis à leur disposition. Les techniques d'anonymisation ou de pseudonymisation[1852] restent insuffisantes face à la masse d'information pouvant être utilisée pour percer l'identité réelle des individus.

B) La fausse protection de l'anonymisation

Les textes de protection des données à caractère personnel insistent sur la non-conservation des données au-delà du délai nécessaire au traitement[1853] pour lequel elles ont été collectées ou sur l'anonymisation ou pseudonymisation des données pour traitements statistiques. Le nouveau règlement européen[1854] a préféré utiliser le terme « pseudonymisation », et en donne la définition suivante : « *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 et soumises à des mesures techniques et organisationnelles afin de*

[1848] "Operator of Silk Road 2.0 WEBsite Charged in Manhattan Federal Court", 6 novembre 2014, en ligne à https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court, consulté le 2 aout 2017.
[1849] Donna Leinwand Leger, "How FBI brought down cyber-underworld site Silk Road", October 21, 2013 *USA TODAY*. URL : https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/ consulté le 15 janvier 2018.
[1850] Comme le révèle le scandale des écoutes de la NSA révélées par Edward Snowden.
[1851] Comme le démontre la révélation par le FBI de la méthode ayant été utilisée pour remonter aux propriétaires du site « *the Silk road* » pourtant hébergé sur le réseau TOR, grâce à une erreur de configuration du site.
[1852] Terme utilisé par le Règlement général sur la protection des données.
[1853] Loi n° 78-17 du 6 janvier 1978, Art. 6 ; Directive 95/46/CE Art. 6.1.e) ; Règlement (UE) 2016/679 Art. 5.1.e).
[1854] 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).*

garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ». Cette approche tient compte des travaux d'Arvid Naranayan[1855] et de Vitaly Shmatikov[1856] sur la base de Netflix, travaux qui ont démontré que face aux moyens et techniques modernes, l'anonymisation des données est quasiment impossible à garantir[1857].

Le 2 octobre 2006, Netflix a lancé un concours public dont le but était de prévoir par un algorithme de traitement des données, quels films ses utilisateurs allaient aimer afin d'améliorer son service de recommandations à ses abonnés. Pour ce concours, Netflix a publié un extrait de sa base de données contenant environ 100 millions de notes formulées par 500 000 de ses clients sur son catalogue de films, entre 1999 et 2005. La base était anonymisée par suppression de toute information personnelle concernant les clients de cet échantillon.

Arvid Naranayan et Vitaly Shmatikov sont arrivés à retrouver, avec 99 % d'exactitude, l'identité des utilisateurs ayant formulé plus de 8 notes, et avec 66 % d'exactitude dans le cas où seulement deux notes étaient disponibles[1858]. Les deux chercheurs texans sont arrivés à désanonymiser la base de données à partir de la date d'attribution des notes, date présente dans la base fournie par Netflix, en rapprochant ces notes avec celles d'un autre site, Movie Database[1859], site sur lequel les internautes peuvent laisser des commentaires et des notes concernant les films qu'ils ont vus. Par corrélation entre la date à laquelle étaient notés les films sur la base de données de Netflix et celle à laquelle le même film était noté de manière similaire sur Movie Database, ils sont arrivés à retrouver les noms des clients de Netflix.

Ils ont également montré dans leur communication que sans utilisation des dates de notation, il est encore possible de désanonymiser une partie importante de la base publiée, en utilisant les films vus par peu de personnes (dans leur expérience, un film qui n'était pas dans le top 500 des films les plus vus). Ils ont réussi à retrouver l'identité de plus de 80 % des utilisateurs ayant noté 8 films dont au moins 6 ne font pas partie du top 500.

La perte de confidentialité est un phénomène de type contagieux. La non-confidentialité d'un site peut permettre de contourner la confidentialité d'un autre site mieux protégé. Les réseaux

[1855] Arvid Naranayan, assistant professor of computer science at Princeton.
[1856] Vitaly Shmatikov, Professor of Computer Science at Cornell Tech. Prior to joining Cornell Tech, he worked at the University of Texas at Austin.
[1857] Exemple repris par le *rapport d'information sur l'open data et la protection de la vie privée* de MM. Gaëtan Gorce et François Pillet, sénateurs, nº 469, Sénat, session ordinaire de 2013-2014, p. 48.
[1858] Arvind Narayanan and Vitaly Shmatikov, "*Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*", The University of Texas at Austin, February 5, 2008, disponible à http://arxiv.org/pdf/cs/0610105v2.pdf .
[1859] http://www.imdb.com/.

sociaux s'entraident mutuellement à lever l'anonymat, le premier sert de base, et avec le second, des informations qui ne sont pas dans le premier sont retrouvées, elles permettent à leur tour en réutilisant le premier réseau, de déduire des informations qui ne sont pas dans le second, et ainsi de suite par propagation[1860]. Cette méthode est utilisée par certains sites pour, à partir de photos taguées et par utilisation de reconnaissance faciale, pour propager les noms des individus présents sur une photo. Une personne physique présente sur plusieurs réseaux sociaux et exposant sur chacun de ces réseaux une partie des informations le concernant, donne en fait une vision plus globale de sa vie privée par regroupement des informations de chaque site[1861]. Le regroupement peut être basé sur le nom, le prénom, la date de naissance (données demandées par tous les réseaux sociaux), mais aussi simplement sur une photographie représentant la personne.

Dans l'exemple de Netflix, les données à caractère personnel considérées intuitivement comme étant des données personnelles d'identification, typiquement le nom, l'âge, le sexe, le numéro de sécurité sociale, etc., ne sont pas la seule source d'identification. En fait, toute donnée particulière suffit pour identifier un individu. Les ordinateurs excellent dans le travail de rapprochement exhaustif lié à l'agrégation des informations : plus il existe d'informations sur un individu, plus il devient facile de l'identifier. Comme l'écrivent Alexandra Bensamoun et Célia Zolinsky[1862], « *ce n'est parfois que le recoupement réalisé grâce au traitement secondaire de données brutes, "neutres", qui pourra les transformer en données personnelles. Cette corrélation des données n'est pas sans conséquence* ».

D'autres techniques, encore plus perfectionnées, permettent d'obtenir des corrélations en observant des masses gigantesques de données. L'équipe Human Dynamics au *MIT Media Lab*[1863] développe des méthodes de prédiction à partir des informations qui peuvent être récupérées par un téléphone portable, sur le comportement économique des personnes en observant les schémas émergents relatifs aux utilisations de cartes bancaires. À partir de données de masse, des corrélations statistiques sont déduites. Aujourd'hui, les algorithmes mis

[1860] Dieudonné Tchuente, Nadine Baptiste-Jessel, Marie-Françoise Canut, « Accès à l'information dans les réseaux socionumériques », *Hermès, La Revue*, 2011/1 (n° 59), pp. 59-64. URL : https://www.cairn.info/revue-hermes-la-revue-2011-1-page-59.htm consulté le 15 janvier 2018.

[1861] Pages Jaunes a été condamné par la CNIL pour avoir enrichi les informations des abonnés au téléphone par consultation des réseaux sociaux pour lesquels ils étaient référencés (CNIL, Délibération de la formation restreinte n° 2011-203 du 21 septembre 2011 portant avertissement à l'encontre de la société Pages Jaunes).

[1862] Alexandra Bensamoun, Célia Zolynski, « *Cloud computing* et *big data*. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux*, 2015/1 (n° 189), pp. 103-121. URL : https://www.cairn.info/revue-reseaux-2015-1-page-103.htm consulté le 15 janvier 2018.

[1863] Site accessible à l'URL http://hd.media.mit.edu/? Consulté le 2 aout 2017.

en jeu par l'intelligence artificielle ont dépassé le stade du domaine des systèmes experts[1864]. À partir de questions ciblées, le système expert déduit par reproduction du raisonnement d'une expertise humaine, des décisions : niveau de sécurité d'un site et actions nécessaires au renforcement de cette sécurité ; profil psychologique d'un individu voire diagnostic ou prédiagnostic médical permettant d'orienter un patient vers le médecin spécialiste concerné. Les algorithmes de l'intelligence artificielle utilisent les données collectées brutes pour déterminer des prédicats nouveaux non prédéfinis et enrichir leur base euristique[1865].

La connaissance technique et théorique avance beaucoup plus vite que les garde-fous légaux difficilement confectionnés (les modifications successives des politiques de confidentialité de Facebook, Google ou Twitter en sont une bonne illustration). L'interconnexion des réseaux est à la perte de confidentialité de la vie privée ce que les transports modernes sont aux épidémies : des propagateurs, des accélérateurs ou des catalyseurs.

L'anonymat peut être aussi levé par des vols de données et de fichiers client de certains fournisseurs de service. En France, ORANGE a dû avertir certains de ses abonnés de tels vols, leur demandant de modifier leur identification de connexion par sécurité[1866]. D'autres fournisseurs ont été objet de cyberattaques ayant pour résultat de mettre sur le réseau des données à caractère personnel qui auraient dû rester confidentielles : photos privées ou anciennes, numéro de téléphone, etc.[1867].

Le Règlement général sur la protection des données demande aux responsables de traitement de réaliser des études d'impact relatives à ces pertes de données, conséquences pour les personnes physiques, mais aussi pour l'amélioration de la prévention en cas de détection de risques importants détectés. Un moyen de protéger les données reste le cryptage de ces données sur le serveur. En cas de vol des données dans possession des clés de cryptage, ces données sont inexploitables. Android et Apple cryptent les données enregistrées sur les smartphones.

[1864] Système expert : Programme informatique conçu pour raisonner. Le système est dit « intelligent », car en réalité le programme est développé pour reproduire le raisonnement logique que pourrait faire un expert humain à propos d'une tâche particulière ou sur un sujet spécifique. Pour cela, le programme s'appuie sur des bases de données de faits et de connaissances très développées. Si le résultat est atteint, le système expert doit alors pouvoir tirer ses propres conclusions de son analyse et même être en mesure de traiter des connaissances incertaines. Il est généralement utilisé comme système d'aide à la décision. (Définition extraite de http://www.e-marketing.fr/Definitions-Glossaire/Systeme-Expert-243288.htm#VqlFpgRD2lY5Rw7e.97).

[1865] « CES 2017 : Intelligence artificielle & analyse prédictive », décembre 2016, *MtoM Mag.com,* URL : http://www.mtom-mag.com/article3152.html consulté le 15 janvier 2018.

[1866] En mai 2014, l'auteur a reçu une lettre en provenance d'ORANGE l'informant du vol de ses données et lui conseillant de modifier ses mots de passe.

[1867] Le Monde, « Les principaux vols de données personnelles depuis 2013 », 23 septembre 2016, *Le Monde Pixels,* URL : http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html consulté le 15 janvier 2018.

§ 2 - Le cryptage des données et des échanges

Une protection possible des échanges consiste à crypter les données transitant sur le réseau ainsi que les données stockées[1868]. Lors de l'usage quotidien du réseau Internet, l'internaute utilise consciemment ou non deux types de chiffrement qui garantissent que ses correspondances demeurent intègres, confidentielles et authentiques ; le chiffrement de bout en bout et le *Transport Layer Security,* anciennement connu comme *Secure Sockets Layer (SSL/TLS).* Dans le premier cas, le chiffrement de bout en bout garantit que seuls l'expéditeur et le destinataire peuvent lire et déchiffrer le message échangé. Si le message est intercepté par un fournisseur d'accès Internet ou l'administration de l'État, ils ne pourront pas connaître le contenu du message, sans l'obtention des clés nécessaires pour décrypter le texte. Apple utilise un chiffrement de bout en bout dans ses applications *iMessage* et *Facetime*[1869], il en est de même pour *Facebook Messenger*, l'application de messagerie de Facebook, et par *Whatsapp*[1870], application utilisée par plus d'un milliard d'individus dans plus de 180 pays,[1871] et rachetée par Facebook en 2014.

Dans la seconde méthode, le chiffrement est appliqué au protocole Internet HTTP qui prend alors la forme sécurisée de HTTPS, ce protocole garantit que toutes les communications établies depuis un navigateur Internet vers une page d'un serveur WEB sont chiffrées (techniquement, le serveur peut imposer le protocole HTTPS ou le refuser)[1872]. Ce protocole est utilisé pour assurer, entre autres, la sécurité des paiements en ligne et en a permis l'utilisation intensive. *SSL/TLS* permet à un navigateur de vérifier l'identité du site WEB auquel il accède grâce à un certificat d'authentification émis par une autorité tierce dite de confiance.

L'utilisation d'outils de cryptage pour un usage individuel a été longtemps prohibée en France. Pendant longtemps, le cryptage était considéré comme arme de guerre de deuxième catégorie[1873], d'où le contrôle strict de l'État. Réglementé à l'origine par le décret-loi du 18

[1868] Olivier Eymard, « Questions de cryptologie », *Délibérée*, 2018/1 (N° 3), pp. 60-63. URL : https://www.cairn.info/revue-deliberee-2018-1-page-60.htm consulté le 12 avril 2018.

[1869] Cf. information sur le site http://www.apple.com/privacy/approach-to-privacy/ consulté le 5 avril 2017.

[1870] « Vos messages sont protégés avec un cadenas, et seuls le destinataire et vous avaient la clé spéciale qui permet de les déverrouiller et de les lire. Afin d'assurer une protection supplémentaire, chaque message que vous envoyez a son propre cadenas unique et sa clé unique. » Whatsapp, *le Chiffrement de bout en bout*, https://www.whatsapp.com/faq/fr/general/28030015, consulté le 5 avril 2017.

[1871] Information issue du site Whatsapp : https://www.whatsapp.com/about/, consulté le 3 aout 2017.

[1872] Vincent Limorte, François Verry et Sébastien Fontaine, *« SSL et TLS »,* en ligne à l'URL : http://www.authsecu.com/ssl-tls/ssl-tls.php, consulté le 3 aout 2017.

[1873] Décret nº73-364 du 12 mars 1973 *relatif à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions ;* Deuxième catégorie - Matériels destinés à porter ou à utiliser au combat

avril 1939[1874] et complété par le décret nº 73-364 du 12 mars 1973, relatif à l'application du décret du 18 avril 1939, ce cadre réglementaire imposait un contrôle minutieux quant à la fabrication, la commercialisation et la détention de ces outils. Étant considéré comme une arme de guerre, le principe de son utilisation en était l'interdiction.

Le décret d'application du 12 mars 1973 a été sujet à plusieurs amendements, dont le décret nº 86-250 du 18 février 1986[1875]. Considérant les innovations technologiques de l'époque, le décret du 18 février 1986 contribua à mieux définir le chiffrement. Toujours qualifié d'arme de guerre de deuxième catégorie, il fut décrit, aux termes de l'article 1, comme « *matériels ou logiciels conçus soit pour transformer à l'aide de conventions secrètes des informations claires ou des signaux en informations ou signaux inintelligibles, soit pour réaliser l'opération inverse* ». Le principe de son interdiction perdurait, mais la demande d'autorisation était faite auprès du ministre des Postes, Télégraphes et Téléphones (PTT) et non plus auprès du ministre de la Défense. Suite à ce changement de tutelle, le régime juridique de la cryptographie va connaître un tournant en décembre 1990 avec l'adoption de la Loi de Réforme des Télécommunications[1876]. La cryptologie est alors considérée comme une branche du droit des télécommunications. La loi du 26 juillet 1996 pour la réglementation des télécommunications[1877], avec ses douze décrets et arrêtés d'application[1878] publiés au Journal

---

les armes à feu : § 4 d) Équipements de chiffrement, de cryptophonie ou de cryptographie. Publié au JORF du 30 mars 1973 p. 3517.

[1874] Décret-loi du 18 avril 1939 *fixant le régime des matériels de guerre, armes et munitions*, Publié au JO du 13 juin1939 pp. 7463-7466.

[1875] Décret nº 86-250 du 18 février 1986, *portant modification du décret nº 73- 364 du 12 mars 1973 relatif à l'application du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions*, publié au JO du 26 Février 1986.

[1876] Loi nº 90-1170 du 29 décembre 1990 *sur la réglementation des télécommunications*, publiée au JORF nº303 du 30 décembre 1990 p. 16439.

[1877] Loi nº 96-659 du 26 juillet 1996 de réglementation des télécommunications, publiée au JORF nº174 du 27 juillet 1996 p. 11384.

[1878] Décret nº98-101 du 24 février 1998 *définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie*, publié au JORF du 25 février 1998 p.2911; Décret nº 98-102 du 24 février 1998 *définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la règlementation des télécommunications*, publié au JORF du 25 février 1998 ; Décret nº 98-206 du 23 mars 1998 *définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable*, publié au JORF nº71 du 25 mars 1998 p. 4448 ; Décret nº 98-207 du 23 mars 1998 *définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation*, publié au JORF nº71 du 25 mars 1998 p. 4449 ; Décret nº99-200 du 17 mars 1999 *définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable,* publié au JORF nº66 du 19 mars 1999 p. 4051 ; Arrêté du 13 mars 1998 *définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie* ; Arrêté du 13 mars 1998 *définissant le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis à autorisation* ; Arrêté du 13 mars 1998 *fixant la forme et le contenu du dossier de demande d'agrément*

Officiel en février et mars 1998, va partiellement assouplir le régime de la cryptologie grâce à son article 17 qui modifie l'article 28 de la loi du 29 décembre 1990 relative au chiffrement. Mais il faudra attendre la loi pour la confiance dans l'économie numérique pour voir la cryptographie reconnue d'usage libre. Présentée à l'Assemblée nationale en janvier 2003 et définitivement adoptée par les parlementaires, le 21 juin 2004, la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[1879] a pour principaux objectifs de donner un essor au commerce électronique et à la sécurité des transactions en ligne. Au terme du chapitre II du titre III de la LCEN, intitulé « *De la Sécurité dans l'Économie Numérique* » le régime actuel est consacré en matière de chiffrement. Cette libéralisation du chiffrement a été ensuite complétée par le décret du 2 mai 2007[1880] et l'arrêté du 25 mai 2007[1881], rendant applicables les articles 30, 31, et 36 de la LCEN. L'article 40 de la loi a abrogé dans le même temps l'article 28 de la loi nº 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications.

Ainsi considéré comme arme de guerre de deuxième catégorie au lendemain de la Seconde Guerre mondiale, il a fallu attendre la contrainte du commerce électronique et de la sécurité des échanges et des paiements pour voir la cryptographie autorisée dans la législation française. Cette autorisation a permis le chiffrement de bout en bout ainsi que l'utilisation du protocole HTTPS utilisant la sécurité issue de SSL/TLS.

En septembre 2014, Apple et Google, qui contrôlent 96 % du marché mondial des smartphones[1882], ont modifié leurs systèmes d'exploitation de manière à garantir un chiffrement total des appareils[1883]. En 2015, le procureur de la République François Molins, avec trois autres

---

des organismes gérant pour le compte d'autrui des conventions secrètes ; Arrêté du 13 mars 1998 *fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes* ; Arrêté du 13 mars 1998 *fixant le tarif forfaitaire pour la mise en œuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi nº 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications*.

[1879] Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique*, publiée au JORF nº0143 du 22 juin 2004 p. 11168.

[1880] Décret nº 2007-663 du 2 mai 2007 *pris pour l'application des articles 30, 31 et 36 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie*, publié au JO du 4 Mai 2007.

[1881] Arrêté du 25 mai 2007 *définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie*, publié au JORF no 127 du 3 juin 2007.

[1882] Source Comtech Kantar Wordpanel en ligne à l'URL https://www.kantarworldpanel.com/fr/smartphone-os-market-share/.

[1883] Annoncé sous IOS 8 par Apple et Android par Google (Vincent Hermann, « Le FBI s'inquiète de l'avancée du chiffrement chez Apple et Google », *NextImpact.com*, 26 septembre 2014, URL : https://www.nextinpact.com/news/90123-le-fbi-sinquiete-avancee-chiffrement-chez-apple-et-google.htm consulté le 28 mars 2018).

procureurs internationaux, a demandé aux deux entreprises de cesser de chiffrer les données qui se trouvent sur les smartphones[1884], pour faciliter la lutte contre le terrorisme et le crime organisé. Aujourd'hui, avec la lutte contre le terrorisme, cette autorisation de chiffrement sur Internet semble vouloir être remise en cause par certains gouvernements et est contestée[1885]. Le cryptage des données est considéré comme un outil donné aux criminels pour communiquer discrètement, sans surveillance. Suite à l'attentat de San Bernadino en Californie, en décembre 2015, et à la saisie d'un iPhone crypté de l'un des auteurs de l'attentat, le FBI avait souhaité la coopération de Apple pour décrypter les données stockées dans la mémoire de l'appareil. Apple s'y est refusé arguant de la protection des données privées de ses utilisateurs[1886]. Lors de la discussion à l'Assemblée nationale du projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, un amendement proposé par un député a été adopté contre l'avis du gouvernement[1887]., Cet amendement vise à renforcer les sanctions pénales à l'encontre de ceux qui refusent de coopérer dans le cadre d'injonctions judiciaires, afin de prévenir des attentats ou d'élucider certains crimes[1888]. Au Royaume-Uni, en novembre 2015, le projet de loi « *Investigatory Powers Bill*, soutenu par le Premier ministre David Cameron[1889], prévoyait de contraindre

[1884] Relaté dans « Anti-terrorisme : l'interdiction du cryptage des smartphones, une mesure peu efficace contre les djihadistes, mais ravageuse pour l'économie et les libertés », *Atlantico*, 11 décembre 2015, en ligne à http://www.atlantico.fr/decryptage/lutte-anti-terrorisme-interdiction-cryptage-smartphones-mesure-peu-efficace-contre-djihadistes-mais-ravageuse-pour-economie-et-2487813.html#1VER0m8RHlfEFQvI.99, consulté le 3 aout 2017.

[1885] Charly Berthet, Tribune – « *Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible* », Le Monde.fr, le 22 août 2016, disponible à https://cnnumerique.fr/tribune-chiffrement/, consultée le 3 aout 2017.

[1886] Spencer Ackerman, Sam Thielman and Danny Yadron , "Apple case: judge rejects FBI request for access to drug dealer's iPhone", 29 February 2016, *The Guardian.* URL: https://www.theguardian.com/technology/2016/feb/29/apple-fbi-case-drug-dealer-iphone-jun-feng-san-bernardino consulté le 15 janvier 2018.

[1887] Discussion du projet de loi *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*, deuxième séance du jeudi 03 mars 2016, amendement nº 90, relaté à http://www.assemblee-nationale.fr/14/cri/2015-2016/20160141.asp#P737240, consulté le 7 aout 2017.
Cet amendement « *fixe clairement la responsabilité pénale des constructeurs de clés de chiffrement refusant de coopérer avec la justice, lesquels seraient désormais passibles de cinq ans d'emprisonnement et 350 000 euros d'amende. Il alourdit également la simple peine d'amende des personnes sollicitées pour la mission en la portant de 3 750 euros à 15 000 euros d'amende et deux ans d'emprisonnement* » (selon M. Philippe Goujon, député, défendant cet amendement). Cet amendement n'a pas été retenu dans le texte final de la loi nº 2016-731 du 3 juin 2016 *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*.

[1888] Conseil constitutionnel, Décision du 30 mars 2018 n°2018-696 QPC *M. Malek B. [Pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie]*

[1889] Le projet prévoyait entre autres, pour les compagnies d'Internet et de téléphonie de maintenir des capacités d'interception permanente des données personnelles (Alan Travis, « Investigatory powers bill: the key points », *The Guardian,* 4 novembre 2015, URL : https://www.theguardian.com/world/2015/nov/04/investigatory-powers-

Apple, Google et les autres entreprises du secteur, de supprimer le cryptage des données sur leurs appareils à l'aide d'une clé « passe-partout », nécessaire pour accéder à ces dites-données « privées » dans le cadre d'une affaire criminelle ou autres dans le genre[1890]. Une clause analogue avait été retirée en juin 1999 du projet de loi sur le commerce électronique[1891].

§ 3 - Les réseaux parallèles

Pour naviguer ou communiquer « sans témoins », l'internaute peut utiliser des outils spécifiques ou des réseaux non accessibles par les moteurs de recherche traditionnels, ni par les explorateurs du marché, à savoir Internet Explorer, FireFox, Chrome ou autre Opera. Si la partie cachée du Net, c'est-à-dire le DeepNet, ou Internet profond, comprend toutes les pages non indexées par les moteurs de recherche pour des raisons techniques ou de sécurité, le DeepNet ne doit pas être confondu avec le Darknet qui est un ensemble de réseaux permettant un échange de fichiers de particulier à particulier de confiance (liaisons *peer to peer*). Le Darknet[1892] a été révélé au grand public par une émission de télévision[1893] et un dossier paru dans TELERAMA[1894], ainsi que lors de la découverte d'un trafic de fausse monnaie utilisant ces réseaux parallèles en novembre 2015[1895].

Inventés à l'origine, durant les années 1970, pour désigner les réseaux qui étaient isolés d'ARPANET (l'ancêtre de l'Internet) pour des raisons de sécurité, les Darknets étaient capables de recevoir des données de la part d'ARPANET[1896], mais avaient des adresses qui n'apparaissaient pas dans les listes réseau et ne répondaient pas aux *ping*[1897] et autres requêtes.

---

bill-the-key-points consulté le 28 mars 2018). Le texte final de *Investigatory Powers Act 2016* ne contient pas cette obligation, seulement une demande d'assistance par le Secrétaire d'État auprès des opérateurs.

[1890] Relaté dans l'article « *Apple : le cryptage de données interdit au Royaume-Uni ?* », iPhonote, daté du 3 novembre 2015, en ligne à https://www.iphonote.com/actu/89908/apple-le-cryptage-de-donnees-interdit-au-royaume-uni, consulté le 7aout 2017.

[1891] Information ZDNet France du 1 et juin 1999, reprise dans https://atelier.bnpparibas/retail/breve/royaume-uni-renonce-reguler-cryptage, consulté le 7 aout 017.

[1892] Irène Bouhadana, William Gilles, Jean Harivel, « Darknet, le côté obscur du net », *Panthéon Sorbonne magazine*, nº 6, janvier-février 2014, pp. 12-15.

[1893] France 2, *Darknet, la face cachée du NET* in Envoyé spécial diffusé le vendredi 14 novembre 2013

[1894] Olivier TESQUET, « *Darknet, immersion en réseaux troubles* » in Télérama nº 3322 du 14 septembre 2013

[1895] Ayant fait l'objet d'une intervention de l'auteur dans le journal de TF1.

[1896] "A history of the Darknet", *McCann Cyber Investigations,* URL: http://mccann-cyber.com/a-history-of-the-darknet/#introduction consulted on 28 March 2018.

[1897] Ping est le nom d'une commande informatique permettant de tester l'accessibilité d'une autre machine à travers un réseau IP, donc sa présence sur le réseau.

Le terme a gagné l'acceptation publique à la suite de la publication d'un article[1898] écrit en 2002 par quatre employés de Microsoft. L'article indique que la présence de Darknets est l'obstacle principal au développement des technologies DRM (Gestion des droits numériques).

A) Darknet, espace de liberté face à la pression des États

Pour accéder aux pages d'un Darknet, il faut être initié et télécharger des logiciels d'accès, tels que TOR, qui sécurisent et chiffrent chaque message et chaque requête. TOR, logiciel disponible librement sur Internet[1899], est l'un des logiciels les plus utilisés pour naviguer anonymement sur Internet.

Le principe de TOR est simple, mais efficace : lorsqu'un internaute se connecte au réseau, ses paquets de données transitent à travers plusieurs couches (d'où la métaphore de l'oignon), ce qui a pour objectif de dissimuler son identité, d'où la difficulté de remonter à l'ordinateur d'origine. En fait, le message va transiter, tant à l'aller qu'au retour, par plusieurs ordinateurs disposant du logiciel sur le réseau, aucun ne connaît de bout en bout le chemin parcouru[1900]. Revers de cette technique, toutes les connexions sont très lentes, puisqu'elles passent par plusieurs relais. Le Réseau TOR fait partie du Darknet. Il permet l'accès à un des réseaux parallèles, il y en a d'autres, qui permettent de communiquer à l'insu des personnes ou des logiciels qui espionneraient ou intercepteraient les communications. TOR utilise des moyens de communication qui sont sécurisés, c'est-à-dire cryptés. Avec TOR, un individu est invisible ou quasi-invisible, car son adresse IP réelle n'est pas inscrite dans les messages échangés.

Originellement développé sous l'égide de la Navy américaine, TOR est aujourd'hui développé et maintenu par une organisation indépendante, le TOR Project. Pour l'année fiscale 2011, 60 % de son financement provenait du gouvernement américain, et 18 % de fondations et de subventions, comme l'indique son rapport[1901]. En 2017, parmi les sponsors figurait toujours le US Department of State. Éternel paradoxe : la protection offerte par le réseau est à la fois utilisée par les militaires américains, à des fins de renseignement notamment, et combattue par la NSA et le GCHQ, son équivalent britannique.

[1898] Peter Biddle, Paul England, Marcus Peinado et Bryan Willman, *The Darknet and the Future of Content Distribution, 2002.*

[1899] At https://www.torproject.org/ .

[1900] Voir Annexe 3 – Principes de fonctionnement de TOR.

[1901] At https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf .

Darknet a été créé à l'origine pour aider les dissidents chinois à communiquer entre eux sans pouvoir être identifiés. La création du Darknet a donc permis aux dissidents d'exister, de pouvoir communiquer entre eux et le reste du monde, et donc de faire suivre l'information à travers le WEB sans aucun risque pour leur sécurité[1902]. Le Darknet est donc originellement un outil de défense des libertés. Les défenseurs de la vie privée considèrent le système TOR comme un bon outil pour les internautes désireux de se protéger. Des journalistes l'utilisent également pour ne pas être repérés dans des régimes répressifs ou échanger avec des sources sensibles sans risquer de les compromettre. « *L'anonymat fait partie de la liberté d'expression. Sans anonymat, les journalistes n'auraient pas de source* »[1903]. TOR fait partie des outils recommandés par Reporters sans frontières (RSF) qui forme des journalistes dans les pays où la liberté de la presse est combattue.

Outre TOR, d'autres réseaux comme I2P[1904], pour Internet Invisible Project, ou Freenet[1905], permettent à plusieurs ordinateurs de communiquer entre eux. Sur le site du réseau anonyme, Freenet[1906], il est écrit : « *Le "Darknet" est un développement récent, que peu d'autres réseaux possèdent : en se connectant uniquement aux personnes à qui ils font confiance, les utilisateurs peuvent grandement améliorer leur sécurité, et ils peuvent toujours se connecter au réseau principal à travers les amis des amis, etc. de leurs amis. Ceci permet à certaines personnes d'utiliser Freenet dans des endroits où Freenet pourrait être illégal, rend Freenet très difficile à bloquer par les gouvernements, et ne se base pas sur le fait d'accéder au "monde libre" via un portail sécurisé* ». Ainsi, Freenet se présente comme un instrument de propagation de la liberté, mais de fait, le Darknet permet également à des réseaux pédophiles ou terroristes d'échanger des informations en toute impunité, nous ramenant à l'antagonisme liberté c/ sécurité.

[1902] Rappelé dans la présentation sur le site https://www.torproject.org/about/overview.html.en consulté le 15 janvier 2018.
[1903] Citation de Jérémie Zimmermann, cofondateur de la Quadrature du Net, organisation de défense des droits des internautes.
[1904] At http://www.i2p2.de/ .
[1905] At https://freenetproject.org/ .
[1906] Freenet est un réseau informatique anonyme et distribué construit sur l'Internet. Il vise à permettre une liberté d'expression et d'information totale fondée sur la sécurité de l'anonymat, et permet donc à chacun de lire comme de publier du contenu. Il offre la plupart des services actuels d'Internet (courriel, WEB, forums, etc.).

B) Darknet, espace libertaire et criminogène

TOR permet également d'accéder à des sites cachés dont l'URL se termine par « . onion » et dont l'adresse n'est pas décodée par les serveurs DNS[1907] du réseau Internet. TOR ne donne pas accès à des sites « oignon » dès son utilisation, il fournit seulement une manière cryptée, chiffrée et surtout masquée pour accéder au WEB normal. L'accès aux services cachés, déployés depuis 2004, n'est qu'un des usages possibles de TOR. Il peut simplement être utilisé pour consulter son courrier, faire de la messagerie instantanée ou se connecter au WEB « visible » via le réseau de façon anonyme, sans utiliser la possibilité d'accès aux sites particuliers.

Pour accéder aux sites « oignon », il faut être conscient qu'ils existent et connaître leurs adresses dans le réseau TOR. L'installation de TOR n'est pas suffisante pour accéder au Darknet associé, le réseau TOR, il faut utiliser un navigateur spécifique à TOR (installé avec le package TOR, *Tor Browser Bundle*) et connaître les adresses des sites à visiter, toutes se terminant par « . *onion* ».

Pour les visiteurs qui ne connaîtraient pas leur destination finale, The Hidden Wiki[1908] (le « Wiki caché ») offre un rapide panorama des ressources du Darknet. Ce portail recense certaines des adresses les plus populaires du Darknet. Outre une vaste offre de solutions d'hébergement et de courriel, le Wiki caché liste aussi bien des blogs parodiques que des forums consacrés à l'occultisme ou à la fabrication d'armes à feu à l'aide d'imprimantes 3D, mais aussi d'accéder à des activités réprimées par la loi.

Sur le réseau TOR, les transactions ne sont pas réalisées en euro ou en dollar, mais en bitcoin. Les euros ou les dollars s'échangent contre des bitcoins auprès de changeurs officieux et non régulés. Fondé sur la cryptographie, un porte-monnaie bitcoin, souscrit en ligne, possède deux clés. La première clé est publique — c'est en quelque sorte l'équivalent d'un RIB, — et destinée à recevoir de l'argent. La seconde est privée, elle permet de régler les achats de manière totalement anonyme[1909]. Pour les gouvernements, le bitcoin devient le nouveau véhicule du blanchiment d'argent[1910]. La sécurité des transactions est garantie par l'utilisation d'une

[1907] Il s'agit d'un serveur spécial qui fait correspondre un nom de serveur à une adresse IP. DNS est l'acronyme de Domain Name System ou système des noms de domaine.

[1908] At http://www.hiddenwiki.org/ .

[1909] La monnaie Bitcoin est gérée de façon décentralisée par la technologie blockchain. Plutôt que de consigner toutes les transactions dans un grand livre comptable (comme le font par exemple les banques centrales), la crypto-monnaie a en effet choisi de décentraliser l'historique des transactions. Ces « blocs » sont détenus par les détenteurs de bitcoins eux-mêmes, et garantissent à chaque instant l'authenticité et l'unicité des transactions.

[1910] Bruno Dalles, « Les nouveaux instruments de paiement, avatars de la monnaie fiduciaire : de nouveaux facteurs de risque en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme », *Annales des*

procédure particulière et un registre des transactions, le BlockChain. Fin août 2016, il y avait environ 16 000 000 de bitcoins en circulation, représentant un montant de plus de 9 000 000 000 US $[1911]. Le système est théoriquement limité à 21 000 000 unités.

Revers de la médaille, l'anonymat total sur le WEB a été utilisé pour d'autres usages que la liberté d'expression par certains groupes criminels, l'un des premiers a été les Farc (Forces armées révolutionnaires de Colombie) qui ont vu dans le Darknet la possibilité de communiquer entre eux plus facilement et de s'adonner à des activités lucratives et illégales sur le WEB[1912].

Le Darknet est devenu la boutique mafieuse du WEB puisqu'il y est possible, par exemple, d'engager un tueur à gages, d'acheter de la drogue ou des armes, d'acheter une fausse carte d'identité et de consulter des sites pédophiles… Tout ce que l'humanité a inventé de criminel est présent et disponible sur le Darknet qui constitue donc un espace de liberté pour le pire ou le meilleur, permettant un développement de la cybercriminalité. La liberté en absence de surveillance peut conduire à une criminalité incontrôlée. L'humanité n'est pas un groupe pacifique et naturellement bon, comme la décrivait Jean-Jacques Rousseau[1913], mais ressemble plutôt à une jungle. Les règles de la société sont à présenter comme des limites à ne pas franchir pour une coexistence pacifiée[1914].

La vie privée peut être anéantie par une société numérique surveillant et enregistrant toute action. Se cacher pour éviter cette surveillance a permis à des organisations criminelles de s'établir sur Internet. Cette criminalité est aussi une source d'atteinte aux libertés et elle peut interférer avec la démocratie en faussant ou orientant les résultats d'élections. Mais la société numérique peut aussi utiliser les moyens nouveaux mis à disposition par la technique pour modifier les processus de décisions démocratiques.

Mines - Réalités industrielles, 2017/4 (Novembre 2017), pp. 23-27. URL : https://www.cairn.info/revue-realites-industrielles-2017-4-page-23.htm consulté le 12 avril 2018.

[1911] Source https://blockchain.info/fr/charts/market-cap consultée le 30 aout 2016.

[1912] Pierre-Marc de Biasi, Clara Schmelck, « Les réseaux du chaos », *Médium*, 2016/4 (N° 49), pp. 70-82. URL : https://www.cairn.info/revue-medium-2016-4-page-70.htm consulté le 12 avril 2018.

[1913] Jean-Jacques Rousseau, *Discours sur l'origine et les fondements de l'inégalité parmi les hommes*, Marc Michel Rey, 1755.

[1914] Enzo Lesourt, « Réconcilier souveraineté individuelle et vie en société : la société écologiste d'André Gorz et la société conviviale d'Ivan Illich », *Natures Sciences Sociétés*, 2013/3 (Vol. 21), pp. 307-314. URL : https://www.cairn.info/revue-natures-sciences-societes-2013-3-page-307.htm consulté le 18 février 2018.

Chapitre 2. L'émergence d'une démocratie participative conséquence de l'ouverture des données

Si la numérisation de la société a un effet collatéral sur la vie privée des individus, elle modifie aussi la relation entre l'individu-citoyen et l'administration. Elle favorise la connaissance et en conséquence crée une interaction entre le citoyen informé et les différents organes gouvernementaux. La démocratie peut bénéficier des techniques numériques pour se modifier et tendre vers une démocratie collaborative où les citoyens participent à la vie de la cité et disposent des libertés publiques, liberté d'expression, de réunion, de pétition, ainsi que des informations nécessaires à leur prise de décision. Cette émergence d'une démocratie collaborative présume une information libre, exacte et disponible.

En 1978, la France promulguait deux lois importantes dans une société où l'informatique commençait à investir les entreprises et l'administration : la loi « informatique et libertés »[1915] pour la protection des données personnelles face aux traitements automatiques et la loi dite « CADA »[1916] pour la diffusion des données administratives. Chacune de ces lois créait une autorité administrative indépendante chargée de veiller au respect des nouveaux droits : la CNIL[1917] et la CADA[1918]. Ce n'est qu'en 2016, avec la loi pour une République numérique[1919] que ces deux autorités administratives disposent d'une instance commune de concertation alors que des liens entre l'Open data et la protection des données à caractère personnel existent[1920].

[1915] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, publiée au Journal Officiel de la République française du 07 janvier 1978, p. 227.
[1916] Loi nº 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*, publiée au Journal Officiel de la République française du 18 juillet 1978, p. 2851.
[1917] Commission nationale de l'informatique et des libertés.
[1918] Commission d'accès aux documents administratifs.
[1919] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, Art. 26 : « *La Commission nationale de l'informatique et des libertés et la Commission d'accès aux documents administratifs se réunissent dans un collège unique, sur l'initiative conjointe de leurs présidents, lorsqu'un sujet d'intérêt commun le justifie* ».
[1920] Matthieu Berguig, François Coupez, « Faut-il réellement craindre l'Open data pour la protection de nos données personnelles ? », *LEGICOM*, 2016/1 (N° 56), pp. 15-24. URL : https://www.cairn.info/revue-legicom-2016-1-page-15.htm consulté le 15 janvier 2018.

Vingt ans plus tard, lors du discours d'Hourtin en 1999[1921], M. Lionel Jospin, Premier ministre, pouvait affirmer : « *L'administration française devient "électronique". En janvier, nous avons publié le décret rendant opposables à l'administration les formulaires mis en ligne. Cette année, près d'un million de contribuables ont calculé le montant de l'impôt sur le revenu par l'Internet. Depuis le début de l'été, les annonces de marchés publics sont disponibles sur le réseau. Nous poursuivons ainsi dans le sens de la diffusion gratuite sur l'Internet des données publiques les plus utiles à nos concitoyens et à nos entreprises* ».

Les techniques numériques ont permis de mettre en œuvre la mise à disposition de tous les documents administratifs. Au travers de cette disponibilité de l'information, le citoyen peut connaître les objectifs atteints ou non d'un gouvernement[1922]. La vie politique devient plus transparente, même si certaines informations restent difficilement accessibles[1923]. En France, l'*open data* désigne à la fois des « *données qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation* » (« *données ouvertes* ») et à la fois la « *politique par laquelle un organisme met à la disposition de tous des données numériques, dans un objectif de transparence ou afin de permettre leur réutilisation, notamment à des fins économiques* » (« *ouverture des données* »)[1924]. Initialement régi par la loi du 17 juillet 1978, la mise à disposition des données et l'organisation et le rôle de la Commission d'accès aux documents administratifs (CADA) sont principalement régis par le Code des relations entre le public et l'administration[1925]. La loi du 29 décembre 2015[1926], qui transpose en droit français la directive du 26 juin 2013[1927], impose de manière expresse un

[1921] Déclaration de M. Lionel Jospin, Premier ministre, sur la mise en œuvre et les orientations de développement du Programme d'action gouvernementale pour la société de l'information (PAGSI) depuis son lancement en 1997 et la préparation du passage électronique à l'an 2000, Hourtin le 26 août 1999, disponible à http://discours.vie-publique.fr/notices/993002100.html, consultée le 11 juillet 2016.

[1922] Jean-Pierre Nioche, « Les trois paradigmes de l'évaluation des politiques publiques face à l'obligation de rendre des comptes et de rendre compte », *Revue française d'administration publique*, 2016/4 (N° 160), pp. 1227-1240. URL : https://www.cairn.info/revue-francaise-d-administration-publique-2016-4-page-1227.htm.

[1923] William Gilles, "From the right to transparency to the right to Open Government in a digital era. A French approach", Irène Bouhadana, William Gilles (dir.), *Revue Internationale des Gouvernements Ouverts* Vol.2 (2015), pp. 11-23. URL : http://ojs.imodev.org/index.php/RIGO/article/view/4/34 consulté le 7 février 2018.

[1924] Commission d'enrichissement de la langue française, « Vocabulaire de l'informatique et du droit », Journal *officiel* du 03 mai 2014 p. 7639.

[1925] Code des relations entre le public et l'administration, Art. L.300-1 et suivants.

[1926] Loi n° 2015-1779 du 28 décembre 2015 *relative à la gratuité et aux modalités de la réutilisation des informations du secteur public* publiée au JORF du 29 décembre 2015 page 24319.

[1927] 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.

« *droit à la réutilisation de la donnée* », celles-ci devant l'être « *sous forme électronique et, si possible, dans un format ouvert* »[1928].

La protection des données à caractère personnel peut devenir un obstacle à l'ouverture de ces données. La loi pour une République numérique[1929] a prévu que la CNIL et la CADA pouvaient se réunir en une instance nouvelle pour traiter ces cas particuliers[1930]. Mais, pour cette raison, Gilles Babinet qui prône de mettre l'open data au service de l'action publique[1931], proposait, dans un entretien à l'Usine nouvelle en février 2013, de supprimer la Commission nationale de l'informatique et des libertés, qualifiée d'« *ennemie de la Nation* »[1932].

Le 2 mai 2014, La France rejoint le « Partenariat pour un gouvernement ouvert », en anglais « *Open Government Partnership* » ou OGP, et souhaite ainsi promouvoir « la transparence, la participation des citoyens à l'action publique »[1933].

Le gouvernement ouvert (en anglais *open government*) est une doctrine de gouvernance qui vise à améliorer l'efficacité et la responsabilité des modes de gouvernance publique[1934]. Elle établit que les citoyens ont le droit d'accéder aux documents et aux procédures de leurs gouvernements afin de favoriser une transparence et une responsabilisation accrue et de donner aux citoyens les moyens nécessaires pour contrôler, superviser et prendre part aux décisions gouvernementales et territoriales[1935].

Le gouvernement ouvert vise à promouvoir : la transparence, comme garant de la confiance entre citoyen et politique, par la publication des données publiques dans le cadre d'une stratégie

---

[1928] Loi n° 2015-1779 Art. 1 et 2.

[1929] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique* publiée au JORF n°0235 du 8 octobre 2016.

[1930] Loi n° 2016-1321 du 7 octobre 2016, Art. 26 et 28.

[1931] « *L'Open data concourt à plusieurs objectifs : amélioration de la connaissance, interactivité avec les citoyens, transparence des institutions publiques et création de nouveaux services nés de la combinaison et d'une réutilisation innovante de ces données*. » (Gilles Babinet, « Pour un new deal numérique », Institut Montaigne, février 2013, en ligne à l'URL : http://www.institutmontaigne.org/ressources/pdfs/publications/etude_pour_un_new_deal_numerique.pdf, consulté le 6 février 2018).

[1932] Relaté par Matthieu Berguig, François Coupez, « Faut-il réellement craindre l'Open data pour la protection de nos données personnelles ? », *LEGICOM*, 2016/1 (N° 56), pp. 15-24. URL : https://www.cairn.info/revue-legicom-2016-1-page-15.htm consulté le 6 février 2018.

[1933] Extrait de la lettre de candidature de la France à l'OGP, Marylise Lebranchu, disponible à http://www.opengovpartnership.org/sites/default/files/Screen%20Shot%202014-05-21%20at%202.02.06%20PM_0.png, consultée le 11 juillet 2016.

[1934] William Gilles, « Le Droit au Gouvernement Ouvert : Enjeux d'un Nouveau Droit à l'Ère du Numérique au Regard de l'Expérience Française », Irène Bouhadana, William Gilles (dir.), *Revue Internationale des gouvernements ouverts,* Vol. 1, 2014, pp. 11-24, URL : http://ojs.imodev.org/index.php/RIGO/article/view/211/352 consulté le 28 mars 2018.

[1935] Melanie Chernoff, « What is open government ? », *opensource.com,* URL: https://opensource.com/resources/open-government consulté le 15 janvier 2016.

de données ouvertes ; la participation citoyenne, en incitant le gouvernement à consulter et à écouter les citoyens pour la prise des décisions en mettant en place des canaux de communication avec eux ; la collaboration avec les composantes de la société civile pour une meilleure efficacité des modes de gouvernance[1936].

[1936] William Gilles, « Le Droit au Gouvernement Ouvert : Enjeux d'un Nouveau Droit à l'Ère du Numérique au Regard de l'Expérience Française », Op. cit.

Section 1. Le gouvernement ouvert

En préface du plan d'action 2015-2017[1937], M. François Hollande, Président de la République, rappelle le principe de notre République : « *Le gouvernement du peuple, par le peuple et pour le peuple* »[1938]. Afin de pouvoir vérifier que les dirigeants respectent ces principes, il est nécessaire comme le proclame la Déclaration des droits de l'homme et du citoyen, que le peuple soit correctement informé. Cette nécessité d'information est une des conditions pour que le citoyen puisse contrôler le bien-fondé des impôts[1939] et leur acceptation. Si en 1789, la diffusion générale des informations butait sur l'utilisation de la seule imprimerie et l'analphabétisme du peuple, aujourd'hui avec la diffusion numérique des données et l'éducation obligatoire, cette information est disponible et mise à disposition de tous.

En 2009, dès qu'il est arrivé au pouvoir, Barack Obama, Président des États-Unis d'Amérique a lancé son initiative de gouvernement ouvert, respectant ainsi l'une de ses promesses de campagne, concernant la transparence de son administration[1940], et donnant une nouvelle impulsion à la loi « *Freedom of Information Act* » de 1 966[1941]. Dans ce mémorandum, le Président énonce trois principes généraux : le gouvernement doit être transparent, le gouvernement doit être participatif, le gouvernement doit être collaboratif. Cette information et cette transparence sont nécessaires à la connaissance, à l'expression de la liberté de choix et à l'épanouissement de la liberté d'expression.

[1937] *Pour une action publique transparente et collaborative : Plan d'action national pour la France 2015-2017*, disponible à http://www.opengovpartnership.org/sites/default/files/2015%2007%2009_Plan%20gouvernement%20ouvert%20FR%20Version%20Finale.pdf, consulté le 11 juillet 2016.

[1938] Définition de la démocratie donnée par Abraham Lincoln sur le site de la bataille de Gettysburg, le 18 novembre 1863.

[1939] Déclaration des droits de l'homme et du citoyen de 1 789 : « Art. 14. *Tous les Citoyens ont le droit de constater, par eux-mêmes ou par leurs représentants, la nécessité de la contribution publique, de la consentir librement, d'en suivre l'emploi, et d'en déterminer la quotité, l'assiette, le recouvrement et la durée.*
« Art. 15. *La Société a le droit de demander compte à tout Agent public de son administration ».*

[1940] Barack Obama, Mémorandum pour un gouvernement ouvert, ("*Memorandum for the Heads of Executive Departments and Agencies - SUBJECT: Transparency and Open Government*"), Publié à https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment, consulté le 11 juillet 2016.

[1941] Public Law 89-487-July 4, 1966.

Sous-section 1. L'information par les données ouvertes

La révolution numérique se caractérise par la production d'une quantité de données toujours plus abondante. L'effet conjugué de l'augmentation exponentielle de ces données, associé à la croissance des capacités de stockage et à la puissance de calcul disponible, permet, tant aux acteurs publics que privés, d'analyser et de diffuser leurs données. Cette ouverture des données administratives peut être une voie de réforme de l'État. Il conduit à l'émergence d'un gouvernement ouvert.

L'ouverture des données, ou en anglais *open data,* ne doit pas être confondu avec le phénomène de données de masse, ou *big data.* Cette dernière notion vise à exploiter sous un angle nouveau les données collectées ou crées à l'origine pour une finalité autre. Elle permet aussi l'enrichissement des données par leur croisement[1942].

Un gouvernement ouvert informe les citoyens sur les raisons de ses choix et sur les résultats obtenus. Pour ce faire, il doit mettre à disposition des citoyens les données nécessaires à cette information. Cette mise à disposition doit être sincère et accessible à tous. Elle doit être réalisée en fournissant des données brutes dans un format accessible à tous et réutilisable. Des freins à cette mise à disposition peuvent exister[1943] : licences d'utilisation excessives (Irlande), délais longs d'accès (Allemagne, Portugal, République Tchèque, République Slovène, Suède) ou faible liberté d'accès légal (Allemagne, Portugal, Suède). La fourniture de données brutes, c'est-à-dire non interprétées ou édulcorées, doit être réalisée dans un format réutilisable directement, c'est-à-dire par exemple, ne pas être proposée sous le format d'une photographie d'un document, sauf pour des documents anciens non numérisés, mais dans un format numérique réutilisable par une application informatique, donc dans un format ouvert. La loi du 21 juin 2004 pour la confiance dans l'économie numérique donne une définition précise d'un format ouvert[1944] : « *On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérables et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre* ». Les

[1942] Pierre-Yves Baudot, « Introduction », *Informations sociales*, 2015/5 (n° 191), pp. 4-7. URL : https://www.cairn.info/revue-informations-sociales-2015-5-page-4.htm consulté le 17 janvier 2018.
[1943] Irène Bouhadana, "The right of access to public information: an analysis of international conventions", Bouhadana Irène, Gilles William (sous la direction.), *International Journal of Open Government*, pp. 1-10, http://ojs.imodev.org/index.php?journal=RIGO, consulté le 20 juillet 2016.
[1944] Loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique*, Art. 4.

formats de diffusion ouverts, donc utilisables par un ordinateur peuvent être le format XML[1945] pour les données, même si ce format a été coédité par Microsoft qui l'utilise dans sa suite bureautique OFFICE, et le format PDF[1946] pour les documents. D'autres formats ouverts sont disponibles et permettent l'échange de données : TXT (texte brut en ASCII) ou RTF (*Rich Text Format*) pour les documents, ODF (*Open Document Format*) pour des documents modifiables par des logiciels libres, etc.

En France, l'ouverture des données administratives a été confirmée dès 1978, par la loi CADA[1947]. En 2011, la « mission ETALAB » est créée auprès du Premier ministre. Elle est chargée de créer et alimenter le portail de données publiques ouvertes data.gouv.fr, en ligne depuis le 5 décembre 2011[1948]. Le 16 septembre 2014, est créée la fonction d'Administrateur Général des Données[1949], placé sous l'autorité du Premier ministre. Son rôle est de coordonner « *l'action des administrations en matière d'inventaire, de gouvernance, de production, de circulation et d'exploitation des données par les administrations* » et d'organiser, « *dans le respect de la protection des données personnelles et des 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* »[1950]. Dans son premier rapport, l'administrateur général des données présente dans son introduction l'analyse prédictive pouvant être effectuée à partir des données disponibles et permettant, entre autres, « *d'augmenter l'autonomie et la liberté de choix des usagers du service public* »[1951]. Il confirme ainsi que l'ouverture des données a pour

[1945] XML ou *Extensible Markup Language*, défini en 1998 et revu en 2004, doit permettre la transmission, la réception et le traitement de données sur le WEB de la même manière que HTML. XML est un sous ensemble de SGML (*Standard Generalized Markup Language*), défini par le standard ISO8879 en 1986, utilisé dans le milieu de la Gestion Electronique Documentaire (GED). XML est un métalangage et il permet de structurer, poser le vocabulaire et la syntaxe des données qu'il va contenir.

[1946] PDF ou *Portable Document Format*, est un langage de description de ps créé par la société Adobe Systems en 1993. Le format ouvert « ISO 32000 — 1:2008 PDF » a été publié par l'Organisation internationale de normalisation (ISO) le 1er juillet 2008. PDF est à présent une norme ISO, intitulée « Gestion de documents - - Format de document portable - - Partie 1 : PDF 1.7 ».

[1947] Loi nº 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*, publiée au Journal Officiel de la République française du 18 juillet 1978, p. 2851.

[1948] Circulaire du 26 mai 2011 *relative à la création du portail unique des informations publiques de l'Etat « data.gouv.fr » par la mission « Etalab » et l'application des dispositions régissant le droit de réutilisation des informations publiques*, publiée au JORF nº 0123 du 27 mai 2011 p. 9140.

[1949] Décret nº 2014-1 050 du 16 septembre 2014 *instituant un administrateur général des données*, publié au JORF nº 0215 du 17 septembre 2014.

[1950] Ibid. Article 2.

[1951] Administrateur général des données, *Les données au service de la transformation de l'action publique*, Rapport au Premier ministre sur la gouvernance de la donnée 2015, décembre 2015, disponible à

conséquence, outre l'information des citoyens, une amélioration de leur autonomie en matière de choix, donc de décision[1952].

Dans l'Union européenne, le mouvement des données ouvertes est encadré par la directive 2003/98/CE[1953]. Dans le cadre de la protection de l'environnement, elle a été complétée par la directive 2007/2/CE[1954] du 14 mars 2007, dite directive INSPIRE, transposée dans le droit français depuis l'ordonnance du 21 octobre 2010[1955]. Au Royaume-Uni, un projet est officiellement lancé en janvier 2010, par Gordon Brown. Ce projet oblige le gouvernement à publier, entre autres, toute dépense supérieure à 25 000 livres sterling en utilisant les technologies du WEB. La République fédérale d'Allemagne a ouvert son site govdata.de en 2013.

Sous-section 2. La transparence gouvernementale

La transparence des gouvernements découle du contrat social[1956]. Mais pour des raisons stratégiques ou politiques, les gouvernements peuvent occulter des informations, soit pour des raisons légales de sécurité et de défense de l'État, soit pour des raisons économiques ou politiques qui faussent les relations inter-étatiques ou l'information citoyenne. Ces informations peuvent se voir révélées par des lanceurs d'alerte[1957]. Une information sincère est nécessaire au citoyen pour évaluer la politique gouvernementale et pouvoir user de son droit de vote en toute liberté et en toute connaissance. L'émergence des fausses nouvelles ou en anglais *fake news,*

http://www.gouvernement.fr/partage/6252-rapport-au-premier-ministre-sur-la-gouvernance-de-la-donnee-2015 consulté le 20 juillet 2016.

[1952] « Au-delà de l'ouverture des données, ce qui est en jeu, c'est l'ouverture de la décision », *Informations sociales*, 2015/5 (n° 191), pp. 20-25. URL : https://www.cairn.info/revue-informations-sociales-2015-5-page-20.htm consulté le 17 janvier 2018.

[1953] Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 *concernant la réutilisation des informations du secteur public*, publiée au Journal officiel n º L 345 du 31/12/2003 pp. 90-96.

[1954] Directive 2007/2/CE du Parlement européen et du Conseil *établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE)*, publiée au Journal officiel de l'Union européenne nº L108/1 du 25/04/2007.

[1955] Ordonnance n° 2010-1232 du 21 octobre 2010 *portant diverses dispositions d'adaptation au droit de l'Union européenne en matière d'environnement* publiée au JORF n°0246 du 22 octobre 2010 page 18885.

[1956] Jean-Jacques Rousseau, *Du contrat social ou Principes du droit politique,* 1762, Marc Michel Rey, Amsterdam.

[1957] Patrice Cailleba, « Lanceur d'alerte et silence organisationnel », *Revue internationale de psychosociologie et de gestion des comportements organisationnels*, 2017/56 (Vol. XXIII), pp. 309-334. URL : https://www.cairn.info/revue-internationale-de-psychosociologie-de-gestion-des-comportements-organisationnels-2017-56-page-309.htm consulté le 17 janvier 2018.

lancées durant les campagnes électorales nord-américaines de 2016[1958] ou françaises de 2017[1959], démontre l'importance d'une information contrôlée dans les processus démocratiques afin de ne pas modifier indûment les choix électoraux.

§ 1 - La légalisation de la transparence

L'ouverture des données est nécessaire à la transparence d'un gouvernement, première étape pour un gouvernement ouvert avec la participation citoyenne et la collaboration. Sous l'ancien régime, la royauté était de droit divin et il était vain de chercher à différencier les finances du souverain de celles de l'État. L'absence de budget réel révèle l'absence de transparence dans le royaume de France[1960]. La première publication d'un budget fut effectuée par Necker[1961] en janvier 1781, en rupture avec la législation de l'époque interdisant toute publication de travaux ou projets concernant les réformes financières ou l'administration passée, courante ou future. Cette absence de transparence était censée protéger le pouvoir. Sous l'influence des auteurs des XVII et XVIII[e] siècle, John Locke[1962], Thomas Paine[1963] ou Montesquieu[1964], cette notion de droit divin va disparaître. Le pouvoir des dirigeants découle d'une acceptation des citoyens, d'un contrat social[1965]. Ce principe est repris dans la déclaration d'indépendance des États-Unis d'Amérique[1966] : « *Les gouvernements sont établis parmi les hommes pour garantir ces droits*

[1958] Durant la campagne présidentielle de 2016, aux États-Unis d'Amérique, une campagne contre Hilary Clinton a été montée à base de fausses informations, relayées ou lancées par l'équipe de campagne de Donald Trump.
[1959] Durant le second tour de la campagne des présidentielles de 2017, le FN, parti de Marine Le Pen, a lancé de fausses informations concernant Emmanuel Macron. Durant l'émission opposant face à face les deux candidats, Marine Le Pen a même évoqué un supposé compte bancaire dans un paradis fiscal.
[1960] William Gilles, "From the right to transparency to the right to open government in digital era. A French approach", Bouhadana Irène, Gilles William (sous la direction.), *International Journal of Open Government*, pp. 11-26, disponible à http://ojs.imodev.org/index.php?journal=RIGO consulté le 20 juillet 2016.
[1961] Connu sous le nom de « Compte-rendu de Necker ».
Compte rendu au Roi, par M. Necker, Directeur Général des Finances, au mois de Janvier 1781, imprimé par ordre de sa Majesté, disponible à http://gallica.bnf.fr/ark:/12148/bpt6k432409 consulté le 20 juillet 2016.
[1962] John Locke, *Two treatises of government*, 1 689 (en français, Traité du gouvernement civil).
[1963] Thomas Paine, *Common sense addressed to the inhabitants of America*, 10 janvier 1776.
[1964] Montesquieu, *De l'esprit des lois*, 1 748.
[1965] Thomas Hobbes, *Leviathan or the matter, form and power of a common wealth ecclesiastical and civil*, 1 651 (en français Le Léviathan, ou Traité de la matière, de la forme et du pouvoir d'une république ecclésiastique et civile).
John Locke, *Questions concerning the law of nature*, 1664.
Jean-Jacques Rousseau, *Du contrat social ou Principes du droit politique,* 1 762.
[1966] The unanimous declaration of the thirteen United States of America, July 4, 1776.

[la vie, la liberté et la recherche du bonheur], et leur juste pouvoir émane du consentement des gouvernés »[1967].

Le dirigeant ou l'assemblée dirigeante à qui le pouvoir a été confié doit rendre compte aux citoyens. Le principe de la transparence fut acté par les révolutionnaires français dans la Déclaration des droits de l'homme et du citoyen de 1789[1968]. La transparence a été formalisée par la loi CADA de 1978[1969] qui oblige toute administration de l'État, collectivité territoriale, établissement public ou organisme, même de droit privé, chargé de la gestion d'un service public à communiquer les documents administratifs aux personnes qui en font la demande[1970]. Cette transparence a été modifiée par ordonnance[1971] et transposée dans le Code des relations entre le public et l'administration, les articles 1 à 9[1972], 20 à 24[1973], de la loi du 17 juillet 1978 étant abrogés par cette ordonnance. C'est pratiquement l'ensemble de la loi n° 78-753 du 17 juillet 1978 (les chapitres I à III) qui se trouve aujourd'hui abrogée[1974]. La communication des documents administratifs y est réaffirmée avec certaines restrictions[1975] issues d'une autre

[1967] *That to secure these Rights, Governments are instituted among Men, deriving their just Powers from the Consent of the Governed*, extrait de la déclaration d'indépendance du 4 juillet 1776, la traduction française est attribuée à Thomas Jefferson

[1968] Déclaration des droits de l'homme et du citoyen de 1789, Articles 14 et 15 cités précédemment.

[1969] 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* publiée au JORF du 18 juillet 1978 p. 2851

[1970] Ibid., article 2.

[1971] Ordonnance n° 2015-1 341 du 23 octobre 2015 *relative aux dispositions législatives du code des relations entre le public et l'administration* publiée au JORF n° 0248 du 25 octobre 2015 p. 19872, entrée en vigueur le 1er janvier 2016.

[1972] Tous les articles du Chapitre Ier : De la liberté d'accès aux documents administratifs.

[1973] Tous les articles du Chapitre III : La commission d'accès aux documents administratifs.

[1974] Tous les articles du Chapitre II : Du droit de réutilisation des informations publiques sont abrogés par l'ordonnance n° 2016-307 du 17 mars 2016.

[1975] Code des relations entre le public et l'administration, Article L.311-5 : « *Ne sont pas communicables :*
« 1° Les avis du Conseil d'État et des juridictions administratives, les documents de la Cour des comptes mentionnés à l'article L.141-10 du code des juridictions financières et les documents des chambres régionales des comptes mentionnés à l'article L.241-6 du même code, les documents élaborés ou détenus par l'Autorité de la concurrence dans le cadre de l'exercice de ses pouvoirs d'enquête, d'instruction et de décision, les documents élaborés ou détenus par la Haute Autorité pour la transparence de la vie publique dans le cadre des missions prévues à l'article 20 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, les documents préalables à l'élaboration du rapport d'accréditation des établissements de santé prévu à l'article L.6113-6 du code de la santé publique, les documents préalables à l'accréditation des personnels de santé prévue à l'article L.1414-3-3 du code de la santé publique, les rapports d'audit des établissements de santé mentionnés à l'article 40 de la loi n° 2000-1 257 du 23 décembre 2000 de financement de la sécurité sociale pour 2001 et les documents réalisés en exécution d'un contrat de prestation de services exécuté pour le compte d'une ou de plusieurs personnes déterminées ;
« 2° Les autres documents administratifs dont la consultation ou la communication porterait atteinte :
« a) Au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif ;
« b) Au secret de la défense nationale ;
« c) A la conduite de la politique extérieure de la France ;
« d) A la sûreté de l'État, à la sécurité publique ou à la sécurité des personnes ;

ordonnance[1976]. Sont ainsi exclus de cette communication, outre les documents pouvant porter atteinte à la défense nationale et aux relations extérieures ou à la sûreté de l'État, les avis du Conseil d'État, certains documents de la Cour des comptes et les documents élaborés par la Haute autorité pour la transparence de la vie publique, les rapports d'audit des établissements de santé et les documents réalisés dans le cadre d'un contrat de prestation de service exécuté pour le compte d'une personne déterminée. Ces restrictions sont à rapprocher des contraintes mises en place pour protéger les déclarations de patrimoine, de revenu et de conflits d'intérêts des parlementaires, ces informations personnelles étant disponibles sous format de photographie de documents souvent manuscrits et pour certains seulement consultables en Préfecture sans droit de divulgation ou de publication. Si l'article 6 de la loi CADA prévoyait certaines restrictions de communication, la liste ne concernait que des documents relatifs à la sécurité de l'État ou à l'instruction d'affaires sensibles, sécuritaires ou commerciales et non les avis du Conseil d'État, ni des documents de la Cour des comptes, ni les rapports d'audit et ni les documents élaborés par la nouvelle Haute autorité pour la transparence de la vie publique. Alors que la France a présidé l'OGP en 2016, elle a mis en place une restriction légale à la transparence et à la communication publique de certains documents. Le refus d'accès à des documents administratifs doit être motivé[1977]. Le rôle de la CADA est repris dans le Titre IV du Livre III du Code des relations entre le public et l'administration. La saisine pour avis de la commission reste un préalable obligatoire à l'exercice d'un recours contentieux en cas de refus d'accès à un document administratif[1978]. En 2016, la commission a examiné 5 214 avis[1979] et a rendu un avis favorable dans 56,8 % des cas, dans les autres cas, l'avis a été défavorable, ou la

« e) A la monnaie et au crédit public ;
« f) Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ;
« g) A la recherche, par les services compétents, des infractions fiscales et douanières ;
« h) Ou sous réserve de l'article L.124-4 du code de l'environnement, aux autres secrets protégés par la loi ».

[1976] Ordonnance nº 2015-1 341 du 23 octobre 2015 *relative aux dispositions législatives du code des relations entre le public et l'administration* publiée au JORF nº 0248 du 25 octobre 2015 p. 19872.

[1977] Code des relations entre le public et l'administration, Article L.311-14 : « *Toute décision de refus d'accès aux documents administratifs est notifiée au demandeur sous la forme d'une décision écrite motivée comportant l'indication des voies et délais de recours* ».

[1978] Code des relations entre le public et l'administration, Chapitre II : Attributions de la Commission d'accès aux documents administratifs, Article L.342-1 créé par l'Ordonnance nº 2015-1 341 du 23 octobre 2015 *relative aux dispositions législatives du code des relations entre le public et l'administration* publiée au JORF nº 0248 du 25 octobre 2015 p. 19872.

[1979] Source *Rapport d'activité 2016 de la Commission d'accès aux documents administratifs*, accessible à http://www.cada.fr/IMG/pdf/rapport_d_activite_2016.pdf consulté le 28 mars 2018.

saisine est irrecevable ou sans objet, ou la commission s'est déclarée incompétente[1980]. La loi pour une République numérique[1981] a rendu obligatoire la publication des avis de la CADA et de la CNIL consultées sur un projet de loi[1982], un décret ou un arrêté.

La transparence des gouvernements est également régie par des lois dans d'autres États. Ainsi aux États-Unis d'Amérique, le congrès a voté et adopté le *Freedom of Information Act*[1983], ou FOIA, loi signée par le Président Lyndon B. Johnson le 4 juillet 1966. Fondée sur le principe de la liberté d'information, elle oblige les agences fédérales à transmettre leurs documents à quiconque en fait la demande, quelle que soit sa nationalité. Cette loi fut suivie d'autres textes concernant la transparence des gouvernements et comme l'écrit Russell L. Weaver, les efforts pour la transparence ont été facilités par les avances technologiques liées aux télécommunications[1984]. En effet, si en son temps, l'invention de l'imprimerie par Gutenberg avait permis la dispersion de la connaissance et du savoir, le développement d'Internet et des techniques de télécommunication ont transformé les possibilités de transparence des gouvernements ouverts. Ces techniques ont aussi permis aux gouvernements de collecter une masse d'informations concernant les citoyens eux-mêmes et il n'est pas certain que les citoyens disposent de suffisamment d'informations d'origine gouvernementale pour être vraiment en mesure d'exercer leur fonction de supervision des actes et projets gouvernementaux. Les États disposent de la possibilité de classifier certaines informations sensibles concernant la sécurité, la défense du territoire. Les informations ainsi classifiées ne peuvent être rendues publiques avant un délai de cinquante ans, voire plus si elles concernent des personnes toujours vivantes. Dans certains cas, sous la pression des médias, ce délai peut être réduit et le gouvernement peut déclassifier et rendre public certaines informations, partiellement ou en totalité. Ainsi en 2014,

[1980] Aucune répartition de ces cas n'est fournie dans le rapport d'activité 2016 déjà cité, dernier rapport disponible au 28 mars 2018.

[1981] Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, Art. 13 et 59.

[1982] Cette publication obligatoire des avis de la CNIL concernant les projets de loi a été supprimée par l'article 40 de la loi n° 2017-55 du 20 janvier 2017 *portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes.* Concernant la CADA, l'article L.342-4 qui prévoyait cette publication a été remplacé par l'article R.342-4 qui ne prévoit plus cette publication (Décret n° 2015-1342 du 23 octobre 2015 *relatif aux dispositions réglementaires du code des relations entre le public et l'administration* (Décrets en Conseil d'État et en conseil des ministres, décrets en Conseil d'État et décrets)). Il a été rétabli par le Décret n° 2016-1564 du 21 novembre 2016 *relatif aux délégations accordées par la commission d'accès aux documents administratifs à son président* et son article 4 qui a renuméroté l'article R.342-4 en R.342-4-1.

[1983] En français : loi sur la liberté d'information.

[1984] Russell L. Weaver, « Transparency, Privacy, and Democracy in a Digital Era », Bouhadana Irène, Gilles William (sous la direction.), *International Journal of Open Government* [2017 – Vol. 4], pp. 49-63, en ligne à http://ojs.imodev.org/index.php/RIGO.

le Sénat américain a dévoilé une partie du rapport concernant la CIA et la pratique de la torture après les attentats du 11 septembre 2001[1985].

§ 2 - Les révélations des lanceurs d'alerte

Outre les difficultés des administrations à ouvrir leurs données brutes, certaines informations font l'objet de rétention par les États qui ne souhaitent pas que certaines dispositions soient connues d'autres États ou de leurs administrés. Devant l'occultation de certaines données, des révélations peuvent être organisées du fait des lanceurs d'alerte[1986]. La surveillance systématique et mondiale des communications par la NSA a été révélée ainsi par la presse après les révélations de Edward Snowden relatives au programme PRISM[1987], les accords entre le Grand-Duché du Luxembourg et des sociétés internationales permettant une optimisation fiscale ont été révélés lors d'une émission d'information télévisée[1988] ou l'existence de comptes offshore au Panama a été divulguée après un an d'enquêtes journalistiques[1989]. Toutes ces révélations ont été rendues possibles grâce à la numérisation des documents et la copie des fichiers concernés. Le lanceur d'alerte prend des risques en révélant certaines informations, sa protection doit légalement être assurée, mais dans la pratique les lanceurs d'alerte voient leur existence transformée après leur révélation. Une tendance existe pour réduire la protection de ces lanceurs d'alerte au travers du secret d'État, du secret économique ou du secret des affaires.

[1985] *Senate Select Committee on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, Foreword by Senate Select Committee on Intelligence Chairman Bianne Feinstein, *Findings and Conclusions, Executive Summary,* Approved December 13,2012, Updated for Release April 3, 2014, Declassification Revisions December 3,2014, at https://web.archive.org/web/20141209165504/http://www.intelligence.senate.gov/study2014/sscistudy1.pdf, consulté le 8 aout 2017.

[1986] Olivier Leclerc, « Lanceur d'alerte », dans *Dictionnaire critique de l'expertise. Santé, travail, environnement.* Paris, Presses de Sciences Po (P.F.N.S.P.), « Références », 2015, pp. 194-202. URL : https://www.cairn.info/dictionnaire-critique-de-l-expertise--9782724617603-page-194.htm consulté le 17 janvier 2018.

[1987] Cf. Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 1. § 2 -B)2) Les États-Unis d'Amérique et le USA PATRIOT Act.

[1988] Cash investigation, France 2, émission diffusée en 2013 et révélant l'affaire LuxLeaks.

[1989] Panama papers : fuite de plus de 11,5 millions de documents confidentiels issus du cabinet d'avocats panaméen Mossack Fonseca, détaillant des informations sur plus de 214 000 sociétés offshores ainsi que les noms des actionnaires de ces sociétés. Révélations conjointes en France par Cash investigations et Le Monde et plusieurs autres journaux dans le monde, à partir du 3 avril 2016. En 2017, le même consortium d'investigation dévoilait la pratique légale, mais abusive des optimisations fiscales.

A) La protection des lanceurs d'alerte

Les lanceurs d'alerte ont contribué, dans la seconde moitié du XX[e] et le début du XXI[e] siècle, à révéler des informations cachées aux citoyens et à dénoncer des scandales ou abus[1990].

L'alerte et le lanceur d'alerte sont définis dans une recommandation du Conseil de l'Europe[1991]. Le lanceur d'alerte révèle des agissements qui constituent une menace ou un préjudice pour l'ordre public, le lanceur d'alerte ne doit pas tirer un profit personnel de ses révélations[1992]. Le Conseil de l'Europe ajoute : « *L'alerte a pour objet de protéger les principes des droits de l'homme et de l'État de droit qui sous-tendent toute société démocratique* »[1993]. Parmi les recommandations du Conseil de l'Europe, la protection du lanceur d'alerte doit être garantie et il ne doit pas subir de représailles pour ses révélations[1994] et il peut demander à conserver l'anonymat.

En France, la protection des lanceurs d'alerte est prévue au travers de plusieurs lois adoptées entre 2007 et 2014, elle concerne les employés du secteur public et du secteur privé pour la divulgation de faits concernant des risques graves en matière de santé, environnement et corruption[1995]. Plus récemment, le gouvernement a modifié et précisé la définition d'un lanceur

---

[1990] « *Le lanceur d'alerte est une personne qui, dans le contexte de sa relation de travail, signale un fait illégal, illicite et dangereux, touchant à l'intérêt général, aux personnes ou aux instances ayant le pouvoir d'y mettre fin.*
« Les lanceurs d'alerte ont contribué, ces 50 dernières années, à une meilleure information des citoyens et ont permis de prévenir scandales et tragédies, de préserver biens publics comme vies humaines et contribuent de manière plus générale au bon fonctionnement démocratique. Dernier recours lorsque les contrôles sont défaillants, ils jouent un rôle fondamental dans la lutte contre la corruption.
« Pourtant, comme en témoignent de nombreux exemples dans l'actualité, ils restent la cible d'intimidations, de menaces et de représailles : licenciement, procès en diffamation, harcèlement… » (source Transparency International France, à https://transparency-france.org/lanceurs-dalerte/ consulté le 18 aout 2016).

[1991] Recommandation du Conseil de l'Europe CM/Rec (2014) 7 adoptée le 30 avril 2014, disponible à https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec_(2014)_7F.pdf consulté le 20 aout 2016.

[1992] « *L'alerte concerne la révélation d'informations sur des activités qui constituent une menace ou un préjudice pour l'intérêt général. Les personnes lancent une alerte, car elles considèrent qu'il doit être mis fin à ces activités ou que des mesures palliatives doivent être prises. Souvent, il s'agit simplement d'informer les employeurs des agissements irréguliers dont ils ignorent l'existence et qu'ils s'empressent de corriger. Dans d'autres cas, les lanceurs d'alertes peuvent estimer nécessaire de contacter les organes réglementaires ou de contrôle, ou les autorités de répression compétentes. Parfois, les lanceurs d'alerte voudront rendre publics ces actes répréhensibles, le plus souvent par le biais de l'Internet et d'autres médias, ou en contactant des groupes de défense de l'intérêt général ou des parlementaires* ».

[1993] Ibid.

[1994] *« - toute forme de représailles est interdite, dès lors que le lanceur d'alerte a des motifs raisonnables de croire en la véracité des informations ;*
« - les lanceurs d'alertes peuvent prétendre au respect de la confidentialité de leur identité de la part des personnes à qui ils ont fait un signalement, à moins qu'ils n'en décident autrement (sous réserve de garanties d'un procès équitable). » (Extrait de la recommandation CM/Rec (2014)7).

[1995] Loi du 13 novembre 2007 n° 1598 *relative à la lutte contre la corruption* (créant l'article L.1161-1 du Code du travail (CT) ; Loi du 29 décembre 2011 n° 2011-2012 *relative au renforcement de la sécurité du médicament et des produits de santé (loi Bertrand)* (créant l'article L.5312-4-2 du Code de la santé publique (CSP) ; Loi du 16

d'alerte et sa protection via la loi dite Sapin 2[1996]. Le lanceur d'alerte révèle un crime, un délit ou une violation grave d'un accord international. Il doit être désintéressé, c'est-à-dire ne pas attendre de gratification de cette révélation qui ne doit pas contrevenir aux principes du secret défense, médical ni professionnel[1997]. La définition respecte la confidentialité du lanceur d'alerte préconisée par la recommandation du Conseil de l'Europe et prévoit sa protection par le Protecteur des droits. Comme le dit Jean-Marc Sauvé[1998], le lanceur d'alerte n'est ni un dissident ni un partisan de la désobéissance. Le droit doit saisir l'éthique du lanceur d'alerte afin que l'alerte ne reste pas l'apanage d'actes héroïques.

B) Le sort des lanceurs d'alerte

Si depuis quelques années, la sauvegarde et la protection des lanceurs d'alerte sont présentes dans la législation, cette protection est due à la révélation de plusieurs affaires internationales et à la pression de l'opinion publique face à la situation des lanceurs d'alerte. Les premiers lanceurs d'alerte ont dévoilé certains risques concernant la santé, risques connus des industriels, comme le caractère addictif et cancérigène des cigarettes dès les années 1990, ou plus récemment la dangerosité du Médiator[1999], mais depuis les révélations d'Edward Snowden en 2013 et le scandale du programme de surveillance généralisé PRISM, les États ont aussi fait l'objet de révélations au grand public par l'intermédiaire de la presse[2000]. Tous ces lanceurs

---

avril 2013 nº 2013-316 *relative à l'indépendance de l'expertise en matière de santé et d'environnement et à la protection des lanceurs d'alerte (loi Blandin)* (créant l'article L.1351-1 du CSP ; Loi du 11 octobre 2013 n º 2013-907 *relative à la transparence de la vie publique*, article 25 ; Loi du 6 décembre 2013 nº 2013-1 117 *relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière* (créant l'article L.1132-3-3 du CT et l'article 6 ter A (Fonction publique).

[1996] Loi nº 2016-1 691 du 9 décembre 2016 *relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique* publiée au JORF nº0287 du 10 décembre 2016.

[1997] Article 6 de la loi nº 2016-1 691 : « *Un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.*
Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre ».

[1998] Introduction au Colloque organisé par la fondation Sciences Citoyennes et Transparency International, « Lanceurs d'alerte : la sécurisation des canaux et procédures », 4 février 2015.

[1999] Irène Frachon, « Figure du lanceur d'alerte : le cas du Mediator. Entretien », *Hermès, La Revue*, 2015/3 (n° 73), pp. 146-150. URL : https://www.cairn.info/revue-hermes-la-revue-2015-3-page-146.htm consulté le 17 janvier 2018.

[2000] Gildas Le Voguer, « Le "complexe industriel" du renseignement américain et la préservation des libertés », *Politique américaine*, 2014/2 (N° 24), pp. 29-44. URL : https://www.cairn.info/revue-politique-americaine-2014-2-page-29.htm consulté le 17 janvier 2018.

d'alerte sont aujourd'hui poursuivis par les États pour divulgation de secrets d'État ou vol de documents, voire diffamation par les entreprises concernées. Edward Snowden est inculpé le 22 juin 2013 par le gouvernement américain sous les chefs d'accusation d'espionnage, vol et utilisation illégale de biens gouvernementaux, d'abord exilé à Hong-Kong, il a trouvé refuge en Russie. Le gouvernement français a refusé de l'accueillir sur le territoire français[2001].

Plus récemment, le 29 juin 2016, le tribunal d'arrondissement de et à Luxembourg a jugé trois français dans le cadre de l'affaire LuxLeaks[2002]. De grandes sociétés internationales, IKEA, Amazon, Apple, McDonald's, BNP-Paribas et d'autres, ont obtenu du gouvernement du Grand-Duché des accords fiscaux avantageux et secrets permettant une optimisation fiscale importante et en conséquence des pertes de rentrées fiscales dans plusieurs pays membres de l'Union européenne. En 2010, les premiers documents ont été transmis par un employé de PWC, le français Antoine Deltour, qui grâce à une faille de sécurité du système utilisé avait pu copier plus de 28 000 documents révélant 350 accords fiscaux validés par l'administration. Le 11 mai 2012, dans le cadre de l'émission Cash Investigation sur France 2, le journaliste français Édouard Perrin, révèle au grand public certains de ces accords. Le 14 mai 2012, la BBC reprenait ces informations avec un entretien d'Édouard Perrin. D'autres documents seront révélés par un autre employé français de PWC, Raphaël Halet, dont l'identité ne sera révélée que plus tard. PWC s'est constituée partie civile et a porté plainte « du chef de vol, violation du secret professionnel et blanchiment-détention », permettant ainsi la tenue du procès. Les chefs d'accusation retenus contre les prévenus sont : contre « *Antoine Deltour : vol domestique, fraude informatique, violation du secret professionnel, violation du secret des affaires, blanchiment-détention ; [contre] Édouard Perrin : violation du secret professionnel, violation du secret des affaires, blanchiment-détention ; [contre] Raphaël David Halet : vol domestique, fraude informatique, violation du secret professionnel, violation du secret des affaires, blanchiment-détention* »[2003].

[2001] « Pourquoi la France a refusé la demande d'asile de Snowden », 5 juillet 2013, *Le Point,* URL : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/pourquoi-la-france-a-refuse-la-demande-d-asile-de-snowden-05-07-2013-1701076_56.php consulté le 17 janvier 2018.

[2002] La Justice — Grand-Duché de Luxembourg, Jugement dans le cadre de l'affaire dite « LuxLeaks », Audience publique du 29 juin 2016, accessible à http://www.justice.public.lu/fr/actualites/2016/06/jugement-affaireluxleaks/index.html, consulté le 19 aout 2016.

[2003] Extrait du jugement cité ci-dessus.

Le tribunal luxembourgeois reconnaît que les deux anciens employés de PWC sont bien des lanceurs d'alerte[2004], mais qu'il n'y a pas de protection en droit luxembourgeois autres « *que en matière de lutte contre la corruption, le trafic d'influence et la prise illégale d'intérêts* », et qu'au niveau européen, « *tant le Parlement européen que la Commission européenne admettent la nécessité de protéger les lanceurs d'alerte de représailles et notamment de poursuites pénales »* [2005]. Le tribunal luxembourgeois admet le statut de lanceur d'alerte, mais reconnaît que sa protection est très limitée au Luxembourg et que la directive européenne alors en cours de discussion devrait restreindre cette protection[2006], ce qui n'a pas été le cas pour le texte définitif sous la pression des journalistes et de certaines associations[2007]. En conséquence, le tribunal a requis une peine d'emprisonnement avec sursis pour les deux ex-collaborateurs de PWC (respectivement 12 et 9 mois) assortie d'une amende de 1 500 euros et 1 000 euros, et la relaxe pour le journaliste. Mais, le 2 août 2016, le parquet faisait appel de ce jugement. En appel, les peines initiales ont été réduites ; Antoine Deltour est condamné à six mois de prison avec sursis et 1 500 euros d'amende, Raphaël Halet à 1 000 euros d'amende. Ils devront s'acquitter d'un euro symbolique de dommages et intérêts à la firme d'audit PricewaterhouseCoopers (PwC), leur ancien employeur constitué partie civile ; le journaliste français a quant à lui été acquitté. En cassation, la condamnation de Antoine Deltour a été

[2004] « *Pour couper court à toute discussion superflue, le Tribunal correctionnel retiendra comme acquis le fait qu'Antoine DELTOUR et Raphaël HALET sont aujourd'hui à considérer comme des lanceurs d'alerte.*
« Effectivement on ne peut pas sérieusement, en 2016 — après l'éclatement du scandale LUXLEAKS et de ses conséquences mondiales, admettre le contraire.
« Il est encore incontestable que les divulgations d'Antoine DELTOUR et également celles de Raphaël HALET relèvent aujourd'hui de l'intérêt général ayant eu comme conséquence une plus grande transparence et équité fiscale. » (extrait du jugement).
[2005] Extrait du jugement.
[2006] *« Cette volonté de changement entraîne cependant un constat simple : à la date d'aujourd'hui, le lanceur d'alerte n'est pas protégé par une quelconque norme juridique au niveau européen.*
« Au contraire, la nouvelle proposition de directive sur le secret d'affaires adoptée par le Parlement européen entend encore resserrer le cadre de cette protection du lanceur d'alerte et augmenter la protection du secret d'affaires au niveau européen : protection du lanceur uniquement pour l'exercice de la liberté d'expression, révélation d'une faute professionnelle ou d'une activité illégale et divulgation dans le cadre du droit du travail ou aux fins de protection d'un intérêt légitime reconnu » (extrait du jugement).
[2007] Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites,* considérant nº 20 : *« Les mesures, procédures et réparations prévues par la présente directive ne devraient pas entraver les activités des lanceurs d'alertes. La protection des secrets d'affaires ne devrait dès lors pas s'étendre aux cas où la divulgation d'un secret d'affaires sert l'intérêt public dans la mesure où elle permet de révéler une faute, un acte répréhensible ou une activité illégale directement pertinents. Cela ne devrait pas être compris comme empêchant les autorités judiciaires compétentes d'autoriser une dérogation à l'application de mesures, procédures et réparations lorsque le défendeur avait toutes les raisons de croire, de bonne foi, que son comportement satisfaisait aux critères appropriés énoncés dans la présente directive ».*

annulée, mais pas celle de Raphaël Halet[2008]. Lors de l'appel, le chef de violation du secret professionnel et du secret des affaires a été abandonné, mais il est à remarquer que lors de l'appel, la directive européenne a été publiée et qu'elle prévoit des dérogations à la divulgation de secrets des affaires dans certaines conditions correspondant à ces lanceurs d'alerte. Mais, même si la condamnation peut être jugée symbolique, les employés de PWC ont été reconnus coupables et condamnés par les juges luxembourgeois.

C) La protection des sources des journalistes

Dans l'affaire LuxLeaks, le journaliste français, Édouard Perrin, avait soulevé la protection de l'article 10[2009] de la Convention européenne des Droits de l'Homme. Cette protection lui a été refusée, car inopérante par le tribunal. Le 15 décembre 2009, la Cour européenne des droits de l'homme avait statué pour une violation de l'article 10 dans l'affaire *Financial Times LTD* et autres c/ Royaume-Uni et dans ses attendus avait proclamé que « *la protection des sources journalistiques est l'une des pierres angulaires de la liberté de la presse* »[2010] reprenant une formulation de 1996.

Dans l'arrêt Goodwin[2011], la Cour de Strasbourg a énoncé que : « *la protection des sources journalistiques est l'une des pierres angulaires de la liberté de la presse (…). L'absence d'une telle protection pourrait dissuader les sources journalistiques d'aider la presse à informer le public sur des questions d'intérêt général. (…) Eu égard à l'importance que revêt la protection des sources journalistiques pour la liberté de la presse dans une société démocratique et à*

[2008] Jean-Baptiste Chastand, « LuxLeaks : la condamnation d'un des lanceurs d'alerte français annulée en cassation », 11 janvier 2018, *Le Monde.fr,* URL : http://www.lemonde.fr/evasion-fiscale/article/2018/01/11/luxleaks-la-condamnation-d-un-des-lanceurs-d-alerte-francais-annulee-en-cassation-au-luxembourg_5240227_4862750.html consulté le 17 janvier 2018.

[2009] Convention européenne des droits de l'homme, Article 10 : « *1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.*

« 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 ».

[2010] Cour européenne des droits de l'homme, 4e Section, Arrêt du15 décembre 2009, Affaire *Financial Times LTD et autres c/ Royaume-Uni*, Requête no 821/03.

[2011] Cour européenne des droits de l'homme, Arrêt du 27 mars 1996, Affaire *Goodwin c//Royaume-Uni*, Requête no 17488/90.

l'effet négatif sur l'exercice de cette liberté que risque de produire une ordonnance de divulgation, pareille mesure ne saurait se concilier avec l'article 10 de la Convention que si elle se justifie par un impératif prépondérant d'intérêt public ».

En France, en 2010[2012], un article 2 est rétabli dans la loi du 29 juillet 1881 sur la liberté de la presse : « *Art. 2 - Le secret des sources des journalistes est protégé dans l'exercice de leur mission d'information du public. […]* ». Mais la loi de 2010 semble insuffisante et Madame Taubira, ministre de la Justice et garde des Sceaux, a déposé en 2013 un projet de loi pour améliorer cette protection[2013], projet de loi non voté par le Parlement. Dans l'exposé des motifs, on peut y lire : « *À cet égard, il est essentiel que la loi puisse assurer de façon pleine et effective la possibilité pour les journalistes d'exercer sans entrave leur mission fondamentale d'information du public, afin qu'ils soient en mesure de jouer leur rôle de "chiens de garde de la démocratie", pour reprendre une expression utilisée à plusieurs reprises par la Cour européenne des droits de l'homme.*

« C'est tout particulièrement les atteintes illégitimes susceptibles d'être commises par les autorités publiques à l'encontre du secret des sources des journalistes qui doivent ainsi être prohibées et prévenues de la façon la plus explicite et la plus efficace possible », reconnaissant ainsi la faiblesse de la protection des sources journalistiques face aux pressions administratives et économiques.

Au niveau européen, en 2013, un projet de directive[2014] prévoit de préciser l'encadrement de la protection du secret des affaires des entreprises, notamment concernant les innovations en cours de développement et la lutte contre l'espionnage industriel. Mais comme le précise la journaliste Élise Lucet de Cash Investigation, cela implique que *« toute entreprise pourra arbitrairement décider si une information ayant pour elle une valeur économique pourra ou non être divulguée* ». Ce qui mettrait dans l'illégalité un journaliste qui révélerait des informations

[2012] Loi nº 2010-1 du 4 janvier 2010 *relative à la protection du secret des sources des journalistes*, publiée au JORF nº 3 du 5 janvier 2010 p. 272.

[2013] Projet de loi *renforçant la protection du secret des sources des journalistes*, Présenté au nom de M. Jean-Marc Ayrault, Premier ministre, par Mme Christiane Taubira, garde des sceaux, ministre de la justice. Enregistré à la Présidence de l'Assemblée nationale le 12 juin 2013 disponible à http://www.assemblee-nationale.fr/14/projets/pl1127.asp consulté le 22 août 2016.

[2014] Proposition de Directive du Parlement européen et du conseil *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites* du 28 novembre 2013, 2013/0402 (COD) accessible à http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com (2013) 0813_/com_com (2013) 0813_fr.pdf consulté le 23 août 2013.

sensibles[2015]. Le projet de directive a été utilisé dans les attendus du tribunal luxembourgeois pour justifier la condamnation dans l'affaire LuxLeaks, en effet si cette directive était définitivement approuvée en l'état, elle obligerait les États membres à introduire une nouvelle définition du secret des affaires, définition qui rendrait illégale la divulgation des données en provenance de PWC dans l'affaire LuxLeaks, mais aussi celle des divulgations des données dites Panama's papers provenant d'un cabinet d'avocats fiscalistes internationaux. Comme indiqué précédemment, les considérations de la Directive publiée reviennent sur cette position en prévoyant des exceptions[2016]. En France en 2015, un amendement prévu dans le projet de loi Macron[2017] et réglementant ces secrets d'affaires a été retiré sous la pression des journalistes et de nombreuses ONG.

La directive finale a été publiée,[2018] mais elle donne une définition du « secret d'affaire » comme étant des informations répondant aux trois conditions suivantes : « *a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles, b) elles ont une valeur commerciale parce qu'elles sont secrètes, c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes* ». Mais, le texte final de la directive prévoit des dérogations, non présentes dans le projet, aux poursuites de divulgation illicite dans les circonstances suivantes : « *a) pour exercer le droit à la liberté d'expression et d'information établi dans la Charte, y compris le respect de la liberté et du pluralisme des médias ; b) pour révéler une faute, un acte répréhensible ou une activité illégale, à condition que le défendeur ait agi dans le but de protéger l'intérêt public général ; c) la divulgation par des travailleurs à leurs représentants dans le cadre de l'exercice légitime par ces représentants de leur fonction conformément au droit de l'Union ou au droit national, pour autant que cette divulgation ait été nécessaire à cet exercice ; d) aux fins de la protection d'un*

[2015] Les Échos, « Elise Lucet lance une pétition pour protéger le secret des sources », *Les Echos.fr, 5 juin 2016,* http://www.lesechos.fr/monde/europe/021115158322-elise-lucet-lance-une-petition-pour-proteger-le-secret-des-sources-1125655.php?ZF99EWQqwz8Pfeuy.99 consulté le 23 août 2016.
[2016] Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016, considérant nº 20, Op. cit.
[2017] La loi nº 2015-990 du 6 août 2015 *pour la croissance, l'activité et l'égalité des chances économiques*, dite « loi Macron ».
[2018] Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Texte présentant de l'intérêt pour l'EEE)*, publiée au JOUE L157 du 15 juin 2016 p. 1.

intérêt légitime reconnu par le droit de l'Union ou le droit national »[2019]. Les dérogations à la poursuite de la divulgation illicite répondant aux critères retenus pour les lanceurs d'alerte ont donc été réintroduites dans le texte définitif de la directive, directive qui doit être transposée dans la législation des États membres au plus tard le 9 juin 2018.

Malgré l'ouverture des données administratives légalisées dans l'Union européenne, l'équilibre entre révélations d'intérêt général et protection des secrets des affaires reste difficile à trouver, la Commission européenne usant elle-même du secret pour certaines négociations internationales, comme la négociation TAFTA[2020] avec les États-Unis d'Amérique, les États comme le Luxembourg ne souhaitant pas que les autres États membres aient connaissance des accords secrets ayant pour but de détourner des produits fiscaux, et les entreprises refusant de publier certaines études d'impact environnementales de produits phytosanitaires dangereux malgré des demandes pressantes des autorités[2021].

La connaissance par les individus, favorisée par Internet, modifie les relations entre l'État, les administrations et le citoyen. Ce dernier peut participer à la vie locale, voire même à certaines réflexions lors de l'élaboration des lois. Une citoyenneté participative est en gestation.

[2019] Directive (UE) 2016/943, Article 5 – Dérogations.

[2020] *Transatlantic Free Trade Area* (TAFTA).

[2021] Le 4 avril 2016, le commissaire européen Andriukaitis a exigé que soient rendues publiques les études toxicologiques sur lesquelles l'Autorité européenne de sécurité alimentaire (EFSA) a fondé son analyse des risques sanitaires présentés par le glyphosate, le principe actif du désherbant « Roundup ». Information révélée par Le Monde (« Roundup : Bruxelles demande à Monsanto de rendre publique ss études », *Le Monde.fr, 7 avril 2010,* URL : http://www.lemonde.fr/planete/reactions/2016/04/07/roundup-bruxelles-demande-a-monsanto-de-rendre-publiques-ses-etudes_4897456_3244.html, consulté le 12 janvier 2017.
Ces études sont, semble-t-il, toujours tenues secrètes.

Section 2. L'interactivité des citoyens

Dans la Grèce antique, le citoyen participait à la vie politique, votait les lois, pouvait proposer des amendements, cette forme de démocratie directe était possible grâce au faible nombre de citoyens, environ 40 000 citoyens à Athènes pour 340 000 Athéniens, mais seuls 6 000 citoyens environ assistaient à l'assemblée des citoyens, ou ecclésia, tel que le critique Aristophane. L'ecclésia vote les lois, le budget, la paix ou la guerre, l'ostracisme, elle tire au sort les bouleutes (présidents du conseil), les héliastes (membres des tribunaux), les 10 archontes (magistrats qui dirigent la république) et élit les dix stratèges. Cette assemblée votait à main levée ou à bulletin secret les projets de loi de la Boulè que lisait un héraut. L'ecclésia a d'abord siégé sur l'Agora avant d'être transférée sur la colline de la Pnyx sous Périclès (Pnyx signifiant en grec « serré »)[2022].

Cette participation directe des citoyens à la vie de la cité a disparu et est devenue impossible dans nos sociétés démocratiques qui ont délégué cette fonction à des représentants élus sans mandat impératif. Seul un contrôle a posteriori permet de vérifier que les professions de foi des candidats sont respectées après l'élection, la seule sentence restant alors le non-renouvellement du mandat.

Avec les techniques numériques qui permettent à un grand nombre d'individus d'être consultés simultanément, la société numérique autorise le retour à une interactivité des citoyens que ce soit tant au niveau local de la commune qu'au niveau de l'État.

Sous-section 1. La participation des citoyens

Dans le cadre de son adhésion à *l'Open Government Partnership*, le gouvernement français écrit[2023] : « *Consulter, concerter et coproduire l'action publique, grâce à la rénovation des dispositifs participatifs, mais aussi en associant les citoyens à la production de l'action publique. Pour moderniser et dynamiser notre démocratie, créons les conditions d'un échange constant avec les citoyens, les associations et les entreprises, de l'identification des problèmes dans un quartier (engagement 10) à l'élaboration de la loi (engagement 12). Le citoyen devient*

[2022] Claude Mossé, *Les institutions grecques à l'époque classique*, Paris, Armand Colin, 1 967.
[2023] « Introduction », *Pour une action publique et collaborative : Plan d'action national pour la France, 2015-2017*, p. 5.

aussi un acteur de l'évaluation des politiques publiques (engagement 13 et 14). C'est l'intelligence collective au service de l'action publique ! ».

Cet échange entre administration et citoyen peut être réalisé au niveau de la ville, mais le citoyen peut aussi remonter des informations vers les collectivités ou l'État, spontanément par des pétitions, ou lors de consultations ou sondages d'opinion.

§ 1 - Les expériences territoriales

La participation des citoyens au niveau territorial existe déjà dans certaines grandes métropoles : Paris, Lille, ou de départements : Loir-et-Cher, voire de Régions : Ile-de-France. Cette participation peut prendre plusieurs formes : référendum terrirorial, consultation pour avis des électeurs, conseils de quartier, voire gestion de budgets délégués. Cette participation des citoyens est une démarche récente qui a pour but de motiver les citoyens à la vie publique en rapprochant les décisions des citoyens et en développant la liberté d'expression, de critiques et de jugement. Cette participation se nourrit de la mise à disposition des informations, mise à disposition des informations brutes par l'administration au titre des données ouvertes, mise à disposition des commentaires et informations complémentaires par les associations ou les citoyens eux-mêmes. Cette démarche nouvelle nécessite information et formation pour devenir efficace[2024].

L'échange entre individus et services publics doit être biunivoque, si les données ouvertes permettent à l'administration de mettre à disposition des habitants des données, les citoyens doivent pouvoir remonter des informations vers l'administration. Cette remontée d'information dérive des cahiers de doléances de Louis XVI ayant abouti à la Révolution française[2025]. Elle est mise en œuvre localement à travers des plateformes mises à disposition par les municipalités pour remonter des incidents, des dégradations ponctuelles, des besoins d'interventions techniques, etc. L'application Jaidemaville[2026] permet de signaler certaines

[2024] Ank Michels, « Les innovations dans la gouvernance démocratique – En quoi la participation citoyenne contribue-t-elle à l'amélioration de la démocratie ? », *Revue Internationale des Sciences Administratives*, 2011/2 (Vol. 77), pp. 275-296. URL : https://www.cairn.info/revue-internationale-des-sciences-administratives-2011-2-page-275.htm consulté le 17 janvier 2018.

[2025] Jean-Luc Chappey, « Philippe Grateau, *Les Cahiers de doléances, une relecture culturelle,* Rennes, Presses Universitaires de Rennes, 2001, 383 p., 22 € », *Revue d'histoire moderne et contemporaine*, 2005/2 (n°52-2), pp. 213-213. URL : https://www.cairn.info/revue-d-histoire-moderne-et-contemporaine-2005-2-page-213.htm consulté le 17 janvier 2018.

[2026] Disponible sur le site http://jaidemaville.com/ .

dégradations ou pannes locales, les services publics sont alertés et il est possible de suivre la prise en compte du signalement. Cette application est opérationnelle dans plusieurs communes : Bordeaux, Talence, Paris, Lille, Marseille, Bègles, Le Bouscat… L'application Beecitiz[2027] est également utilisée par d'autres municipalités avec ces mêmes fonctions et services. La mairie de Paris a lancé l'application pour smartphones DansMaRue Paris[2028]. Cette application permet de signaler graffitis, objets abandonnés, défaut d'éclairage, malpropreté, dégradation de chaussée, etc., mais il semblerait que le suivi des signalements ne soit pas réalisé dans l'application, mais par envoi d'un message électronique, au contraire de Jaidemaville. Ces applications montrent par ailleurs que ces services parfois expérimentaux souffrent de la multiplicité des applications, par exemple Paris utilise trois applications différentes : Jaidemaville, DansMaRue et Beecitiz pour le même service.

Outre les signalements, des consultations peuvent être organisées pour connaître les souhaits et avis des citoyens. Sur le site « Madame la Maire, j'ai une idée », la mairie de Paris prévoit de recueillir des projets de financement pour des activités de quartier, les Parisiens inscrits sur le site pourront voter les budgets retenus, la mairie de Paris a prévu de consacrer 480 millions d'euros sur l'ensemble de la mandature, soit 5 % du budget d'investissement[2029].

La technique numérique et Internet permettent de mettre en place cette participation citoyenne à la vie de la cité, mais ces initiatives restent cependant confinées faute d'une information générale à tous les citoyens concernés. Ainsi, la plateforme qui recueillait des idées et propositions concernant le statut de Paris, après clôture de la consultation, n'a recueilli que 50 propositions[2030].

La participation des citoyens à la vie locale est possible et souvent souhaitée, mais faute d'information et d'harmonisation, cette participation reste encore marginale. D'autres modes de participation existent et sont parfois à l'initiative des personnes physiques.

[2027] Disponible sur le site http://www.beecitiz.com/.
[2028] Disponible sur le site https://play.google.com/store/apps/details?id=fr.paris.android.signalement pour le système Android ou sur le site https://itunes.apple.com/fr/app/dansmarue/id662045577?mt=8 pour Apple.
[2029] https://idee.paris.fr/co-construisons-paris consulté le 31 août 2016.
[2030] https://idee.paris.fr/les-sujets-du-moment consulté le 31 août 2016.

§ 2 - Les nouveaux modes de participation

Sans évoquer à nouveau les possibilités liées au WEB 2.0 en matière de réaction et de diffusion de l'information par des personnes physiques non professionnelles de l'information, les techniques numériques permettent aux citoyens de réagir en ligne au travers des sondages et des pétitions. Le sondage est passif, la personne répond à un questionnaire préétabli. Il permet de recueillir un avis global. La pétition est active, la personne signe un texte de revendication pour s'opposer ou demander une action à une entité « supérieure ».

A) Les sondages en ligne

Alors que les premiers sondages étaient réalisés par des enquêteurs allant « sur le terrain » interroger les personnes sondées, puis par appels téléphoniques effectués à partir de centres d'appel, les sondages d'opinion sont réalisés en majorité par Internet après envoi d'un message invitant les personnes sélectionnées à accéder au site de collecte des opinions. Cette technique permet d'obtenir des résultats plus rapidement et avec un coût moindre de réalisation pour les instituts de sondage, même si le nombre de sollicitations doit être supérieur au nombre de personnes prévu pour l'échantillon compte tenu des pertes liées aux non-réponses à la sollicitation et à la difficulté de constituer a priori un échantillon représentatif.
La loi du 25 avril 2016[2031] a défini le sondage d'opinion comme étant « *quelle que soit sa dénomination, une enquête statistique visant à donner une indication quantitative, à une date déterminée, des opinions, souhaits, attitudes ou comportements d'une population par l'interrogation d'un échantillon* »[2032]. Ce même article précise : « *Les personnes interrogées sont choisies par l'organisme réalisant le sondage de manière à obtenir un échantillon représentatif de la population concernée* ». Ainsi quel que soit le mode de réalisation d'un sondage d'opinion, l'ensemble des personnes interrogées doit répondre aux critères de représentativité de la population concernée par les résultats du sondage : la population française pour un sondage général, les citoyens électeurs du secteur concerné pour un sondage lié à une élection locale ou nationale, la composition de cet échantillon doit être précisée lors de la

[2031] Loi n° 2016-508 du 25 avril 2016 *de modernisation de diverses règles applicables aux élections*, publiée au JORF n°0098 du 26 avril 2016.
[2032] Article 6 de la loi n° 2016-508 modifiant l'article 1er de la loi n° 77-808 du 19 juillet 1977 *relative à la publication et à la diffusion de certains sondages d'opinion*.

diffusion des résultats. Une commission des sondages est créée par la loi[2033] et chargée de vérifier le respect des contraintes légales concernant la réalisation et la diffusion des sondages. Les sondages ont été utilisés par les entreprises industrielles et commerciales pour tester auprès de consommateurs potentiels ou effectifs l'acceptabilité de nouveaux produits ou services. Ces sondages à usage privé existent toujours et des entreprises comme Carrefour[2034], la FNAC[2035] ou Le Monde[2036], par exemple, disposent d'un panel interrogé régulièrement pour tester leur image par rapport à la concurrence, les retombées d'une campagne marketing, l'acceptabilité d'un futur service, une nouvelle maquette de journal. Ces enquêtes rapides sont exclusivement effectuées par Internet au travers d'une invitation envoyée par courrier électronique aux membres actifs du panel. Mais les sondages les plus connus sont les sondages effectués en période électorale. Ils sont encadrés par la loi et la diffusion des résultats est suspendue quelques jours avant l'élection[2037]. Ces sondages peuvent porter à contestation soit du fait de l'écart des prévisions avec les résultats réels comme ce fut le cas en 2002 lors du premier tour de l'élection présidentielle en France ou de l'élection présidentielle de 2016 aux États-Unis d'Amérique, soit parce qu'ils peuvent être considérés comme des tentatives de modification des résultats en incitant les électeurs « flottants » à porter leurs voix sur un candidat donné. En France, cette manipulation se fonde sur le rachat et la concentration des instituts de sondage par des groupes financiers[2038]. Certains hommes politiques contestent la façon de présenter des résultats qui leur sont défavorables, ainsi que les contrôles effectués par la commission des sondages[2039].

Une autre forme de sondage est utilisée par les sites marchands. Il consiste à demander à un acheteur d'un produit ou à un utilisateur d'un service de donner un avis qualificatif sur l'objet ou le service acheté, comme lors d'une certification qualité ISO 9001. Malheureusement, cet avis peut parfois être faussé par l'utilisation abusive d'« usines à click » qui crée de toute pièce

[2033] Loi nº 77-808 du 19 juillet 1977 *relative à la publication et à la diffusion de certains sondages d'opinion*, publiée au JORF du 20 juillet 1977 p. 3837.
[2034] Le panel Carrefour géré par Harris Interactive.
[2035] Au travers du Lab'Client FNAC.
[2036] Par L'équipe des Enquêtes du groupe Le Monde.
[2037] Loi nº 77-808 déjà citée.
[2038] En 2008, la SOFRES a pour actionnaire les fonds d'investissement américain Fidelity. CSA est contrôlé par Vincent Bolloré également propriétaire du Groupe Havas, d'une télé, de plusieurs quotidiens gratuits. IPSOS est contrôlé par ses deux fondateurs après avoir attiré des financiers comme Pinault ou Fidelity. BVA a pour actionnaires les fonds d'investissement Rotchild et Vincent Bolloré. IFOP a pour propriétaire Laurence Parisot, ancienne présidente du MEDEF. LH2 (ex-Louis Harris) a été vendu par TNS à deux de ses dirigeants. (Source « *A qui appartiennent les instituts de sondages ?* », 20 mars 2008, en ligne à https://www.legrandsoir.info/SONDO-MENSONGES-a-qui-appartiennent-les-instituts-de-sondages.html, consulté le 9 aout 2017).
[2039] Voire à ce sujet Conseil d'État, décision du 8 février 2012, affaire nº353357, *M. Mélenchon*.

des commentaires positifs non liés à un véritable achat. La loi pour une République numérique tente de lutter contre de tels abus au travers des sites de confiance[2040].

Dans un sondage, l'individu est passif, seule sa liberté d'expression est reconnue. Il n'a pas le choix des questions, ni de la formulation des réponses. Il ne choisit pas le sondage auquel il va répondre. Le moteur d'un sondage est l'institut qui organise, choisit les questions et les personnes sondées et analyse les réponses. Il existe une méthode pour remonter une opinion non sollicitée, la pétition.

B) Les pétitions citoyennes

Le droit de pétition est l'un des quelques outils de démocratie participative à disposition des citoyens et de la société civile en France et dans l'Union européenne. La signature de pétitions à l'attention des gouvernants, demandant la modification d'une politique publique, est une tradition d'intervention des citoyens dans la vie publique. En France, les cahiers de doléances de 1789, prévus dans la convocation des États généraux du 24 janvier 1789, avaient pour but d'informer le monarque Louis XVI des conditions de vie des sujets de Sa Majesté, des difficultés du commerce et de la justice et ils devaient permettre de sortir de la crise financière. Les cahiers de doléances qui demandaient la modification des impôts et appelaient à une certaine égalité et à la rédaction d'une Constitution, sont une des premières pétitions citoyennes. La rédaction de ces cahiers de doléance était collective, parfois influencée par le rédacteur[2041].

Le droit de pétition est garanti en France depuis la Révolution de 1789[2042]. Il est garanti par la Constitution de 1958 dans l'article 68, pétition adressée au Conseil économique, social et environnemental, et l'article 72-1, pétition adressée aux assemblées délibérantes des collectivités locales. Il est également prévu un droit de pétition adressée aux assemblées dites « constitutionnelles », c'est-à-dire l'Assemblée nationale et le Sénat[2043]. Au niveau européen,

[2040] Loi n°2016-1 321 du 4 octobre 2016 *pour une République numérique*, Titre II, Chapitre 1er, Section 3 – la loyauté des plateformes et information des consommateurs, articles 49 à 53.

[2041] Walton Charles, « La liberté de la presse selon les cahiers de doléances de 1789 », *Revue d'histoire moderne et contemporaine*, 2006/1 (n° 53-1), pp. 63-87. URL : https://www.cairn.info/revue-d-histoire-moderne-et-contemporaine-2006-1-page-63.htm consulté le 17 janvier 2017.

[2042] Perrine Preuvot, « Le droit de pétition : mutations d'un instrument démocratique », *Jurisdoctoria* n° 4, 2010.

[2043] Ordonnance n° 58-1100 du 17 novembre 1958 *relative au fonctionnement des assemblées parlementaires, Article 4 et, pour l'Assemblée nationale*, par les articles 147 à 151 du Règlement de l'Assemblée nationale et, pour le Sénat, par les articles 87 et suivants du Règlement du Sénat.

un droit de pétition vers le Parlement européen est prévu par le traité de Maastricht de 1992[2044], repris dans l'article 44 de la Charte des droits fondamentaux de l'Union européenne, et il a été étendu vers la Commission par le traité de Lisbonne[2045] avec l'initiative citoyenne.

Les procédures pour déposer une pétition tant au niveau de l'Assemblée nationale[2046] et du Sénat ou du Conseil économique, social et environnemental[2047] qu'au niveau du Parlement européen ou de la Commission européenne restent complexes. Les deux textes régissant les pétitions vers les assemblées constitutionnelles précisent les conditions d'enregistrement et d'examen extrêmement complexes des pétitions. Celles-ci doivent dans un premier temps être adressées au président de l'Assemblée. Pour l'Assemblée nationale, « *les pétitions reçues à la présidence de l'Assemblée nationale et susceptibles d'être enregistrées comme telles sont transmises à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République. Les pétitions jugées recevables sont inscrites sur un rôle général et examinées, en principe une à deux fois par session, par la commission précitée. Sur les conclusions du rapporteur nommé à cette fin et généralement compétent pour l'ensemble des pétitions de la législature, la commission des lois peut prendre trois types de décisions : le classement pur et simple de la pétition, le renvoi de celle-ci à une autre commission*

[2044] Traité sur l'Union européenne (92/C 191/01), Article 8 D – « *Tout citoyen de l'Union a le droit de pétition devant le Parlement européen conformément aux dispositions de l'article 138 D.*
« Tout citoyen de l'Union peut s'adresser au médiateur institué conformément aux dispositions de l'article 138 E » ;
« Article 138 D – « *Tout citoyen de l'Union, ainsi que toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre, a le droit de présenter, à titre individuel ou en association avec d'autres citoyens ou personnes, une pétition au Parlement européen sur un sujet relevant des domaines d'activité de la Communauté et qui le ou la concerne directement* ».

[2045] Article 8B du Traité sur l'Union européenne - « *1. Les institutions donnent, par les voies appropriées, aux citoyens et aux associations représentatives la possibilité de faire connaître et d'échanger publiquement leurs opinions dans tous les domaines d'action de l'Union.*
« 2. Les institutions entretiennent un dialogue ouvert, transparent et régulier avec les associations représentatives et la société civile.
« 3. En vue d'assurer la cohérence et la transparence des actions de l'Union, la Commission européenne procède à de larges consultations des parties concernées.
« 4. Des citoyens de l'Union, au nombre d'un million au moins, ressortissants d'un nombre significatif d'États membres, peuvent prendre l'initiative d'inviter la Commission européenne, dans le cadre de ses attributions, à soumettre une proposition appropriée sur des questions pour lesquelles ces citoyens considèrent qu'un acte juridique de l'Union est nécessaire aux fins de l'application des traités.
« Les procédures et conditions requises pour la présentation d'une telle initiative sont fixées conformément à l'article 21, premier alinéa, du traité sur le fonctionnement de l'Union européenne ».

[2046] Paul-Louis Courier, « Pétition à la Chambre des députés. Pour les villageois que l'on empêche de danser », *Le Télémaque*, 2005/1 (n° 27), pp. 7-10. URL : https://www.cairn.info/revue-le-telemaque-2005-1-page-7.htm consulté le 12 avril 2018.

[2047] Marie de Cazals, « La saisine du Conseil économique, social et environnemental par voie de pétition citoyenne : gage d'une Ve République « plus démocratique » ? », *Revue française de droit constitutionnel*, 2010/2 (n° 82), pp. 289-312. URL : https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2010-2-page-289.htm consulté le 12 avril 2018.

permanente, à un ministre ou au médiateur de la République, la soumission de la pétition à l'Assemblée.

Les examens de pétitions donnent lieu, périodiquement, à la publication d'un feuilleton destiné aux parlementaires, résumant l'objet des requêtes, la décision prise pour chacune d'elles par la commission des lois et, si la pétition a été transmise, la réponse apportée à celle-ci »[2048].

Dans son discours du 3 juillet 2017 devant le Congrès, le Président de la République, M. Emmanuel Macron a annoncé qu'il révisera le droit de pétition afin que « *l'expression directe de nos concitoyens soit mieux prise en compte et que les propositions des Français puissent être présentées à la représentation nationale* »[2049].

Aujourd'hui, des sites Internet[2050] proposent de déposer des pétitions pour obtenir des signatures : Avaaz, SumOfUs, Change.org[2051]. Le site de Avaaz se présente comme « *le mouvement qui permet aux citoyens de peser sur les décisions politiques partout dans le monde* »[2052]. Ces sites connaissent des problèmes de crédibilité faute de pouvoir garantir le nombre de signataires d'une pétition ou de ne pas être le fruit d'une manipulation, certains de ces sites appartenant à des groupes, d'autres comme Avaaz sont des ONG. L'utilisation de l'extension « .org » n'est pas une garantie, Change.org d'origine américaine est une société, une entreprise sociale en droit américain. De plus, le respect de la protection des données personnelles recueillies lors de la signature d'une pétition n'est pas toujours garanti, ces sites sont suspectés de vendre les données personnelles, dont les adresses mail des signataires. Elles monnaient auprès d'associations ou d'ONG faisant appel à leur plateforme pour des pétitions, le coût des signatures (estimé entre 0,50 € et un euro)[2053].

Alors qu'Emmanuel Macron, Président de la République, prévoyait de publier un statut de première dame pour son épouse, face à la création sur Internet d'une pétition s'opposant à ce

[2048] Extrait de « le droit de pétition à l'Assemblée nationale », en ligne à http://www2.assemblee-nationale.fr/decouvrir-l-assemblee/les-petitions, consulté le 10 aout 2017.
[2049] Elena Scappaticci, « Droit de pétition : de quoi parle Emmanuel Macron ? », *le scan politique*, Le Figaro.fr, publié le 03 juillet 2017 à http://www.lefigaro.fr/politique/le-scan/2017/07/03/25001-20170703ARTFIG00278-droit-de-petition-de-quoi-parle-emmanuel-macron.php, consulté le 10 aout 2017.
[2050] Robert Boure, Franck Bousquet, « Enjeux, jeux et usages d'une pétition politique en ligne. « La pétition Vauzelle » », *Réseaux*, 2010/6 (n° 164), pp. 127-159. URL : https://www.cairn.info/revue-reseaux-2010-6-page-127.htm consulté le 12 avril 2018.
[2051] Isabelle Huré, « Change.org, autorités et processus d'autorisation », *Communication & langages*, 2017/2 (n° 192), pp. 83-102. URL : https://www.cairn.info/revue-communication-et-langages1-2017-2-page-83.htm consulté le 12 avril 2018.
[2052] https://www.avaaz.org/page/fr/ consulté le 10 aout 2017.
[2053] Catherine Petillon, « *Pétitions en ligne : le marché des mobilisations* », Pixel du 19 février 2016, sur France Culture, en ligne à https://www.franceculture.fr/emissions/pixel/petitions-en-ligne-le-marche-des-mobilisations, consulté le 10 aout 2017.

statut et recueillant un nombre important de signatures en quelques jours[2054], une simple charte couvrant la période de la mandature a été publiée[2055], le projet de statut a été abandonné[2056]. Mais, alors qu'un référendum départemental avait opté pour la construction d'un aéroport à Notre-Dame-des-Landes, le gouvernement a préféré renoncer à cette construction devant l'agitation d'un groupe d'opposants occupant la zone prévue pour cette construction[2057] et la pression des groupes écologiques.

Dans le cadre de la simplification du droit à pétition, un site gouvernemental officiel, contrôlé et sécurisé, permettrait de développer et sécuriser cette interactivité des citoyens. Un tel site a été utilisé pour une élaboration coopérative de la loi pour une République.

Sous-section 2. L'élaboration coopérative des lois

L'élaboration d'un projet de loi est une opération complexe dont le fonctionnement échappe au citoyen. En 2015, la France a réalisé une expérimentation d'un nouveau mode d'élaboration des lois, impliquant des personnes morales et des personnes physiques, avec la loi pour une République numérique.

§ 1 - La consultation relative à la loi pour une République Numérique

Au niveau national en 2015, l'élaboration de la loi pour une République Numérique a été sujette à une expérience de consultation des citoyens par le biais de l'Internet[2058]. La participation permet aux citoyens de s'exprimer de manière directe. Elle permet aux minorités de s'exprimer et de se faire entendre. Elle renforce l'adhésion des citoyens à l'issue du processus et de la

[2054] « Première dame : la colère gronde contre l'éventuel statut officiel de Brigitte Macron », *SudOuest.fr,* 6 aout 2018, URL : http://www.sudouest.fr/2017/08/06/premiere-dame-la-colere-gronde-contre-l-eventuel-statut-officiel-de-brigitte-macron-3674385-710.php consulté le 28 mars 2018.

[2055] Charte de transparence relative au statut du conjoint du Chef de l'État, 21 août 2017, Site internet de la Présidence de la République, URL : http://www.elysee.fr/communiques-de-presse/article/charte-de-transparence-relative-au-statut-du-conjoint-du-chef-de-l-etat/ consulté le 28 mars 2018.

[2056] « Pas de statut mais une "charte de la transparence" pour Brigitte Macron », *France Inter,* 21 aout 2018, URL : https://www.franceinter.fr/politique/pas-de-statut-mais-une-charte-de-la-transparence-pour-brigitte-macron consulté le 28 mars 2018.

[2057] Renoncement annoncé le 17 janvier 2017 à l'issue du conseil des ministres pat le Premier ministre Edouard Philippe, malgré l'épuisement des possibilités de recours judiciaires et administratifs.

[2058] https://www.republique-numerique.fr/ toujours en ligne le 31 août 2016.

décision[2059]. L'individu devient participant, comme l'avènement du WEB 2.0 lui a donné la possibilité de s'exprimer et de devenir communicant.

Lors de son audition par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, le 15 décembre 2015, Mme Axelle Lemaire, secrétaire d'État chargée du numérique, a déclaré dès le début de son audition : « *Le projet de loi pour une République numérique a fait l'objet d'un long travail préparatoire, selon une méthode originale, et même inédite : il a d'abord, en effet, été alimenté par une consultation publique lancée par le Conseil national du numérique, ce qui a permis à un très grand nombre d'acteurs concernés par ce sujet de s'exprimer. Cette consultation a duré six mois, et des réunions publiques ont été organisées dans plusieurs régions. Le Conseil national du numérique a ensuite rendu un rapport, qui a été à l'origine de la stratégie numérique du Gouvernement. Le projet de loi a ensuite été rédigé puis soumis à l'ensemble de nos concitoyens grâce à une plateforme en ligne, en toute transparence. Cette étape a permis d'apporter au texte des modifications très substantielles - plus de quatre-vingt-dix changements ont été opérés, et cinq articles ont été ajoutés. C'est donc d'une véritable co-construction de la loi qu'il s'est agi. Le texte a été vraiment enrichi. Je forme le vœu que cette méthode soit reprise dans le futur* »[2060].

Du 26 septembre 2015 au 18 octobre 2015, les citoyens français ont pu participer en ligne à l'élaboration de ce texte soumis par la secrétaire d'État, Axelle Lemaire. Une loi portant sur trois grands axes (la sécurité des données ; la neutralité du net et l'ouverture des données ; l'accès à tous au numérique) sur laquelle ils ont pu débattre, voter et proposer des amendements. Concrètement, une fois inscrits, les citoyens pouvaient donner leurs avis, commenter, modifier les articles, proposer un nouvel article, mais également voter pour les propositions des autres. Ils ont ainsi approuvé à une large majorité l'Open Data des organismes publics.

Le projet de loi initial a été amendé par le gouvernement pour tenir compte de certaines propositions issues de la consultation des citoyens et des commentaires des instances légales, Conseil d'État, CNIL, etc. Dans le communiqué de presse du gouvernement, il est précisé : « *Le 26 septembre, il y avait 30 articles. Depuis, 5 autres articles, nés du débat et de l'intelligence*

[2059] Ank Michels, « Les innovations dans la gouvernance démocratique – En quoi la participation citoyenne contribue-t-elle à l'amélioration de la démocratie ? », *Revue Internationale des Sciences Administratives*, 2011/2 (Vol. 77), pp. 275-296. URL : https://www.cairn.info/revue-internationale-des-sciences-administratives-2011-2-page-275.htm.

[2060] Audition disponible à http://www.assemblee-nationale.fr/14/cr-cloi/15-16/c1516026.asp, consultée le 10 aout 2017.

collective s'y sont ajoutés, et d'autres articles ont été scindés ou ajoutés pour porter le texte à 41 articles »[2061].

Le texte a été voté en première lecture par l'Assemblée nationale puis par le Sénat qui a introduit des amendements dont certains ont été repris des propositions formulées lors de la consultation et qui n'avaient pas été reprises par le gouvernement. Un texte commun a été approuvé en commission mixte paritaire, il a été voté en seconde lecture par les deux chambres et promulgué[2062].

§ 2 - Les leçons de la consultation

Sur le site dédié à la consultation, il est indiqué : « *Au total, ce sont 21 330 contributeurs qui ont voté près de 150 000 fois et déposé plus de 8 500 arguments, amendements et propositions de nouveaux articles sur le site republique-numerique.fr* »[2063]. Pour cette expérience nouvelle, la possibilité pour les citoyens français, mais aussi pour tout contributeur potentiel du fait de l'ouverture du site vers des pays autres que la France, de commenter et proposer des amendements avant le dépôt du projet de loi au Parlement, il peut être jugé que 21 330 contributeurs soient un échantillon peu représentatif et peu significatif, mais le site a été visité par 137 725 internautes différents[2064]. Au niveau de la population française, cette participation ne représente qu'un faible échantillon, mais malgré tout, plus qu'un échantillon moyen d'un sondage national qui porte en général sur quelques milliers de personnes, mais personnes ciblées par catégories socioprofessionnelles. Comme pour les expériences locales, un manque d'information peut expliquer ce résultat médiocre, les internautes étant en majorité originaires de l'Ile-de-France, et l'accès à la plateforme a été majoritairement dû aux réseaux sociaux plutôt qu'à un accès via les moteurs de recherche faute d'information large. De plus, pour participer il faut s'intéresser au sujet, il faut comprendre le sujet, il faut avoir le temps d'y participer et enfin, il faut se sentir légitime pour y contribuer, penser que son avis sera pris en compte. De

[2061] Axelle Lemaire, « Edito », *Projet de loi pour une République numérique : 21 330 citoyens ont co-écrit le projet de loi*, disponible en ligne à https://www.republique-numerique.fr/media/default/0001/02/da09b380f543bfab2d13da7424cec264dca669c6.pdf, consulté le 11 aout 2017.

[2062] Loi nº 2016-1 321 du 7 octobre 2016 pour une République numérique, publiée au JORF nº 235 du 8 octobre 2016.

[2063] Source https://www.republique-numerique.fr/, consulté le 11 aout 2017.

[2064] Chiffres donnés sur le site dédié à la préparation de la loi pour une République numérique à https://www.republique-numerique.fr/media/default/0001/02/2377a996950cadd5a093dc9e3a621c0e1f9a19f5.pdf consulté le 31 août 2016.

fait, il faut changer de paradigme politique et remettre la politique entre les mains des citoyens, alors qu'ils s'en éloignent actuellement comme semble l'indiquer la faible participation aux élections présidentielles et législatives de 2017.

Une synthèse a été publiée par le gouvernement[2065], ainsi que des réponses du gouvernement aux propositions citoyennes[2066]. Pour Axelle Lemaire, « *la consultation citoyenne que le gouvernement a voulue reposait sur une idée : celle que le numérique, par la mise en réseau des savoirs, des connaissances, des interprétations, était l'instrument idéal pour parfaire une loi, qui plus une loi pour la République numérique.* […] *Avec ce projet de loi, la République se réinvente par et pour le numérique. Par le numérique, parce que le numérique est un outil pour réinventer la participation politique dans notre pays. Pour le numérique, parce que ce projet de loi, c'est celui d'une République qui donne sa chance à tous et qui mise sur le numérique pour construire la France de demain* »[2067]. La mise en réseau des connaissances et compétences, comme pour l'encyclopédie en ligne Wikipédia, a été voulue et souhaitée pour un essai de participation citoyenne et politique.

Cette élaboration participative d'une loi, rendue possible par la technique numérique et les réseaux sociaux, même si la procédure doit être améliorée pour toucher plus de citoyens, ouvre une modernisation de la vie législative. Mais, elle nécessite une information précise, car elle peut créer un sentiment de frustration puisque dans ce type de consultation, le gouvernement ne s'engage pas à tenir compte de l'ensemble des propositions et remarques. En fait, la même frustration a existé lors de la préparation des ordonnances sur le droit du travail en 2017, car il y a eu concertation, discussion, mais pas négociation, le gouvernement gardant le contrôle sur le contenu final du texte des Ordonnances promulguées. Par ailleurs, le poids des lobbies n'a pas été analysé, mais l'autoroute des lobbies n'est pas à sens unique ; ainsi, la quadrature du net et les défenseurs d'un Internet libre ont eu leur mot à dire. Pour la première fois, il est possible de voir l'action des lobbies et donc de les mettre en évidence. De plus, le texte est passé devant toutes les commissions de contrôle possibles : l'Autorité de la concurrence, la CNIL (Commission nationale de l'informatique et des libertés), le CNUM (Conservatoire numérique des arts et métiers), l'ARCEP (Autorité de régulation des communications électroniques et des

[2065] https://www.republique-numerique.fr/project/projet-de-loi-numerique/synthesis/synthese-1 consultée le 31 aout 2016.
[2066] https://www.republique-numerique.fr/project/projet-de-loi-numerique/step/reponses consulté le 31 août 2016.
[2067] Axelle Lemaire, « Edito », *Projet de loi pour une République numérique : 21 330 citoyens ont co-écrit le projet de loi*, disponible en ligne à https://www.republique-numerique.fr/media/default/0001/02/da09b380f543bfab2d13da7424cec264dca669c6.pdf, déjà cité.

postes), la CADA (Commission d'accès aux documents administratifs) ou le Conseil du numérique après être passé devant le Conseil d'État[2068].

Elle ne peut sans doute pas être utilisée pour toute loi, mais elle marque un changement de paradigme législatif, les citoyens étant consultés sur le projet avant le processus parlementaire. Cette expérience montre la possibilité de consulter les citoyens sur un texte en cours de préparation, ouvrant ainsi une voie pour une participation citoyenne à l'élaboration de certaines lois. Une telle expérience ne peut avoir lieu que si les citoyens disposent de l'information nécessaire et restent libres dans l'expression de leurs remarques.

Si elle ne peut pas être utilisée pour les lois organiques ou les lois de finances pour des raisons évidentes, elle pourrait être utilisée pour les lois régissant la société. Cette démarche est à rapprocher de celle utilisée pour la loi « travail » en 2016 qui n'a été adoptée que grâce à l'utilisation de l'article 49-3 de la Constitution, c'est-à-dire sans vote de l'Assemblée nationale et qui a été l'objet de nombreuses manifestations des syndicats contestant cette loi et en demandant le retrait faute de négociations préalables, ou faute de ne pas avoir vu leurs propositions et oppositions prises en compte.

Le gouvernement d'un État peut ainsi se voir influencé par les techniques numériques tant dans son fonctionnement transparent vers les citoyens que lors de l'élaboration des lois avec une participation active des citoyens. Le « gouvernement du peuple par le peuple et pour le peuple » prend ainsi une véritable signification.

Si la vie privée des citoyens se trouve modifiée par les techniques nouvelles par l'évolution de la frontière entre vie privée et vie publique, la vie des citoyens l'est également par la mise en place d'une réelle interactivité.

[2068] Comme l'écrit Robin Grassi, dans un article daté du 4 janvier 2016 « Loi pour une République numérique : coup de com ou démocratie ? » en ligne à http://radio-londres.fr/2016/01/loi-numerique-com-democratie/, consulté le 11 aout 2017.

Titre 2. La société numérique face au besoin d'harmonisation et d'adaptation permanente et rapide

L'exploitation des données à caractère personnel dans une société fortement numérique crée des risques pour les individus. La protection légale de la vie privée est complexe, car, d'un côté, les méthodes de collecte de ces données sont polymorphes, évolutives et parfois indirectes, et d'un autre côté, les individus eux-mêmes de par leur stratégie personnelle peuvent avoir des attitudes très différentes d'exposition de ces données à caractère personnel. La protection de la vie privée nécessite, au-delà de la régulation de la collecte des données à caractère personnel, de réguler la géolocalisation, la revente des données collectées, le contrôle de leur traitement automatique[2069]. La complexité de la régulation tient également à la dispersion des composants de collecte des données à caractère personnel : terminaux mobiles, tablettes et smartphones, bornes de contrôle, terminaux de paiement ou de retrait d'espèces, objets connectés, etc. Il apparaît difficile de réguler de manière uniforme toutes les situations dans lesquelles les données à caractère personnel sont collectées et traitées. La France, avec la loi informatique et libertés[2070] et la création de la Commission nationale de l'informatique et des libertés, ou CNIL, a opté pour une autorisation préalable ou une déclaration des traitements automatiques selon leurs conséquences sur les libertés individuelles. Avec la création, en 2004[2071], des Correspondants informatique et libertés ou CIL dans les entreprises et les administrations, la régulation a été partiellement déportée au niveau des entreprises si un correspondant informatique et libertés a été désigné et si la CNIL en a été informée[2072]. Le règlement général sur la protection des données de l'Union européenne[2073]qui remplace la directive 95/46/CE et est applicable à partir du 25 mai 2018, a supprimé cette autorisation ou déclaration préalable en obligeant les entreprises à respecter un code de bonne conduite et en augmentant le pouvoir de sanction des organismes de contrôle tels la Commission nationale de l'informatique et des

[2069] Cette régulation est assurée par la loi n°78-17, la directive 95/46/CE et le Règlement général sur la protection des données ainsi que par la Commission nationale de l'informatique et des libertés et par le G29.
[2070] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, publiée au JORF du 7 janvier 1978 p. 227.
[2071] Loi nº 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, article 4 modifiant le chapitre IV Formalités préalables à la mise en œuvre des traitements.
[2072] Extrait du nouvel article 22 de la loi nº78-17 issu de la loi nº2004-801 : « *Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne est envisagé.*
« La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés ».
[2073] 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).*

libertés. Le correspondant informatique et libertés devient le *Data Protection Officer* (DPO), traduit en français par Délégué à la Protection des Données, et sa désignation devient obligataire tant pour le secteur privé que le secteur public[2074]. Avec ce nouveau règlement, l'Union européenne semble rejoindre la régulation des États-Unis d'Amérique et ses règles de bonne conduite auxquelles adhèrent les entreprises sur une base de volontariat sans contrôle effectif du respect de ces règles[2075].

L'Union européenne à côté des règles de bonne conduite, édicte des règles générales de protection de la vie privée, règles qui, si elles ne sont pas respectées, peuvent entraîner des sanctions administratives significatives[2076] et non plus symboliques[2077]. La réglementation mise en place, si elle protège la vie privée des individus, permet et facilite la libre circulation des informations. Il n'en demeure pas moins que certaines sociétés situées dans des territoires non réglementés, ou ayant des règlements moins contraignants pourront continuer à collecter et traiter des données illégalement via Internet faute de pouvoir agir sur ces sociétés pour les pénaliser et obtenir le respect des règles européennes[2078]. Au travers d'une protection accrue de la vie privée, de contrôles effectifs et de sanctions prononcées sur le territoire où la collecte est réalisée, les États doivent lutter contre les abus des sociétés commerciales et mercantiles. De plus, le règlement pour la protection des données personnelles introduit ou étend deux notions protectrices : le consentement et le droit à l'effacement ou droit à l'oubli. Un droit à l'autodétermination informationnelle est ainsi créé au niveau de l'Union. Ce droit découvert par la Cour constitutionnelle allemande dès 1983[2079], introduit dans la loi n°78-17 par la loi

---

[2074] Claire Bernier, « Le RGPD en 4 leçons pour les retardataires », *Sécurité et stratégie*, 2017/4 (28), pp. 85-90. URL : https://www.cairn.info/revue-securite-et-strategie-2017-4-page-85.htm consulté le 14 avril 2018.

[2075] Josef Drexl, « Le commerce électronique et la protection des consommateurs », *Revue internationale de droit économique*, 2002/2 (t. XVI), pp. 405-444. URL : https://www.cairn.info/revue-internationale-de-droit-economique-2002-2-page-405.htm consulté le 18 janvier 2018.

[2076] « […] *amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR 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* ».

[2077] Article 47 de la loi nº 78-17 (dans sa version modifiée par l'article 8 de la loi n°2011-334 du 29 mars 2011 et antérieure à la modification apportée par l'article 65 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique) : « […] *Lors du premier manquement, il ne peut excéder 150 000 euros. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 euros ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros* ».

[2078] L'article 3 paragraphe 3 indique : « *3. Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union, mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public* ». En conséquence, un responsable du traitement établi dans un lieu où le droit d'un État membre ne peut s'appliquer car non reconnu par l'État dont le lieu dépend, semble ne pas être impliqué par le règlement.

[2079] Cour constitutionnelle de Karlsruhe, 15 déc. 1983, *EuGRZ,* 1983, pp. 171 et s.

pour une République numérique[2080] et consacré par le Règlement général sur la protection des données [2081] permet à l'individu de contrôler les données à caractère personnel qu'il permet de voir collecter, traiter et diffuser sur le réseau. Pour Yves Poullet[2082], cette autodétermination informationnelle est la condition d'une véritable démocratie délibérative. Il pose la question : « *peut-on envisager une véritable liberté d'expression si chacun se sait observé dans ses choix et activités ?* » La protection de la vie privée est devenue une condition de survie de nos démocraties. Elle nécessite une véritable reconnaissance de sa priorité et une harmonisation au niveau international face à un marché unique numérique[2083].

[2080] L'article 54 de la loi n° 2016-1321 du 7 octobre 2016 a ajouté à l'article 1er de la loi n° 78-17 du 6 janvier 1978 : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.* »
[2081] 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).*
[2082] Yves Poullet, « La loi des données à caractère personnel :. un enjeu fondamental pour nos sociétés et nos démocraties ? », *LEGICOM*, 2009/1 (N° 42), pp. 47-69. URL : https://www.cairn.info/revue-legicom-2009-1-page-47.htm consulté le 18 janvier 2018.
[2083] Catherine Barreau, « Le marché unique numérique et la régulation des données personnelles », *Annales des Mines - Réalités industrielles*, 2016/3 (Août 2016), pp. 37-41. URL : https://www.cairn.info/revue-realites-industrielles-2016-3-page-37.htm consulté le 13 avril 2018.

Chapitre 1. Vers une sanctuarisation de la vie privée

La protection de la vie privée au travers des données à caractère personnel peut être prévue dans la constitution des États, dans une simple loi ou faire l'objet de jurisprudence nationale ou européenne. En outre, la protection des personnes à l'égard de traitements automatisés de données à caractère personnel est prévue par la Convention nº 108[2084], l'article 8 de la Convention européenne des droits de l'homme, la directive 95-46/CE transposée dans tous les États membres, ainsi que le règlement 2016/679 qui, à partir de mai 2018, abrogera et se substituera à la directive et sera d'application directe dans tous les États membres. Cette protection reste localisée au territoire européen de par la compétence de la Cour européenne des droits de l'homme et du Conseil de l'Europe, ou aux États membres pour la Cour de justice de l'Union européenne.

La vie privée et le traitement des données à caractère personnel sont protégés par plusieurs textes en Europe. L'article 8 de la Convention européenne des droits de l'homme[2085] restreint, dans son second paragraphe, l'ingérence des États dans la limitation de ce droit à une juste proportionnalité entre liberté individuelle et bénéfice d'ordre public. Dès son préambule, la Convention nº 108[2086] reconnaît la nécessité pour les États signataires « *de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples* ». Dans l'article 6 du traité sur l'Union européenne[2087], la valeur juridique de la Charte des droits fondamentaux a la même valeur juridique que les traités, elle devient contraignante au sein de l'Union. L'article 7 de la Charte consacre le droit au respect de la vie privée et familiale[2088] et son article 8 le droit à la protection des données à caractère personnel.

[2084] Conseil de l'Europe, STE nº108, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,* ouverture du traité Strasbourg, 28/01/1981, entrée en vigueur 01/10/1985.

[2085] CEDH, Article 8 : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

[2086] Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 janvier 1981.

[2087] Traité signé le 13 décembre 2007 à Lisbonne par les représentants des 27 États membres, dit traité de Lisbonne.

[2088] Charte des droits fondamentaux de l'Union européenne, art. 7 : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* ».

Malgré ces textes fédérateurs et les décisions de la Cour européenne des droits de l'homme[2089] ou de la Cour de justice de l'Union européenne, il appartient aux États d'élaborer le cadre législatif national de protection de ces principes, en complément du nouveau règlement opposable à l'ensemble des États membres. En effet, il relève de la législation de définir les limites de cette protection face aux contraintes et besoins de la sécurité nationale et de l'intérêt public[2090], en respectant le principe de proportionnalité contrôlé tant par les Cours suprêmes étatiques, le Conseil constitutionnel en France, que par les Cours européennes, la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme.

[2089] Voir Cour européenne des droits de l'homme, Division de la recherche, *Internet : la jurisprudence de la Cour européenne des droits de l'homme »,* Conseil de l'Europe/Cour européenne des Droits de l'Homme, 2011, mise à jour Juin 2015, URL : http://www.echr.coe.int/Documents/Research_report_internet_FRA.pdf consulté le 18 janvier 2018.
Christophe Bigot, « La protection de la vie privée par la Cour européenne des droits de l'homme », *LEGICOM*, 2009/2 (N° 43), pp. 43-49. URL : https://www.cairn.info/revue-legicom-2009-2-page-43.htm consulté le 18 janvier 2018.

[2090] La France a prévu d'adapter la législation française au Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (réglement général sur la protection des données) et de transposer la Directive (UE) 2016/680 relative aux traitements mis en œuvre 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 par modification de la loi n° 78-17. Dans l'avis de la CNIL, cette dernière a regretté que la lecture des dispositions de cette protection soit rendue difficile par l'éclatement de ces dispositions dans plusieurs textes d'origine nationale (la loi n° 78-17 adaptée) et d'origine communautaire (le règlement). (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)).

Section 1. L'exposition de la vie privée dans la société numérique

Sous-section 1. Les données à caractère personnel objets des traitements automatiques

La vie privée des individus se trouve exposée soit du fait d'autrui, soit du fait de la personne elle-même. Comme l'écrit François Rigaux en 1980, « *La vie privée est menacée sur deux fronts : les fichiers gérés par les administrations publiques, surtout s'ils sont interconnectés, confèreront aux autorités de l'État une mémoire prodigieuse des faits et gestes du moindre de leurs administrés ; quant aux fichiers du secteur privé, ils risquent d'accroître un pouvoir économique déjà très concentré dans les grandes entreprises, les dispensateurs du crédit, les fédérations patronales. Ainsi, ne suffit-il plus, comme le faisaient les constitutions libérales, de défendre le citoyen contre l'arbitraire ou l'injustice des organes de la puissance publique. Il faut encore s'armer contre les agents de droit "privé", personnes physiques ou personnes morales, que leur maîtrise de moyens financiers et technologiques considérables met précisément à même de renforcer cette puissance par l'utilisation de la cybernétique* »[2091].
Quelques trente plus tard, l'interconnexion des des fichiers administratifs est devenue une réalité pour lutter contre la fraude, et les données personnelle détenues par les GAFA sont devenues dangereuses pour nos démocraties comme le montre le détournement des données détenues par Facebook et utilisées par Cambridge Analytica durant la campagne électorale nord-américaine de 2017[2092].

§ 1 - Les données gérées par les administrations publiques

L'administration collecte au nom de l'efficacité des contrôles une masse d'informations à caractère personnel et crée par analogie des profils, mais aussi des photographies des individus :

[2091] François Rigaux, "La loi applicable à la protection des individus à 1'égard du traitement automatisé des données à caractère personnel", *Revue critique de droit international privé*, Éditions Sirey, 1980, pp. 444-445, cité par Evelyne Lentzen, « Fichiers nominatifs et vie privée », *Courrier hebdomadaire du CRISP* 1982/3 (nº 948-949), pp. 1-59.
[2092] Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens", March 19, 2018, *The New York Times,* URL: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html consulted April 14, 2018.

état civil, données biométriques, revenus, patrimoine, délits, etc. Ces données sont soit fournies directement par les personnes physiques impliquées lors des recensements, des déclarations d'événements familiaux, mariage, naissance, divorce ou décès, voire dans des déclarations rendues obligatoires et périodiques comme les déclarations de revenus ou les déclarations de dons et les mutations. Certains éléments sont fournis à l'administration par des tiers : revenu salarial pour les employés, revenus mobiliers par les organismes financiers ou bancaires, mais aussi informations obtenues indirectement par des enquêtes de voisinage dans les procédures judiciaires ou les enquêtes administratives liées à la lutte contre le terrorisme. Les nouvelles technologies conduisent à plus d'efficacité dans l'administration, que ce soit l'administration fiscale ou l'administration sociale[2093] et les forces de police et de sécurité.

Les fichiers administratifs ont été à l'origine de la prise de conscience des risques pour les personnes physiques et de la promulgation de la loi informatique et liberté dès 1978[2094]. Les conditions de partage et de collecte des données à caractère personnel ont évolué depuis la promulgation de cette loi. Est ainsi apparue la Déclaration Sociale Nominative (DSN)[2095] qui permet à la Caisse Nationale d'Assurance Vieillesse ou CNAV de collecter auprès des employeurs les données relatives au salaire des employés et de les partager avec les organismes de protection sociale. Cette déclaration sociale nominative a remplacé la Déclaration Automatisée des Données Sociales Unifiée utilisée précédemment par chacun des organismes de protection sociale.

Depuis la loi de finances de 1999[2096], l'administration fiscale peut utiliser le NIRPP pour rapprocher les données fiscales d'une personne physique. Dans un arrêt du 1er octobre 2015[2097], la Cour de justice de l'Union européenne a considéré que l'exigence de traitement loyal de données personnelles oblige une administration à informer préalablement les personnes

[2093] Yann Algan, Maya Bacache-Beauvallet, Anne Perrot, « Administration numérique », *Notes du conseil d'analyse économique*, 2016/7 (n° 34), pp. 1-12. URL : https://www.cairn.info/revue-notes-du-conseil-d-analyse-economique-2016-7-page-1.htm consulté le 18 janvier 2018.

[2094] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, publiée au JORF du 7 janvier 1978 p. 227.

[2095] Créée par l'article 35 de la loi nº 2012-387 du 22 mars 2012 *relative à la simplification du droit et à l'allégement des démarches administratives*, publiée au JORF nº0071 du 23 mars 2012 p. 5226.

[2096] Décret n º 99-1047 du 14 décembre 1999 *pris pour l'application de l'article 107 de la loi de finances pour 1999 (nº 98-1266 du 30 décembre 1998) relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects.*

[2097] Cour de justice de l'Union européenne, 3ème chambre, arrêt du 1er octobre 2015 *Smaranda Bara e.a. c/ Președintele Casei Naționale de Asigurări de Sănătate et autres.*

concernées du transfert de leurs données vers une autre administration afin qu'elle en fasse un traitement.

Dans le cadre de la protection de l'enfance, les échanges de données administratives liées à l'environnement familial et à la protection sociale doivent concilier efficacité et protection de la vie privée des personnes majeures, mais aussi des enfants mineurs[2098]. L'article 16 de la Convention des droits de l'enfance précise : « *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. L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* »[2099]. En France, les textes régissant la protection de l'enfance et la prévention de la délinquance[2100] tentent de concilier le travail administratif de protection de l'enfance et de leur famille à la nécessité de protection de l'ordre public et de la prévention de la délinquance lors de l'échange des informations entre administrations. Le partage des informations concernant un mineur y est réglementé[2101].

Ainsi au niveau administratif, tant au niveau des organismes de protection sociale qu'à ceux impliqués dans la protection de l'enfance et la prévention de la délinquance, le fonctionnement en réseau avec échange des informations y est prévu, autorisé et contrôlé par la législation. Cet échange en réseau peut être international dans le cadre de la lutte contre l'immigration clandestine, le terrorisme ou la grande criminalité[2102].

Parmi les informations collectées par des administrations, il y a lieu de considérer les informations collectées lors des procédures judiciaires, informations souvent accumulées, voire thésaurisées pour servir le cas échéant. Ces informations, souvent biométriques, concernent les empreintes digitales, l'iris des yeux capturé par une caméra, les échantillons d'ADN, etc. Ces

---

[2098] Lise-Marie Schaffhauser, « Constitution de réseaux et protection de la vie privée. Cadre juridique dans le domaine du travail social et avec les familles », *Informations sociales* 2008/3 (nº 147), pp. 82-89.

[2099] *Convention Internationale relative aux Droits de l'Enfant* (1989), traité international adopté par l'Assemblée générale des Nations Unies, le 20 novembre 1989.

[2100] Loi nº 2007-293 du 5 mars 2007 *réformant la protection de l'enfance*, publiée au JORF nº55 du 6 mars 2007 p. 4215.

[2101] *Code de l'action sociale et des familles*, Art. L.226-2-2. – « *Par exception à l'article 226-13 du code pénal, les personnes soumises au secret professionnel qui mettent en œuvre la politique de protection de l'enfance définie à l'article L.112-3 ou qui lui apportent leur concours sont autorisées à partager entre elles des informations à caractère secret afin d'évaluer une situation individuelle, de déterminer et de mettre en œuvre les actions de protection et d'aide dont les mineurs et leur famille peuvent bénéficier. Le partage des informations relatives à une situation individuelle est strictement limité à ce qui est nécessaire à l'accomplissement de la mission de protection de l'enfance. Le père, la mère, toute autre personne exerçant l'autorité parentale, le tuteur, l'enfant en fonction de son âge et de sa maturité sont préalablement informés, selon des modalités adaptées, sauf si cette information est contraire à l'intérêt de l'enfant* ».

[2102] Cf. Partie 1. Titre 2. Chapitre 1. Section 2. Sous-section 3. § 2 - Les échanges d'informations.

informations sont gérées de façon automatique avec un haut degré de sécurité, et elles permettent, associées à des algorithmes de plus en plus performants, de réduire les temps d'investigation et les délais de résolution des affaires. Ces données qui peuvent être échangées entre services de police peuvent faire l'objet d'abus par ces forces de police et se voir opposer des refus d'effacement une fois l'affaire réglée juridiquement. La Cour européenne des droits de l'homme[2103] a ainsi condamné le Royaume-Uni pour avoir refusé l'effacement d'empreintes digitales et d'empreintes ADN d'un mineur et d'un suspect majeur qui avaient été l'un mis hors de cause et l'autre acquitté. Ce refus avait été justifié par le Royaume-Uni sur la base du *Police and Evidence Criminal Act* de 1984, mais dans son considérant nº 125, la cour a estimé la mesure non proportionnée[2104]. La Cour en a déduit que l'article 8 de la convention européenne de sauvegarde des droits de l'homme a été violé. La Cour a également condamné la France pour sa gestion du fichier STIC[2105] et la conservation d'informations après un classement sans suite. Mais, ayant à juger le cas de prises de photographies lors d'une manifestation, la Cour a considéré qu'il n'y avait pas de violation de la convention en cas de prises d'images n'ayant pas fait l'objet d'un traitement[2106] bien que les clichés soient conservés pendant dix ans. Ainsi, la Cour européenne des droits de l'homme considère comme licite et ne contrevenant pas à l'article 8 de la convention la conservation de photos prises sur la voie publique pendant une durée déterminée et ne faisant pas l'objet d'un traitement nominatif ou de reconnaissance faciale.

Les données administratives peuvent aussi être des données relatives : à la santé d'une personne physique, Caisse d'assurance maladie[2107] ; au revenu et patrimoine, centres fiscaux ; au niveau d'études, Éducation nationale ; etc. Toutes ces données font l'objet d'études statistiques

[2103] Cour européenne des droits de l'homme, *Affaire S. et Marper c/ Royaume-Uni*, Requêtes nº 30562/04 et 30 566/04, Arrêt du 8 décembre 2008.

[2104] CEDH, Affaire S. et Marper, considérant nº 125 : « *la Cour estime que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions, mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique* »

[2105] Cour Européenne des Droits de l'Homme, Affaire *Brunet c/ France*, Requête nº 21010/10, Arrêt du 18 septembre 2014.

[2106] Cour Européenne des Droits de l'Homme, *Affaire Friedl c/ Autriche,* Requête nº 15225/89, Arrêt du 25 janvier 1995.

[2107] Emmanuelle Rial-Sebbag, « Chapitre 4. La gouvernance des Big data utilisées en santé, un enjeu national et international », *Journal international de bioéthique et d'éthique des sciences*, 2017/3 (Vol. 28), pp. 39-50. URL : https://www.cairn.info/revue-journal-international-de-bioethique-et-d-ethique-des-sciences-2017-3-page-39.htm consulté le 13 avril 2018.

anonymisées. Entre autre, la Caisse nationale de l'assurance maladie dispose d'une base de données concernant la santé des français sur plusieurs années[2108]. La publication de ces données agrégées peut cependant révéler indirectement des informations personnelles[2109], par exemple, savoir que dans un village, un seul foyer paie l'ISF peut suffire à en déduire l'assujetti[2110].
Si l'administration collecte et traite une masse importante de données à caractère personnel, des sociétés privées peuvent également constituer des bases de données dévoilant des pans de vie personnelle.

§ 2 - Les données gérées par des organismes privés

Certains organismes privés détiennent également des informations personnelles : les banques, au travers des domiciliations bancaires des revenus et des dépenses enregistrées sur les comptes courants ou comptes d'épargne ; les établissements commerciaux, par l'intermédiaire des cartes de fidélité ou des commandes du e-commerce ; les employeurs, etc. Certains de ces établissements doivent aussi de par la loi échanger des informations à caractère personnel avec l'administration : l'employeur avec le fisc ou les organismes de protection sociale ; les banques avec le fisc ou les organismes de lutte contre le blanchiment d'argent (TRACFIN). D'autres informations personnelles transitent sur les réseaux sociaux et dans les messageries électroniques, en principe protégées légalement contre les intrusions par le secret des correspondances, mais utilisées par certains opérateurs comme Google pour cibler des publicités. Toutes ces informations collectées, stockées, analysées permettent de prédire certaines actions individuelles. Elles s'ajoutent aux données collectées par la vidéosurveillance ou l'exposition volontaire ou non des individus sur les réseaux sociaux.
Sur les réseaux sociaux, les utilisateurs y dévoilent des informations multiples et variées sur leur vie privée sans prendre de réelles précautions pour éviter la dispersion de ces informations contenues soit dans leurs propos, soit dans des photos ou des scènes filmées. Ils y dévoilent

[2108] Hélène Caillol, « Ouverture des données de santé : l'expérience de l'Assurance maladie », *Informations sociales*, 2015/5 (n° 191), pp. 60-67. URL : https://www.cairn.info/revue-informations-sociales-2015-5-page-60.htm consulté le 14 avril 2018.
[2109] Éric Pechillon, « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique*, 2015/8 (Volume 91), pp. 645-649. URL : https://www.cairn.info/revue-l-information-psychiatrique-2015-8-page-645.htm consulté le 14 avril 2018.
[2110] Hélène Tanghe, Paul-Olivier Gibert, « L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales*, pp. 79-93. URL : https://www.cairn.info/revue-francaise-des-affaires-sociales-2017-4-page-79.htm consulté le 13 avril 2018.

autant leurs pensées intimes que les événements de leur vie familiale[2111]. Si en principe ces données ne sont partagées que par les « amis », beaucoup d'utilisateurs des réseaux sociaux type Facebook contrôlent mal l'acceptation de ces « amis » et dévoilent sur le net des informations intimes pour être dans la norme de leur cercle de relations réel. Ils recherchent au travers des réseaux sociaux et de leur profil à faire « bonne impression »[2112]. Le caractère imprévisible de cette mise en visibilité de soi et les risques liés au jugement des autres, voire à la stigmatisation, sont liés au mauvais contrôle du public touché ou de son élargissement. Le nombre d'amis sur Facebook est perçu comme un « scoring ». Le niveau de dévoilement de soi semble lié au niveau d'étude scolaire et universitaire des utilisateurs selon l'étude de Sociogeek[2113]. L'exposition de soi est liée au sentiment de pudeur qui crée une obligation d'autocontrôle. La permissivité de la société dans certains domaines entraîne un constat de relâchement de cet autocontrôle. Le règlement général sur la protection des données permet aux utilisateurs de réseaux sociaux de demander la communication des données collectées et enregistrées pour un utilisateur. Dans une émission d'information[2114], un journaliste a obtenu l'ensemble des données collectées le concernant. Outre les données librement fournies, il a constaté que les informations concernant les correspondants de son carnet d'adresse avaient été recopiés. De plus, lors de chaque accès à son compte, Facebook avait enregistré l'heure de l'accès et sa géolocalisation.

Limiter les pratiques d'utilisation des services de l'Internet pour se protéger des intrusions dans sa vie privée ne semble pas envisageable pour certains utilisateurs[2115]. De plus, pour la sphère commerçante, la question de la protection de la vie privée est vécue comme « l'épine dans le pied » qui empêche ou restreint la collecte des données et donc le profilage des clients potentiels[2116].

[2111] Caroline Vallet, « Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs », *Droit et société* 2012/1 (nº 80), pp. 163-188.

[2112] Fabien Granjon, « Du (dé) contrôle de l'exposition de soi sur les sites de réseaux sociaux », *Les Cahiers du numérique* 2014/ (Vol. 10), pp. 19-44.

[2113] Les résultats de cette étude ne sont plus en ligne. Il est possible d'en avoir une synthèse à l'URL [http://www.generationcyb.net/Une-enquete-sur-la-pudeur-dans-les,1662], consultée le 7 septembre 2017.

[2114] Envoyé spécial du 12 avril 2018, sur France 2.

[2115] Bénédicte Rey, « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique 2014*/ (Vol. 10), pp. 9-18.

[2116] Fabrice Rochelandet, « V. Réglementation, corégulation ou laissez-faire : une approche comparative », dans *Économie des données personnelles et de la vie privée.* Paris, La Découverte, « Repères », 2010, pp. 88-114. URL : https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-88.htm consulté le 13 avril 2018.

Le dévoilement de la vie privée sur les réseaux sociaux représente une source d'information accessible et peu coûteuse. De plus, l'utilisation des moteurs de recherche permet de réaliser des recoupements capables de compléter le profil d'un individu, profil qui peut être utilisé pour une embauche, une stigmatisation de l'individu ou autres[2117]. Souvent, les informations « gênantes » ont été mises en ligne pendant l'enfance et l'adolescence, quelque fois par des personnes malveillantes. Concernant les enfants, la publication de photos sur Internet par les parents est considérée comme une pratique à risque par la gendarmerie nationale[2118], permettant d'attirer des internautes mal intentionnés, comme des prédateurs sexuels, mais aussi de perturber les enfants, dont le consentement n'est pas nécessairement demandé avant la publication des clichés.

La loi pour une république numérique[2119] permet au jeune adulte de demander l'effacement de données dévoilées lors de l'enfance. Le Règlement général sur la protection des données [2120] permet cette demande d'effacement dès que l'utilisation des données n'est plus conforme à la raison de la collecte et donc ne correspond plus au consentement, ou quand la législation de l'État l'autorise. Ce droit à l'effacement est difficile à mettre en œuvre pour des raisons techniques liées à la duplication des données sur Internet et pour des raisons économiques, les données à caractère personnel ont une réelle valeur marchande, elles créent de la valeur dans nos sociétés numériques[2121].

Sous-section 2. Les difficultés inhérentes à une protection efficace des données personnelles

Lors de la publication de l'arrêt *Google Spain* de la Cour de justice de l'Union européenne[2122], de nombreux commentaires parlaient de la reconnaissance d'un droit à l'oubli numérique alors

[2117] Cf. l'enrichissement des données des abonnés au téléphone par Pages Jaunes, cité précédemment.
[2118] « *Photos d'enfants sur Facebook. La gendarmerie appelle à la vigilance* », Ouest France, 29 février 2016, à http://www.ouest-france.fr/high-tech/facebook/photos-denfants-sur-facebook-la-gendarmerie-appelle-la-vigilance-4064712, consulté le 8 septembre 2017.
[2119] Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, Article 63.
[2120] 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),* Article 17.
[2121] Fabrice Rochelandet, *Économie des données personnelles et de la vie privée.* Paris, La Découverte, « Repères », 2010.
[2122] Cour de justice de l'Union européenne, Arrêt de la Cour (grande chambre) du 13 mai 2014. Affaire C-121/12, *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*.

que la décision ne concerne que l'effacement des références dans les moteurs de recherche[2123]. Statuant sur l'interprétation et l'application de la directive de 1995[2124] aux moteurs de recherche, la Cour de justice de l'Union européenne a conclu que l'exploitant d'un moteur de recherche est responsable du référencement des données personnelles présentes sur des pages WEB publiées par des tiers et reconnaît, sous certaines conditions, à la personne dont les données personnelles ont été indexées par le moteur de recherche un droit à l'oubli, dont la mise en œuvre entraîne l'effacement des liens hypertextes du moteur de recherche vers ces pages[2125]. Si les liens sont effacés, l'information n'en demeure pas moins présente sur les serveurs disposant de l'information. Cet arrêt de la Cour de justice de l'Union européenne a relancé le débat sur un véritable droit à l'effacement ou droit à l'oubli[2126].

Le droit à l'oubli pour les mineurs a été inscrit dans la législation française par la loi pour une République numérique et au niveau européen ce droit à l'oubli est présent dans le Règlement général sur la protection des données se substituant à la directive 96/45/CE le 25 mai 2018. Cette protection pour les mineurs doit être complétée par une éducation des utilisateurs, les sollicitations des principaux acteurs de l'Internet étant de plus en plus subtiles et associées à des services addictifs et de proximité, refuser de donner ses données revient à se priver de nouveaux services. Le règlement européen fait, malgré tout, reposer la protection des personnes physiques sur le consentement et l'information, notions issues du droit civil des obligations[2127].

§ 1 - La consécration du droit à l'oubli

L'autodétermination informationnelle permet aux personnes physiques de contrôler la collecte des données à caractère personnel, les traitements qui leur seront appliqués, l'exactitude de ces informations. Mais, pour disposer pleinement de ses données, il faut pouvoir les détruire, ce qui

[2123] « La consécration par la CJUE d'un droit de déréférencement par les moteurs de recherche : principe, exceptions et mise en œuvre », *LEGICOM*, 2015/1 (N° 54), pp. 89-105. URL : https://www.cairn.info/revue-legicom-2015-1-page-89.htm consulté le 18 janvier 2018.

[2124] 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*, publiée au Journal officiel nº L 281 du 23/11/1995 pp. 31-50.

[2125] Marion Polidori, « L'arrêt *Google Spain* de la CJUE du 13 mai 2014 et le droit à l'oubli », *Civitas Europa*, 2015/1 (n° 34), pp. 243-266. URL : https://www.cairn.info/revue-civitas-europa-2015-1-page-243.htm consulté le 18 janvier 2018.

[2126] Jean-Paul Jean, « Aspects contemporains et comparés de l'oubli en Europe », *Histoire de la justice*, 2018/1 (n° 28), pp. 123-134. URL : https://www.cairn.info/revue-histoire-de-la-justice-2018-1-page-123.htm consulté le 18 janvier 2018.

[2127] *Code civil* art. 1101-1104, 1113-1122.

implique que les personnes physiques puissent décider d'effacer certaines données[2128]. Ce droit à l'oubli relancé par l'arrêt Google Spain est mis en place progressivement. Après le droit au déréférencement, un droit à l'oubli concernant les mineurs apparaît, ainsi qu'un droit spécifique pour les personnes décédées avant une consécration dans le Règlement général sur la protection des données.

A) Le droit à l'oubli des mineurs

Lors de la discussion au Parlement français de la loi pour une République numérique, le règlement européen sur la protection des données personnelles était en cours de négociations. Ce nouveau règlement permet aux mineurs de disposer d'un droit à l'effacement donc à l'oubli, droit demandé par le défenseur des droits[2129]. La loi nº 2016-1 321 du 7 octobre 2016 [2130] a ajouté dans la loi nº 78-17 du 6 janvier 1978, une obligation pour le responsable d'un traitement d'effacer sur demande de la personne concernée les données à caractère personnel collectées auprès d'une personne mineure au moment de la collecte[2131]. En cas de refus, il revient à la

[2128] Karine Favro, « Introduction », *LEGICOM*, 2016/1 (N° 56), pp. 3-12. URL : https://www.cairn.info/revue-legicom-2016-1-page-3.htm consulté le 18 janvier 2018.
[2129] « Rapport du Défenseur des droits au Comité des droits de l'enfant des Nations unies (27 février 2015) - Présentation et recommandations », *Journal du droit des jeunes*, 2015/5 (n° 345 - 346), pp. 78-85. URL : https://www.cairn.info/revue-journal-du-droit-des-jeunes-2015-5-page-78.htm consulté le 18 janvier 2018.
[2130] Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique* publiée au JORF nº0235 du 8 octobre 2016.
[2131] Loi nº 2016-1 321 du 7 octobre 2016, article 63 - « *La loi nº 78-17 du 6 janvier 1978 précitée est ainsi modifiée :*
« 1º L'article 40 est ainsi modifié :
« a) Au début du premier alinéa, est ajoutée la mention : "I.-" ;
« b) Après le cinquième alinéa, il est inséré un II ainsi rédigé : "II.-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.
"Les deux premiers alinéas du présent II ne s'appliquent pas lorsque le traitement de données à caractère personnel est nécessaire :
"1º Pour exercer le droit à la liberté d'expression et d'information ;
"2º Pour respecter une obligation légale qui requiert le traitement de ces données ou pour exercer une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
"3º Pour des motifs d'intérêt public dans le domaine de la santé publique ;

Commission nationale de l'informatique et des libertés de se prononcer sur la demande dans un délai de trois semaines. Des exceptions sont prévues par la loi : respect d'une obligation légale ou exercice d'une mission de service public, exercice du droit à la liberté d'expression et d'information, motifs de santé publique, archivage dans l'intérêt public ou scientifique, exercices ou défense de droits en justice.

B) Le droit à l'oubli des personnes décédées ou la mort numérique

Une autre forme d'oubli concerne la rémanence des données à caractère personnel après la mort. Le sort des données post-mortem doit être déterminé afin que ces dernières ne soient pas soumises à l'éternité numérique[2132]. La loi pour une République numérique[2133] prévoit que toute

"4° À des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure où le droit mentionné au présent II est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ;
"5° A la constatation, à l'exercice ou à la défense de droits en justice." ;
« c) Les deux derniers alinéas sont supprimés ».

[2132] Nathalie Martial-Braz, « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », Dalloz IP/IT 2016, p. 525.

[2133] Loi n° 2016-1321 du 7 octobre 2016, article 63 : « *2° Après l'article 40, il est inséré un article 40-1 ainsi rédigé :*
« Art. 40-1.-I.-Les droits ouverts à la présente section s'éteignent au décès de leur titulaire. Toutefois, ils peuvent être provisoirement maintenus conformément aux II et III suivants.
« II. Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.
« Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.
« Les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.
« Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.
« Les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés à la présente section. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel.
« Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect de la présente loi.
« La personne peut modifier ou révoquer ses directives à tout moment.
« Les directives mentionnées au premier alinéa du présent II peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés.
« Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite.

personne peut émettre des volontés précisant les dispositions concernant ses données personnelles et leur traitement après son décès. En cas d'absence de directives formulées du vivant du défunt, les héritiers peuvent exercer ces droits. Ainsi, un compte Facebook, LinkedIn ou autre, peut être clos après le décès d'une personne. Avant la promulgation de la loi, ces comptes de personnes décédées restaient à la libre disposition du responsable du traitement qui avait pour seule obligation de les actualiser[2134], les droits attachés aux données personnelles expirant avec le décès de la personne concernée. Depuis quelques années, Facebook, LinkedIn, Gmail ont mis en place des formulaires permettant de signaler le décès d'une personne. Par défaut, le compte concerné n'est pas clos, mais transformé en compte « commémoratif », il appartient aux héritiers de demander la clôture du compte, mais la procédure est parfois complexe et tous ces sites demandent un certificat de décès pour prendre en compte la demande. La loi pour une République numérique, en créant un nouveau droit permet de contrôler les données à caractère personnel après la mort, de façon harmonisée, quel que soit l'opérateur concerné.

Après les mineurs et les morts, le droit à l'oubli pour toutes les personnes physiques est enfin consacré par le Règlement général sur la protection des données.

C) Le droit à l'oubli consacré par le Règlement général sur la protection des données

Le Règlement général sur la protection des données [2135] consacre l'autodétermination informationnelle en plaçant la collecte et le traitement des données personnelles sous le régime du consentement. Pour le Larousse, le consentement est l'acte « de donner son accord à une action, à un projet ». En droit civil français, le consentement peut être vicié par l'erreur, le dol et la violence[2136], ces vices peuvent entraîner une nullité relative du contrat[2137]. L'erreur est une

« III. En l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés à la présente section […] ».

[2134] Loi n° 78-17, extrait de l'article 40 avant promulgation de la loi n° 2016-1321 : « *Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence* ».

[2135] 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).*

[2136] Code civil, Art. 1130.

[2137] Code civil, Art. 1131.

cause de nullité si elle porte sur les qualités essentielles de la prestation[2138]. Le dol consiste à obtenir le consentement de l'autre par des manœuvres ou des mensonges[2139], elle est une cause de nullité alors même qu'elle ne porterait sur le simple motif du contrat[2140]. La violence est reconnue si le consentement a été obtenu sous la pression d'une contrainte[2141]. Après une ère de « renoncement négocié », c'est-à-dire un assujettissement aux forces du marché qui crée et organise des contraintes[2142], la personne physique retrouve la libre disposition de ses données à caractère personnel sans qu'un droit de propriété spécial ne soit créé[2143] au travers du consentement, du droit à la portabilité des données et au droit à l'oubli.

Dans le considérant n° 65 du règlement européen, il est écrit : « *Les personnes concernées devraient avoir le droit de faire rectifier des données à caractère personnel les concernant, et disposer d'un "droit à l'oubli" lorsque la conservation de ces données constitue une violation du présent règlement ou du droit de l'Union ou du droit d'un État membre auquel le responsable du traitement est soumis* ». En particulier, ce droit devrait pouvoir être exercé quand les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées et particulièrement lorsque la personne était mineure lors de la collecte ou qu'elle n'était pas consciente des risques inhérents au traitement. Ce droit à l'effacement ou droit à l'oubli est régi par l'article 17 du règlement.

Cet article prévoit l'obligation de l'effacement par le responsable du traitement sur demande de la personne concernée dans plusieurs cas : les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou qu'elles ont été traitées d'une autre manière ; le consentement au traitement a été retiré ; la personne s'oppose au traitement ; les données ont fait l'objet d'un traitement illicite ; une obligation légale d'effacement existe dans le pays concerné ; les données ont été collectées auprès d'un mineur de 13 ans. De plus, si les données ont été rendues publiques par le responsable du traitement, il doit informer les responsables du traitement qui traitent ces données à caractère personnel de la demande d'effacement de ces données par la personne concernée. Les mêmes exceptions que celles prévues par la loi pour une République numérique sont formulées. Ce règlement n'est opposable aux États qu'à partir

[2138] Code civil, Art. 1133.
[2139] Code civil, Art. 1137.
[2140] Code civil, Art. 1139.
[2141] Code civil, Art. 1140.
[2142] Geneviève Vidal, « Prendre la mesure du renoncement négocié », *Multitudes*, 2017/3 (n° 68), pp. 54-59. URL : https://www.cairn.info/revue-multitudes-2017-3-page-54.htm consulté le 20 janvier 2018.
[2143] Nathalie Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p.253.

du 23 mai 2018, mais il est à remarquer qu'en droit pénal français, il existe plusieurs cas d'effacement légal d'une information relative à une condamnation d'une personne physique ou morale : la réhabilitation pénale et l'amnistie, ils devraient pouvoir justifier une demande d'effacement des référencements aux données enregistrées concernant les condamnations amnistiées. Dans ce cas, la jurisprudence Google Spain peut être appliquée directement. Le cas d'espèce semble plus complexe dans le cas d'une mise en examen ou d'une enquête préliminaire ou judiciaire faisant l'objet d'un non-lieu, car dans ces cas, il y a information du public et donc conflit entre droit de l'information et protection de la vie privée[2144].

Ainsi en 2013, la Cour européenne des droits de l'homme a considéré qu'il n'était pas dans le rôle des autorités judiciaires de réécrire l'histoire en ordonnant d'effacer toute trace des informations publiées de par le passé[2145] pour refuser le retrait d'un article du site d'un journal. En 2014, suite à une question préjudicielle, la Cour de justice de l'Union européenne[2146] a considéré que : « *un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive [95/46/CE] lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé* ». Elle en a déduit que dans ces conditions une personne physique pouvait demander à un moteur de recherche de ne plus faire apparaître ces données dans une recherche sur son nom. Ainsi de ces deux arrêts complémentaires, il ressort qu'une information licite lors de sa publication n'a pas à être effacée, mais que si sa pertinence disparaît avec le temps, il peut être demandé à un moteur de recherche de ne plus la faire remonter lors d'une recherche[2147]. Il semble que ce soit la facilité offerte par les moteurs de recherche d'associer des données lors d'une recherche sur un nom d'une personne physique qui constitue l'atteinte à la vie privée plus que l'information elle-même, information qui peut toujours être obtenue par un autre procédé d'accès, car toujours

[2144] Emmanuel Derieux, « Vie privée et données personnelles – Droit à la protection et « droit à l'oubli » face à la liberté d'expression », *Les Nouveaux Cahiers du Conseil constitutionnel*, 2015/3 (n° 48), pp. 21-33. URL : https://www.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2015-3-page-21.htm consulté le 13 avril 2018.

[2145] Cour européenne des droits de l'homme, *Affaire Węgrzynowski et Smolczewski c/ Pologne*, Requête nº 33846/07, Arrêt du 16 juillet 2013.

[2146] Cour de justice de l'Union européenne, Arrêt de la Cour (grande chambre) du 13 mai 2014 (demande de décision préjudicielle de l'Audiencia Nacional - Espagne), *Google Spain SL, Google Inc. / Agencia de Protección de Datos (AEPD), Mario Costeja González,* Affaire C-131/12.

[2147] Emmanuel Derieux, « Vie privée et données personnelles – Droit à la protection et "droit à l'oubli" face à la liberté d'expression », *Nouveaux Cahiers du Conseil constitutionnel* nº48, 1 juin 2015, p.2.

présente. Si cette information a été publiée sur une version papier d'un journal, elle n'est pas effacée des exemplaires publiés et conservés dans les archives du journal donc toujours accessible lors d'une recherche manuelle.

§ 2 - La pression des acteurs internationaux

La loi pour une République numérique et le Règlement général sur la protection des données de l'Union européenne mettent en exergue la nécessité du consentement explicite de l'utilisateur pour la collecte initiale des données à caractère personnel ainsi que pour leur utilisation complémentaire. Ce consentement doit être libre et éclairé. Ce consentement doit pouvoir être retiré selon une procédure aussi simple que celle utilisée pour son obtention. Si ce consentement a été donné pour un traitement particulier, l'extension du traitement doit faire l'objet d'un nouveau consentement. De plus, la durée de conservation des données ne doit pas dépasser la durée nécessaire au traitement proprement dit. Ces contraintes ont été mises en place pour protéger les données à caractère personnel, et en conséquence la vie privée. Les données à caractère personnel, biens immatériels, ont une valeur économique croissante justifiant les investissements effectués pour leur collecte et leur traitement[2148].

Ces données ont une valeur marchande et sont monnayées sur le marché mondial. Les services proposés aux internautes par Google sont gratuits et, malgré cette gratuité, le chiffre d'affaires de Google est estimé à 74 541 Md $ en 2015, en augmentation de 13,6 % en un an, ses bénéfices étant de 23 425 Md $[2149]. Le chiffre d'affaires et les bénéfices sont en croissance régulière.

[2148] Jean Frayssinet, « La régulation de la protection des données personnelles », *LEGICOM*, 2009/1 (N° 42), pp. 5-9. URL : https://www.cairn.info/revue-legicom-2009-1-page-5.htm consulté le 22 janvier 2018.
[2149] Informations disponibles à https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/ consultés le 27 décembre 2016.

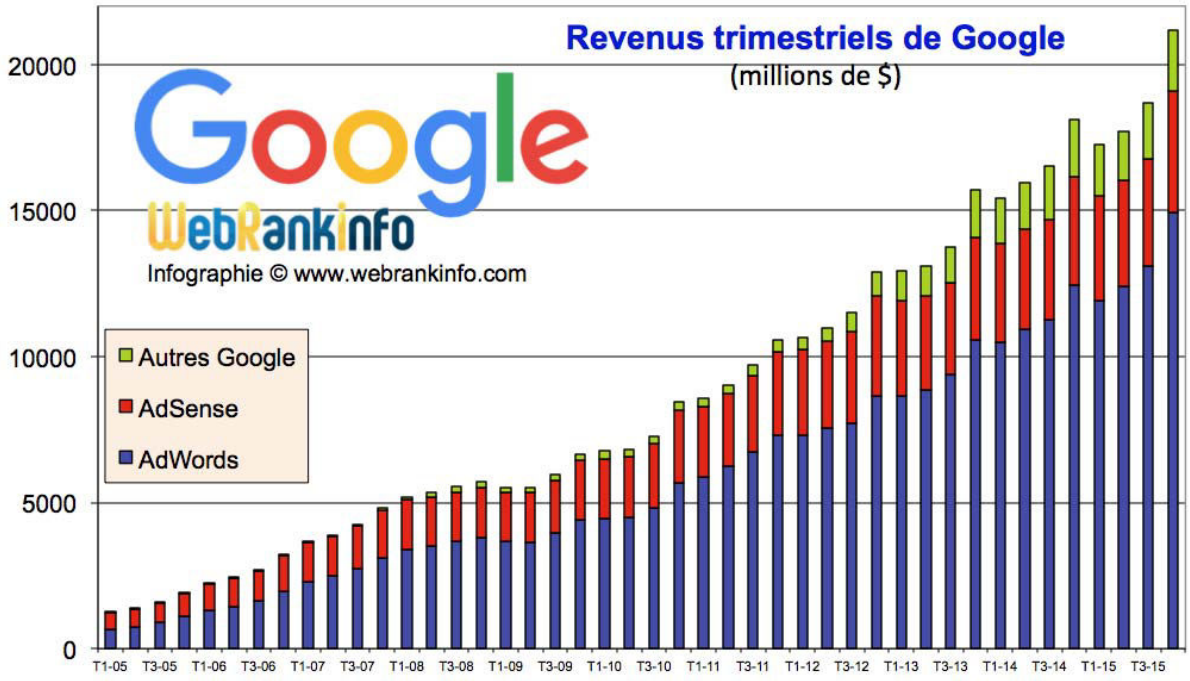


Figure 4 Évolution des revenus trimestriels de Google
(source http://www.webrankinfo.com/dossiers/google/resultats-financiers-t4-2015)

Ces chiffres expliquent les réticences des principaux acteurs du WEB à formaliser cet accord explicite préalable. Un lobbying puissant a permis de retarder l'adoption du règlement européen de plusieurs années, mais aussi d'en assouplir certaines règles en remplaçant la déclaration préalable par des codes de conduite et un mécanisme de certification[2150].

De plus, dans ses considérants, le Règlement général sur la protection des données précise que la libre circulation des données à caractère personnel ne doit pas être entravée par la protection des individus[2151]. Ainsi, les données collectées en France, mais traitées en Irlande, par exemple, ne sont pas soumises aux restrictions de la législation française relatives à la protection des individus, et la législation française ne peut en interdire le transfert vers l'Irlande pour leur traitement[2152]. La Convention n° 108 prévoit également que les flux transfrontaliers des données à caractère personnel ne peuvent pas être interdits du seul fait de leur protection, sauf si ce

[2150] Règlement (UE) 2016/679Section 5, art. 40-43.
[2151] Règlement général sur la protection des données , Considérant nº 13 : « *[…] Pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. […]* » transcrit dans l'article 1er §2 : *« La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* ».
[2152] Au nom de la libre circulation des données au sein de l'Union européenne.

transfert a lieu directement vers un pays non contractant[2153]. Le Royaume-Uni est actuellement contractant de la Convention n° 108 et membre de l'Union européenne, à ce titre le Règlement général sur la protection des données ou la directive 95/46/CE ainsi que la libre circulation des données à caractère personnel sont applicables. Après l'effectivité du Brexit, seule la Convention n° 108 restera effective et l'ensemble de la réglementation de l'Union européenne, y compris la Charte des droits fondamentaux de l'Union européenne, ne lui sera opposable. Les transferts nouveaux vers le territoire du Royaume-Uni ne pourront s'effectuer que si le Royaume-Uni est déclaré adéquat par la Commission, mais quel sera le sort des traitements existant et des données stockées ou transitant actuellement sur le territoire. Il faudra sans doute attendre le résultat des négociations en cours pour le savoir[2154]. Compte-tenu du statut particulier de l'Irlande avec le Royaume-Uni, absence de frontière avec l'Irlande du Nord, après un dumping fiscal incitant les entreprises nord-américaines à s'y installer, l'Irlande sera-t-elle le pays d'évasion des données vers les États-Unis d'Amérique ?

À l'opposé de la décision de la Cour constitutionnelle fédérale de l'Allemagne qui déduit de la protection de la personne physique la protection des données personnelles[2155], la protection des personnes physiques est assurée au travers de la protection des données à caractère personnel garantie par le règlement général de protection des données[2156]. De plus, alors que le considérant n° 15 préconise la neutralité de la protection face aux différentes techniques de traitement, il exclut les données collectées non structurées, c'est-à-dire la masse de données collectées au travers des moteurs de recherche de Google ou autres[2157], données qui peuvent servir au profilage d'un individu par rapprochement d'autres données. En effet, le traitement des données de masse fait appel à des algorithmes non déterministes d'apprentissage

[2153] Convention n° 108, Art.12.

[2154] Hélène Gaudemet-Tallon, Fabienne Jault-Seseke, *Droit international privé*, Recueil Dalloz 2017, p. 1011.

[2155] Yves Poullet, Antoinette Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développeemnt personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *Reinventing Data Protection ?* Octobre 2007, pp. 157-222, URL : http://www.crid.be/pdf/public/6050.pdf consulté le 22 janvier 2018.

[2156] Règlement général sur la protection des données , Article 1er §1 et 2 : « *1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.*
« *2. 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* ».

[2157] Ibid. Considérant no 15 : « *Afin d'éviter de créer un risque grave de contournement, la protection des personnes physiques devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées. Elle 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. Les dossiers ou ensembles de dossiers de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés ne devraient pas relever du champ d'application du présent règlement* ».

automatique permettant d'extraire d'une masse de données les éléments utiles au profilage statistique d'un individu ou groupe d'individus.

De plus, alors que la directive 95/46/CE imposait une notification de tous les traitements automatiques concernés par la protection des données personnelles, le règlement prévoit la suppression de cette obligation et son remplacement par des procédures et des mécanismes ciblant exclusivement les traitements engendrant ou susceptibles d'engendrer un risque élevé pour la protection des données à caractère personnel[2158]. L'évaluation de ces risques au moyen d'une analyse d'impact reste de la responsabilité du responsable du traitement. Le règlement instaure le respect et l'adhésion à des règles de bonne conduite par les entreprises ou les responsables de traitement, donc un contrôle a posteriori en lieu et place d'une déclaration préalable. Le règlement rejoint ainsi les habitudes du monde anglo-saxon et des États-Unis d'Amérique qui avaient basé les règles du « safe harbor » sur de telles déclarations et adhésion, règles jugées insuffisantes par la Cour de justice de l'Union européenne[2159] faute de contrôles de suivi de ces règles après adhésion et de la possibilité pour les autorités des États-Unis d'accéder aux données à caractère personnel transférées pour les besoins de traitement ainsi que l'a révélé Edward Snowden. Avec ce nouveau règlement, une partie des attendus de la Cour ne sont plus d'actualité et la procédure de Safe Harbor aurait été plus difficilement invalidée.

Les pénalités en cas de non-respect des obligations du règlement ont été fortement alourdies par rapport à la législation actuelle[2160], et rendues dissuasives, mais l'autorité judiciaire et l'autorité de contrôle sont celles du lieu du traitement[2161], et non celles du lieu de la personne physique contestant le traitement, rendant ainsi plus complexes les recours et rompant

---

[2158] Ibid. Considérant nº 89 : « *La directive 95/46/CE prévoyait une obligation générale de notifier les traitements de données à caractère personnel aux autorités de contrôle. Or, cette obligation génère une charge administrative et financière, sans pour autant avoir systématiquement contribué à améliorer la protection des données à caractère personnel. Ces obligations générales de notification sans distinction devraient dès lors être supprimées et remplacées 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. […] » transcrit dans l'article 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* ».

[2159] Cour de justice de l'Union européenne, décision du 6 octobre 2015, Affaire C-362/14 *Maximillien Schrems / Data Protection Commisioner.*

[2160] 10 000 000 euros ou 2 % du chiffre d'affaires annuel d'une société (art. 83.4) ou 20 000 000 euros ou 4 % du chiffre d'affaires annuel d'une société (art. 83.5 et 83,6).

[2161] Règlement général sur la protection des données , Art.56.

l'équilibre entre une personne physique et une société multinationale disposant d'une cohorte de juristes.

Ce déséquilibre est aggravé par une absence d'harmonisation des législations. Le Règlement général sur la protection des données se présente comme un socle de protection qui peut être complété par les différents États membres[2162]. Compte-tenu de la libre circulation des données, les dispositions additionnelles ne seront pas reconnues dans un autre État membre, la juridiction compétente étant celle de l'État où a lieu le traitement, le conflit des lois applicables sera évocable par les responsables de traitements. Cette difficulté liée au degré de liberté laissé aux États membres est soulevé par la commission nationale de l'informatique et des libertés dans son avis concernant le projet de loi d'adaptation de la législation nationale au règlement général sur la protection des données[2163].

[2162] Règlement (UE) 2016/679 Article 6 §2 « *2. Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX* ».

[2163] Commission nationale de l'informatique et des libertés, 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).

Section 2. Le besoin d'une harmonisation au niveau européen

En France, la protection des libertés fondamentales est originellement issue de l'application des principes généraux du droit reconnus par le juge administratif[2164] et de l'application des principes fondamentaux reconnus par les lois de la République[2165]. Les sources des libertés fondamentales sont les textes constitutionnels : la Déclaration des droits de l'homme et du citoyen de 1789, le Préambule de la Constitution de 1946, le Préambule de la Constitution de 1958, la Charte de l'environnement depuis son inclusion dans la Constitution en 2005 ; ou des traités : la Convention européenne des droits de l'homme et des libertés fondamentales (CEDH) de 1950, la Charte des droits fondamentaux de l'Union européenne de 2000. En complément à ces textes, la protection des personnes et de la vie privée provient de la loi : l'article 9 du Code civil, la loi nº 78-17 Informatique et libertés ; ou de textes européens : la Convention n° 108 de 1981[2166], de la directive 95/46/CE, du Règlement général sur la protection des données [2167]. Ainsi, si les libertés fondamentales sont protégées directement par des textes de niveau constitutionnel, la vie privée et les données à caractère personnel ne le sont que par la loi ou les traités.

En Allemagne ou en Espagne, pays dont la Constitution a été écrite après une période de dictature, les libertés fondamentales sont inscrites et listées limitativement dans la Constitution. Pour vérifier qu'une liberté ne peut supporter d'atteinte, il suffit de se reporter au texte de la Constitution ou loi fondamentale. Ces deux pays ont une vision déclarative des libertés fondamentales. Pour ces deux pays, il s'agit de montrer une rupture avec un passé dictatorial et un passage vers le respect des libertés.

[2164] Il s'agit de protéger les libertés publiques concédées par l'administration, autorisation de s'exprimer, autorisation d'aller et venir, etc., contre les atteintes portées à ces libertés par les lois ou règlements. Cette protection sera assurée par le Conseil d'État avec les principes généraux du droit, et par le Conseil constitutionnel avec le bloc de constitutionnalité (Louis Favoreu, *Droit des libertés fondamentales*, Précis Dalloz, 2009).

[2165] Selon les États, les droits fondamentaux sont d'essence constitutionnelle ou législative (voire Louis Favoreu, *Droit des libertés fondamentales*, Précis Dalloz, 2009). En France, la liberté de la vie personnelle est protégée par la loi (*Code civil*, article 9), même si le Conseil constitutionnel lui a donné valeur constitutionnelle en la rattachant à la liberté de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 (Conseil constitutionnel, décision nº 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*). La loi française, en général, tend à limiter l'exercice des libertés en encadrant ces libertés par la défense de l'intérêt général.

[2166] Conseil de l'Europe, Traité n° 105, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* du 28 janvier 1981.

[2167] 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).*

Au Royaume-Uni, et particulièrement en Angleterre, l'affirmation des droits fondamentaux a eu lieu très tôt avec l'émergence de la nécessité de limiter le pouvoir du souverain, par et pour la protection des droits et libertés de l'individu, historiquement des seigneurs. Cette limitation a été faite par le renforcement du pouvoir du Parlement et une ébauche de modèle parlementaire qui a impressionné Montesquieu[2168] qui rapportera en France les structures anglaises et la séparation des pouvoirs. Aujourd'hui, la tentation de défendre les libertés par les seuls tribunaux britanniques existe.

Au niveau européen, la protection de la vie privée est prévue dans l'article 8 de la Convention européenne des droits de l'homme, dans la Convention n° 108 qui reconnaît la nécessité pour les États signataires « *de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples* » dès son préambule, dans l'article 7 de la Charte des droits fondamentaux de l'Union européenne qui précise que : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* » et dans le premier alinéa de son article 8 qui ajoute : « *toute personne a droit à la protection des données à caractère personnel le concernant* ».

La directive 95/46/CE énonce les règles de protection des données à caractère personnel pour l'ensemble des États membres, chacun ayant transposé dans son droit interne ces règles, créant ainsi un niveau cohérent de protection. Le 25 mai 2018, le règlement général sur la protection des données est applicable directement dans tous les États membres, garantissant ainsi le même socle de protection des données à caractère personnel dans l'Union européenne.

La protection de la vie privée est prévue dans les législations nationales des États membres, soit au niveau constitutionnel, soit au niveau législatif.

Sous-section 1. La protection dans les pays sortis du fascisme

Quatre pays européens ont connu au cours du XXe siècle des régimes totalitaires restreignant les libertés des individus et même leur sûreté : l'Allemagne avec le nazisme et Hitler, l'Italie avec le fascisme et Mussolini, l'Espagne avec le franquisme du général Franco, et le Portugal avec la dictature de Salazar. Ces pays, lors de l'élaboration de leur nouvelle Constitution, ont

[2168] Montesquieu voit dans les institutions britanniques, l'exemple parfait de la séparation et de l'équilibre des pouvoirs (Livre onzième, « Des lois qui forment la liberté politique dans son rapport avec la constitution ». Chapitre VI « De la Constitution d'Angleterre » pp. 115 & suivantes, in Montesquieu, *De l'Esprit des Lois* (1748) Introduction et notes par J. Erhard. Paris Éditions Sociales 1969).

protégé la liberté de leurs citoyens et leur législation est contraignante en termes de protection de la vie privée.

§ 1 - L'ancrage des droits au respect de la vie privée dans les valeurs fondamentales

L'Allemagne et l'Italie dont les constitutions ont été promulguées au sortir de la Seconde Guerre mondiale protègent par leur constitution les libertés et droits fondamentaux des individus, dont la vie privée. Mais au milieu du XXe siècle, l'informatique n'existant pas, la protection des données à caractère personnel est du ressort de la loi. L'Espagne et le Portugal, sortis des régimes fascistes après l'apparition de l'informatique, ont intégré la protection des individus face à l'informatique dans leur constitution et prévu que la loi prendrait en charge cette protection.

A) Dans les pays sortis du fascisme à la fin de la Seconde Guerre Mondiale

En Allemagne, l'article 13 de la constitution[2169] énonce l'inviolabilité du domicile et les principales libertés, mais compte tenu de la date d'élaboration de cette loi fondamentale, la loi définit et régit la protection des données personnelles[2170]. Le droit allemand régit notamment « la collecte, le traitement et l'exploitation des données personnelles ». L'idée sous-jacente est que les fournisseurs n'ont pas le droit de collecter plus de données que nécessaire pour l'objectif poursuivi, à moins que la personne concernée ne les y autorise et que cela n'aille à l'encontre d'aucune autre disposition sur la protection des données[2171]. La Cour suprême allemande en a déduit le droit de l'autodétermination informationnelle[2172].

[2169] *Grundgesetz für die Bundesrepublik Deutschland*, ou en français Loi fondamentale pour la République fédérale d'Allemagne, du 8 mai 1949, parfois appelée Constitution de Bonn ou *Bonner Grundgesetz*.
[2170] *Bundesdatenschutzgesetz (BDSG, in der Fassung vom 14. August 2009)* – traduction : Loi fédérale allemande sur la protection des données (telle que modifiée jusqu'à la loi du 14 août 2009).
[2171] Cette protection est à rapprocher de la protection prévue par le Règlement général sur la protection des données, art. 25 : « […] *seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, 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* ».
[2172] En allemand : *Recht auf informationelle Selbstbestimmung.*

En décembre 1983, suite aux recours introduits par plusieurs associations, la Cour constitutionnelle fédérale allemande[2173] affirme[2174] l'inconstitutionnalité de certaines dispositions de la Loi sur le Recensement[2175] adoptée à l'unanimité par le Parlement fédéral allemand. La décision repose sur l'article 1er relatif à la dignité humaine et l'article 2 relatif au droit de la personnalité de la Constitution fédérale. Pour la Cour, la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel. Dans cette décision, la Cour a affirmé le droit à l'autodétermination informationnelle caractérisée par le pouvoir de l'individu de décider lui-même, sur la base du concept d'autodétermination, quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui[2176].

Alors qu'aux États-Unis d'Amérique, pour décider de l'existence d'un droit à la protection de la vie privée contre l'intrusion gouvernementale, la Cour suprême utilise le critère sociologique de l'existence d'attentes légitimes du public[2177] à ce que tel pan de l'existence humaine soit exempt de la surveillance ou de l'intrusion étatique[2178], la Cour allemande a opté pour un principe normatif, selon une méthode spécifiquement européenne qui consiste à mettre en balance des intérêts concurrents et à établir dans chaque situation où le droit au respect de la vie privée est impliqué, s'il existe des raisons légitimes et suffisamment importantes pour permettre des atteintes à ce droit. L'article 8 §2 de la Convention européenne des droits de l'homme prévoit cette évaluation « normative »[2179], évaluation systématiquement utilisée par le Conseil constitutionnel français.

[2173] En allemand : *Bundesverfassungsgerichsthof*.

[2174] *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*.

[2175] En allemand : *Volkszählungsurteil*.

[2176] Yves Poullet, Antoinette Rouvroy, *Une réévaluation de l'importance de la vie privée pour le démocratie*, actes de la conférence « Reinventing Data Protection ? », Bruxelles, octobre 2007 disponible à http://www.crid.be/pdf/public/6050.pdf, consulté le 27 décembre 2016.

[2177] *Legitimate expectation of privacy*.

[2178] Cette notion a été introduite par le juge Harlan dans son opinion divergente dans l'affaire Katz v. United States (US Supreme Court, 389 U.S. 347 (1967).

[2179] Convention européenne des droits de l'homme, Article 8 – « *Droit au respect de la vie privée et familiale*
« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
« 2. 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 ».

Dans ses attendus, la Cour allemande protège « l'autodétermination informationnelle » face aux possibilités pour les traitements de collecter automatiquement et massivement des données, de les rapprocher d'autres données permettant de constituer un profil de la personnalité d'un individu sans que ce dernier ne dispose des moyens de contrôler l'exactitude du profil ainsi constitué ou de l'utilisation qui en est faite. Pour la Cour, le standard applicable est le droit de tout individu de développer librement sa personnalité, le droit de la personnalité étant protégé par les articles 2 et 1 de la Loi fondamentale[2180]. La protection des données personnelles découle de la mise en œuvre de ces principes, sans référence dans le raisonnement de la Cour à la loi existante sur la protection des données.

Cette libre disposition des données personnelles est reprise dans l'article 54 de la loi pour une République numérique[2181] qui complète l'article 1er de la loi nº 78-17[2182] par l'alinéa suivant : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ». Ce principe d'autodétermination est repris par le Conseil d'État dans son étude 2014[2183], comme étant « de nature à renouveler le sens de la protection des données à caractère personnel ». Le Conseil d'État en dresse plusieurs avantages : le principe permet à l'individu de rester libre de conduire son existence ; il affirme la primauté de la personne qui doit être en mesure d'exercer sa liberté, il permet de prendre la mesure des enjeux pour les libertés publiques dans la protection des données personnelles et enfin, le droit à « l'autodétermination informationnelle » apparaît d'une grande ambition au regard de la perte générale de maîtrise par les individus de leurs données. Le Conseil d'État en fait d'ailleurs l'objet de sa première proposition dans cette étude : « *Concevoir le droit à la protection des données personnelles comme un droit à "l'autodétermination informationnelle" […]* ». Le Règlement général sur la protection des données a repris sans le nommer ce concept avec le consentement et le droit à l'effacement.

En conséquence, les fournisseurs de stockage en « cloud » doivent être en mesure de rendre des comptes à leurs clients à tout moment sur les données qu'ils ont enregistrées sur eux, et pouvoir

---

[2180] « *Article 1er. La dignité de l'Homme est inviolable. Tout État et toute autorité a pour tâche de la respecter et de la protéger.*
« Article 2. Tout individu a droit au libre développement de sa personnalité pour autant qu'il ne viole pas les droits d'autrui ou l'ordre constitutionnel ou l'ordre moral ».

[2181] Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, publiée au JORF nº0235 du 8 octobre 2016.

[2182] Cet article était le seul article non modifié par la loi nº 2004-801 du 6 août 2004 qui avait transposé la directive 95/46/CE en droit français.

[2183] Conseil d'État, *Le numérique et les droits fondamentaux*, Les rapports du Conseil d'État, 2014, pages 264 et suivantes.

corriger ou effacer ces données à leur demande. Si des données personnelles sont traitées d'une quelconque façon par un fournisseur tiers, elles doivent être protégées, notamment contre tout accès non autorisé. De plus, des lois locales peuvent s'appliquer dans les Länder, les autorités de protection de la vie privée de Hambourg ont ainsi envoyé une injonction à Google en expliquant que le géant californien était en violation de deux lois locales : la première portant sur les médias de télécommunications et la seconde sur la protection des données[2184]. Ainsi, bien que la protection des données à caractère personnel ne soit pas explicitement inscrite dans la Constitution de 1949, la Cour constitutionnelle en a déduit le principe de l'autodétermination informationnelle pour les personnes physiques et placé cette protection au niveau constitutionnel.

En Italie, l'inviolabilité du domicile et le secret de la correspondance sont également protégés par les articles 14 et 15 de la Constitution de 1947[2185], mais la protection des données personnelles ne fit l'objet d'une loi qu'en 1996[2186] pour transposer la directive 95/46/CE en droit italien. La protection des données personnelles et de la vie privée est, actuellement, régie par un décret législatif de 2003[2187] intitulé « Code en matière de protection des données personnelles »[2188]. Son article 13 prévoit le droit de demander, à tout moment, l'accès, la suppression, la modification ou la mise à jour des données personnelles. Cette protection n'est pas rattachée à la Constitution

B) Dans les pays sortis tardivement des dictatures

En Espagne, la Constitution date de 1978[2189], outre l'inviolabilité du domicile et le secret des communications postales, télégraphiques et téléphoniques, son article 18 garantit à chacun le droit à l'honneur, à l'intimité personnelle et familiale et à sa propre image. Ce même article

[2184] Guillaume Belfiore, « *Vie privée : l'Allemagne relance son offensive contre Google* », 1er octobre 2014, à http://www.clubic.com/pro/entreprises/google/actualite-730451-vie-privee-allemagne-relance-offensive-google.html consultée le 7 octobre 2016.

[2185] *Costituzione della Repubblica Italiana* ou Constitution de la République italienne promulguée le 22 décembre 1947.

[2186] Loi 675 du 31 décembre 1996 *portant protection des personnes et des organismes publics et privés à l'égard du traitement de données à caractère personnel*.

[2187] D.Lgs 196/2003 (Privacy), ou en français : Décret législatif italien 196/03 sur la confidentialité.

[2188] Giovanni Buttarelli, « Présentation du système italien de protection des données » in Vincent Téchené, *Compte-rendu de la réunion du 24 avril 2013 de la Commission internationale Italie du barreau de Paris,* Grande Bibliothèque du Droit, URL : http://www.lagbd.org/index.php/Futur_de_la_r%C3%A9glementation_des_donn%C3%A9es_personnelles_en_Europe_-_France_Italie_(fr)_(it) consulté le 23 janvier 2018.

[2189] *Constitución española* publiée au Journal officiel le 29 décembre 1978.

prévoit la limitation par la loi de l'usage de l'informatique pour préserver l'honneur et l'intimité personnelle et familiale des citoyens et le plein exercice de leurs droits[2190].

Dans son préambule, la Constitution portugaise[2191] de 1978 énonce : « *L'Assemblée constituante proclame la décision du peuple portugais de défendre l'indépendance nationale, de garantir les droits fondamentaux des citoyens, d'établir les principes de base de la démocratie, d'assurer la primauté de l'État de droit démocratique […]* »[2192]. Son article 34 énonce l'inviolabilité du domicile et de la correspondance. Mais son article 26 protège l'individu, sa réputation, son image et garantit[2193] la protection de la vie privée. De plus, son article 35[2194] prévoit, par la loi, l'utilisation de l'informatique, la protection des données à

2190 "*Artículo 18*
"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
"2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
"3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
"4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."
Soit en français (traduction du Tribunal Constitutionnel d'Espagne) :
Article 18.
1. Le droit à l'honneur, à l'intimité personnelle et familiale et à sa propre image est garanti à chacun. 2. Le domicile est inviolable. On ne pourra y entrer ou le perquisitionner sans le consentement de celui qui y habite ou sans une décision judiciaire, hormis en cas de flagrant délit.
3. Le secret des communications et, en particulier, des communications postales, télégraphiques et téléphoniques est garanti, sauf décision judiciaire.
4. La loi limitera l'usage de l'informatique pour garantir l'honneur et l'intimité personnelle et familiale des citoyens et le plein exercice de leurs droits.

2191 Constituição da República Portuguesa.

2192 *A Assembleia Constituinte afirma a decisão do povo português de defender a independência nacional, de garantir os direitos fundamentais dos cidadãos, de estabelecer os princípios basilares da democracia, de assegurar o primado do Estado de Direito democrático […]*

2193 "*Artigo 26.º (Outros direitos pessoais)*
"1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação.
"2. A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias. […] »
Soit en français :
Article 26
Autres droits de la personne
1. À chacun est reconnu le droit à l'identité personnelle, au développement de la personnalité, à la capacité civile, à la citoyenneté, au respect et à la réputation, à l'image, à la parole et à la protection de l'intimité de la vie privée et familiale, et à la protection légale contre toute forme de discrimination.
2. La loi établira des garanties effectives contre l'obtention et l'utilisation abusives ou contraires à la dignité humaine de toute information relative aux personnes et aux familles.

2194 "*Artigo 35.º (Utilização da informática)*
"1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
"2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.

caractère personnel, la restriction de l'accès à ces données et le refus de l'attribution d'un numéro national individuel tel que le NIR français[2195]. La transposition de la directive 95/46/CE a nécessité une révision constitutionnelle[2196].

Ainsi, ces deux pays sortis d'une dictature après l'apparition de l'informatique ont introduit la protection des personnes physiques face aux dangers de l'informatique dans leur Constitution. Au Royaume-Uni cette protection est issue de la tradition.

§ 2 - La protection sociétale anglo-saxonne

L'Angleterre n'a pas de constitution écrite, mais sa tradition protège les Anglais contre les abus du pouvoir par des chartes concédées par les souverains lors de leur avènement. Les principaux textes protégeant les libertés fondamentales sont : La *Magna Carta* de 1 215 qui affirme

"3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
"4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
"5. É proibida a atribuição de um número nacional único aos cidadãos.
"6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
"7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."
Soit en français :
Article 35 Utilisation de l'informatique
1. Tous les citoyens ont le droit d'avoir accès aux données informatisées les concernant. Ils peuvent exiger leur rectification et leur mise à jour et d'être informés de l'utilisation qui en sera faite, conformément à la loi.
2. La loi définit le concept de données personnelles, ainsi que les conditions applicables à leur traitement automatisé, leur accès, leur transmission et leur utilisation. Elle en assure la protection, notamment par le biais d'une autorité administrative indépendante.
3. L'informatique ne peut pas être utilisée pour le traitement de données concernant les convictions philosophiques ou politiques, l'affiliation à un parti ou à un syndicat, la foi religieuse, la vie privée et l'origine ethnique. Il est fait exception à ce principe lorsque les données sont traitées avec le consentement exprès de la personne concernée, dans les conditions prévues par la loi et garantissant la non-discrimination ou lorsqu'il s'agit de données recueillies à des fins statistiques qui ne permettront pas d'identifier les personnes auprès desquelles elles ont été obtenues.
4. L'accès de tiers à des données informatisées contenant des renseignements personnels est interdit, sauf dans les cas exceptionnels prévus par la loi.
5. Il est interdit d'attribuer aux citoyens un numéro national unique.
6. Tout citoyen a le droit d'avoir librement accès aux réseaux informatiques à usage public. La loi définit le régime applicable à la circulation transfrontalière de données et établit les formes appropriées de la protection des données personnelles et de certaines autres dont la sauvegarde se justifie pour des raisons d'intérêt national.
7. Les données personnelles inscrites sur fichiers non informatiques jouissent de la même protection que celle attribuée aux fichiers informatiques, et prévue aux paragraphes précédents, conformément à la loi.

[2195] Communément appelé numéro de sécurité sociale.
[2196] Rapporté dans Note de synthèse du Sénat in *La protection des données personnelles,* Octobre 1999, en ligne à l'URL : https://www.senat.fr/lc/lc62/lc620.html consultée le 23 janvier 2018.

différents droits et principes de règne ; *l'Habeas Corpus* de 1679 qui pose les bases des garanties individuelles, prises dans le sens de la sûreté ; le *Bill of Rights* de 1689 qui souligne le caractère primordial de la supériorité des droits essentiels sur le pouvoir normatif du Roi et l'Acte d'*Establishment* de 1701 qui réaffirme le devoir de respect des droits et libertés par la Couronne et le Parlement.

Il n'y existe pas un droit de la vie privée tel qu'il en existe en France ou dans d'autres États membres de l'Union européenne. Cette protection peut être assurée par d'autres moyens : actions ou plaintes devant les juges civils ou devant une commission d'autorégulation, la « *Press Complaints Commission* (PCC) », créée en début 1991[2197] et remplacée en septembre 2014 par l'*Independent Press Standards Organisation* ou IPSO. L'imprécision du concept de « *privacy* » laisse une marge d'appréciation aux juges et leur donne un pouvoir discrétionnaire large pouvant conduire à des risques d'abus. Comme aux États-Unis d'Amérique, cette protection est sociologique et non normative. En effet, en 1979, la Chambre des Lords[2198], Cour suprême du Royaume-Uni, rejette les arguments des requérants qui contestaient la légalité d'écoutes téléphoniques policières sans autorisation judiciaire, au motif qu'il n'existait pas de droit au respect de la vie privée au Royaume-Uni, que la Convention européenne n'avait pas d'effet direct en droit interne et que le devoir de confidentialité pouvait être levé pour des motifs d'intérêt général. La Cour européenne des droits de l'homme a remis en cause cette décision[2199] en jugeant qu'il y avait bien eu une violation au droit de la vie privée. C'est donc bien sous l'influence des conventions internationales que le droit au respect de la vie privée est, aujourd'hui, protégé au Royaume-Uni.

En France, la vie privée ne connaît une protection légale que depuis 1970 avec l'article 9 du Code civil.

[2197] Eric Barendt, « La protection de la vie privée en Angleterre », *LEGICOM* 1999/4 N° 20, pp. 115-120.
[2198] House of Lords, *Malone v Commissioner for the Metropolis Police* (n° 2), [1979] Chancery Division 344.
[2199] Cour européenne de droits de l'homme (chambre plénière), Affaire nà. 8691/79, *Case of Malone v. the United Kingdom,* 2 août 1984.

Sous-section 2. Le refus français de la protection directe des données personnelles et de la vie privée par la Constitution

La protection de la vie privée en France n'est pas directement protégée par la Constitution de 1958. Ce n'est qu'en 1970[2200], par l'introduction d'un article 9 dans le Code civil que cette protection de la vue privée a été réalisée. Cet article précise : « *Chacun a droit au respect de sa vie privée. Les juges peuvent […] prescrire toutes mesures […] propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée ; ces mesures peuvent, s'il y a urgence, être ordonnées en référé* ». En 1978, l'article 1er de la loi informatique et libertés[2201] ajoutait : « *l'informatique ne doit pas porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Il semble donc que la protection de la vie privée et des données à caractère personnel ne soit que du ressort de la loi et ne soit effective que tardivement, après les années 1970. Avant, seules la diffamation ou l'injure relevaient de la loi pour la presse ; or la diffamation n'est plus un délit si les faits dévoilés sont réels et effectifs.

En 1993, dans un rapport présenté au Président de la République[2202], le Comité présidé par le doyen Georges Vedel, constatait que « *la consécration constitutionnelle de certains droits nouveaux* [parmi lesquels] *appartient l'affirmation du respect de la vie privée et de la dignité de la personne] paraît […] très opportune eu égard aux conditions d'évolution de la société française »*, et en conséquence, il proposait d'ajouter à l'article 66 de la Constitution, la phrase : « *Chacun a droit au respect de sa vie privée et de la dignité de sa personne* ». Dans la lettre accompagnant ce rapport, Georges Vedel se posait la question d'introduire dans la Constitution des instances autres que le Conseil économique et social, devenu depuis le Conseil économique, social et environnemental, ou CESE[2203], en particulier la Commission nationale de l'informatique et des libertés. Ces deux mesures auraient renforcé la protection de la vie privée des individus, pérennisé et protégé les attributions de la Commission nationale de

[2200] Loi nº 70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens*, publiée au JORF du 19 juillet 1970 p. 6751.
[2201] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*.
[2202] Comité consultatif pour une révision de la Constitution, présidé par le doyen Georges Vedel, *Rapport au Président de la République, Propositions pour une révision de la Constitution*, 15 février 1993.
[2203] Modification apportée par l'article 33 de la loi constitutionnelle nº 2008-724 du 23 juillet 2008 *de modernisation des institutions de la Ve République.*

l'informatique et des libertés au travers d'une loi organique. Ces propositions ne furent pas retenues.

En 1997, au terme d'une analyse minutieuse de la jurisprudence du Conseil constitutionnel, un auteur concluait ses développements consacrés au droit au respect de la vie privée, en relevant qu'il n'était pas certain que ce principe « *ait, en lui-même, valeur constitutionnelle* »[2204].

Toutefois, en 1999, le Conseil constitutionnel a déduit le principe du respect de la vie privée de l'article 2 de la Déclaration des droits de l'homme et du citoyen[2205]. En effet pour le Conseil constitutionnel, la liberté, proclamée comme *« droit naturel et imprescriptible de l'homme »* à l'article 2 de la Déclaration de 1 789, *« implique le respect de la vie privée »*. Après le droit international, la protection de la vie privée est relayée par la jurisprudence constitutionnelle[2206]. En s'appuyant sur cette décision, et l'existence de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, ainsi que les articles 7 et 8 de la Charte européenne des droits fondamentaux du 7 décembre 2000, en 2008, le Comité de réflexion[2207] sur le préambule de la Constitution a conclu qu'il était « *apparu au comité que la réaffirmation expresse, dans le Préambule de la Constitution, du droit au respect de la vie privée et à la protection des données personnelles serait dépourvue de toute portée pratique, faute d'ajouter une composante significative aux contraintes juridiques auxquelles est d'ores et déjà soumis le législateur par le double effet de la jurisprudence du Conseil constitutionnel et des traités internationaux* ». Cette décision a été prise malgré le plaidoyer du président de la Commission nationale informatique et liberté de l'époque, M. Alex Türk qui considérait que nos sociétés devenaient de plus en plus dépendantes des nouvelles technologies d'information et de communication et qu'il n'existait aucune limite technique à la collecte croissante des données personnelles. À l'occasion de la présentation du 28e rapport annuel de la CNIL[2208], M. Alex Türk demandait cette protection constitutionnelle des données personnelles arguant que : « *Du lever au coucher, nous sommes tous plus ou moins soumis [à] un double traçage :*

[2204] Nicolas Molfessis, *Le Conseil constitutionnel et le droit privé*, préf. M. Gobert, LGDJ, 1 997, no 163.
[2205] Conseil constitutionnel, Décision no 99-416 du 23 juillet 1999, *Loi portant création d'une couverture médicale universelle,* JO du 28 juillet 1999, p. 11250, considérant no 45.
[2206] Irène Bouhadana, « Constitution et droit à l'oubli numérique : état des lieux et perspectives », Irène Bouhadana, William Gilles (dir.), *Vie privée, vie publique à l'ère du numérique,* mai 2011, Revue de l'Institut du Monde et du Développement – RIMD 2011-1.
[2207] Comité de réflexion sur le préambule de la Constitution, présidé par Mme Simone Veil, *Redécouvrir le Préambule de la Constitution, Rapport au Président de la République*, La Documentation française, Décembre 2008.
[2208] Commission nationale de l'informatique et des libertés, *28ème rapport d'activité 2007 de la Commission nationale de l'informatique et des libertés*, mai 2008, La documentation française.

un traçage dans l'espace [à travers le développement des systèmes de biométrie, de vidéosurveillance ou de géolocalisation, qui] met en cause la liberté d'aller et venir ; [et] un traçage dans le temps, [permis par les moteurs de recherche ou les réseaux sociaux sur Internet, qui] met en cause la liberté de pensée et d'expression »[2209]. En 2013, la Commission de l'informatique et des libertés, en la personne de sa présidente Mme Isabelle Falque-Pierrotin continue à demander la protection constitutionnelle des données personnelles face à la notion de droit de propriété des données personnelles qui permettrait une cession de cette propriété aux géants de l'Internet et au fait qu'aujourd'hui, les données personnelles sont uniquement protégées par le concept de vie privée[2210].

Par ailleurs, dans un rapport du Sénat de 2009[2211], les rapporteurs précisent qu'ils « *ont acquis la conviction qu'en ce qui concerne la conciliation entre développement technologique et droits au respect de la vie privée et à la protection des données, ni la loi, ni a fortiori la Constitution ne devraient contenir de dispositions trop rigides, qui risqueraient de se retrouver rapidement dépassées par le développement technologique et d'entraver ce dernier, sinon de rester inappliquées* ». Ils ajoutent qu'il « *leur a semblé évident qu'à l'heure où le développement technologique suscite, à juste titre, des craintes de voir se multiplier et s'amplifier les risques d'atteintes à la vie privée, l'inscription de cette notion dans le cœur de notre texte constitutionnel aurait valeur de symbole fort* ». Mais, contrairement à Mme Falque-Pierrotin, les « *rapporteurs ne considèrent pas […] qu'il serait utile d'inscrire dans notre Constitution à la fois le principe de respect de la vie privée et le droit à la protection des données à caractère personnel : […] le droit à la protection des données à caractère personnel doit être regardé comme une déclinaison du principe de respect de la vie privée, et non comme un droit autonome et spécifique dont la reconnaissance devrait être élevée au niveau constitutionnel* ».

Ainsi, les données personnelles ne sont pas protégées directement par la Constitution, mais indirectement par la jurisprudence constitutionnelle. Cette protection constitutionnelle directe

---

[2209] Relaté dans « *La CNIL veut inscrire dans la Constitution la protection des données personnelles* », Le Monde.fr avec AFP, 13 mai 2009, sur http://www.lemonde.fr/societe/article/2008/05/16/la-cnil-veut-inscrire-dans-la-constitution-la-protection-des-donnees-personnelles_1046127_3224.html, consulté le 6 juin 2016.

[2210] Boris Manenti, *Données personnelles : la Cnil milite pour modifier la Constitution, L'autorité a plaidé auprès des parlementaires et du gouvernement pour inscrire une garantie de la protection des données personnelles dans la révision constitutionnelle*. 24 mai 2013, Le cahier tendance de l'Obs, http://o.nouvelobs.com/high-tech/20130524.OBS0534/donnees-personnelles-la-cnil-milite-pour-modifier-la-constitution.html consulté le 6 juin 2016.

[2211] M. Yves Détraigne et Mme Anne-Marie Escoffier, *Rapport fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par le groupe de travail (2) relatif au respect de la vie privée à l'heure des mémoires numériques*, 27 mai 2009.

est demandée par certains acteurs. En 2010, la sénatrice Anne-Marie Escoffier a décidé de saisir le Ministère de la Justice de cette question de la reconnaissance d'un tel droit au niveau constitutionnel. La réponse du Ministère de la Justice a repris l'argumentaire développé dans le rapport du Comité de réflexion de 2008[2212].

Pour la Commission de l'informatique et des libertés, chargée de cette protection, les données personnelles doivent être explicitement protégées, alors que pour certains parlementaires, seule la vie privée doit faire l'objet de cette protection constitutionnelle, les données à caractère personnel restant quant à elles liées à la protection de la vie personnelle, permettant ainsi aux géants de l'Internet de continuer à utiliser librement et mercantilement ces données tant que la vie privée des individus reste apparemment protégée.

Comme le constate Mme Falque-Pierrotin[2213], « *en matière constitutionnelle, la reconnaissance d'un principe de respect de la vie privée par le Conseil constitutionnel a été, jusqu'à présent, essentiellement conçue dans une perspective "défensive". Il s'agit de s'assurer de la proportionnalité des mesures susceptibles d'y porter atteinte, et en particulier, de la conformité des dispositions relatives à l'identification des individus aux objectifs de valeur constitutionnelle que peuvent être l'ordre public, la sûreté, la défense de la propriété* ». Elle considère que « *la protection des données personnelles […] constitue […] un droit fondamental à part entière, au croisement du droit de propriété […] de la liberté d'expression […] et de la protection de la vie privée. Plus généralement, poser la question de la vie privée sur Internet, c'est s'interroger sur les données à caractère personnel concernant une personne qui sont ou peuvent être rendues disponibles, à son initiative ou à son insu, et qui peuvent faire l'objet d'une réutilisation, d'une exploitation ou d'un stockage potentiellement dommageables* ». Dans la société numérique, l'individu est éclaté et vu à travers des données biométriques, comportementales, de santé et d'identité, données qui sont dispersées et dont l'individu doit reprendre le contrôle par une reconnaissance explicite au sommet de la hiérarchie des normes des nouvelles dimensions des libertés individuelles et publiques, révélées et façonnées par l'Internet et les nouvelles technologies.

L'Allemagne et la France ont une approche normative du respect des principes. Le droit au respect de la vie privée est en Allemagne un principe issu directement de la Loi fondamentale

[2212] Stéphane Astier, « Le droit au respect de la vie privée, droit constitutionnellement reconnu », *JurilexBlog* du 21 janvier 2010, en ligne à http://www.jurilexblog.com/droit-respect-vie-privee-droit-constitutionnellement-reconnu-260783, consulté le 18 aout 2017.

[2213] Isabelle Falque-Pierrotin, « La Constitution et l'Internet », *Les Nouveaux Cahiers du Conseil constitutionnel* 2012/3 (nº 36), pp. 31-44.

et la protection des données à caractère personnel s'en déduit naturellement. En France, la protection de la vie privée n'est déduite qu'indirectement de la Constitution, et la protection de la vie privée est en partie assurée au travers de la protection des données à caractère personnel, donc d'un cadre législatif. Compte tenu de l'évolution des techniques, la protection allemande semble mieux adaptée aux évolutions techniques, car indépendante de la technique et des moyens utilisés, la protection des données étant une conséquence de la protection constitutionnelle de la dignité humaine et du contrôle de son évolution. De plus, la constitutionnalisation de la protection des données accorde un privilège constitutionnel par rapport aux textes législatifs ayant le même objet et permet un contrôle de la constitutionnalité de la mise en œuvre de ces textes, mais atténue l'intelligibilité des régimes de protection des données qui sont la dignité et l'autonomie individuelle.

Si la Constitution ne protège pas directement la vie privée et les données à caractère personnel, cette protection étant assurée par le juge constitutionnel, la loi pour une République numérique a introduit dans notre droit le principe de libre disposition de ces données personnelles en ajoutant en fin de l'article premier de la loi n° 78-17 dite informatique et liberté : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ». Mais, cette autodétermination informationnelle légale autant que la reconnaissance de la protection de la vie privée par l'article 9 du Code civil ou de la jurisprudence du Conseil constitutionnel ne semblent pas reconnaître les droits de la personnalité, droit à l'image ou droit à l'honneur. Les techniques de vidéosurveillance ou de géolocalisation attaquent ces droits reconnus par la Convention de sauvegarde des droits de l'homme. Les lois de lutte contre le terrorisme ou la criminalité mettent en œuvre des techniques contournant la protection de la vie privée. Reconnaître constitutionnellement un droit au respect et à la protection de la vie privée permettra d'inscrire cette protection dans les droits fondamentaux au même titre que la liberté d'expression, la liberté religieuse ou la sûreté. Est-ce parce que la vie privée n'avait pas la valeur qu'elle a acquise actuellement au siècle des Lumières et des philosophes qu'il faut la laisser protégée par les seuls lois ou traités internationaux sans lui donner valeur constitutionnelle directe ? Cette reconnaissance serait symboliquement importante face aux attaques gouvernementales et mercantiles internationales et donnerait à cette protection une réelle consistance, sans que cette protection ne soit issue d'un nouveau droit dérivé du droit de

propriété comme certains auteurs semblent le désirer, et comme le Conseil d'État le récuse dans son étude 2014, au profit d'un droit à l'autodétermination[2214].

La lisibilité de cette protection se trouve aujourd'hui réduite de par la répartition sur plusieurs textes, le Règlement général sur la protection des données et la loi n° 78-17 modifiée pour la prise en compte de ce règlement et de la directive (UE) 2016/680 du 27 avril 2016. La CNIL regrette dans son avis sur le projet de loi d'adaptation cet éclatement. Faute d'avoir introduit cette protection dans la Constitution, elle se trouve relever des textes de l'Union européenne, le règlement général sur la protection des données et la charte des droits fondamentaux de l'Union européenne, et de textes nationaux, la loi n° 78-17 et la jurisprudence du Conseil constitutionnel. Sur quelles bases, à l'avenir, s'appuiera le Conseil constitutionnel en cas d'atteinte aux droits de la personne : vie privée et données à caractère personnel ?

[2214] Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, pp. 25 et suivantes.

Chapitre 2. Vers un changement de rythme législatif

Face à l'évolution des techniques numériques, la protection des libertés nécessite de pouvoir élaborer des lois ou des règlements rapidement. L'adoption du règlement général sur la protection des données personnelles a démontré la difficulté d'élaborer et de finaliser des règles juridiques de protection des données personnelles compte tenu de l'évolution rapide des techniques, des intérêts divergents en jeu et des intérêts économiques sous-jacents, sans oublier les retombées sociologiques. Le consensus nécessaire à l'élaboration et l'adoption de règles adaptées à l'environnement numérique nécessite de modifier le processus d'élaboration des textes. Le Règlement général sur la protection des données est précédé de nombreux considérants qui ne sont pas contraignants pour les États membres[2215]. Ce qui ne figure pas dans les articles du Règlement reste soumis à la législation nationale de chaque État membre. Après plusieurs années de négociations, le 25 mai 2018, la protection des données personnelles connaîtra un nouveau socle commun au sein de l'Union européenne, mais des niveaux de protection différents selon les États membres continueront d'exister.

Les premières lois de protection sont apparues dans la seconde moitié des années 1970, Norvège, France et Allemagne. Lors de la promulgation de ces premières lois, la technique informatique commençait à se développer, les ordinateurs, outils chers et peu nombreux, ne savaient pas encore communiquer entre eux et les capacités de stockage étaient embryonnaires par rapport aux techniques actuelles, la bande magnétique était le support le plus utilisé. À cette époque, la France s'est dotée de deux lois innovantes : la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; la loi nº 78-783 du 17 janvier 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses propositions d'ordre administratif, social et fiscal ; complétées dix ans plus tard par la loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique, dite loi Godfrain. Les deux premières lois créaient de nouveaux droits pour les individus, ces deux lois ont connu de nombreuses modifications, jusqu'à la loi nº 2016-1321 du 7 octobre 2016 pour une République numérique, et la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes. Les principales modifications sont liées à la réglementation de l'Union européenne tendant à une harmonisation législative au sein de

[2215] Claire Bernier, « Le RGPD en 4 leçons pour les retardataires », *Sécurité et stratégie*, 2017/4 (28), pp. 85-90. URL : https://www.cairn.info/revue-securite-et-strategie-2017-4-page-85.htm consulté le 26 janvier 2018.

l'Union, mais aussi modifications rendues nécessaires de par l'évolution de la technique et de la société. La dernière de ces trois lois, la loi Godfrain, définissait pour sa part de nouveaux délits d'intrusion, d'altération et de maintien dans un système de traitement automatique de données. Cette dernière loi, relativement courte avec son article unique, n'a connu que peu de modifications et a été rédigée indépendamment des techniques utilisées, privilégiant les faits délictueux aux moyens utilisés pour les réaliser. Cette loi reste l'une des lois les plus efficaces pour lutter contre la cybercriminalité[2216] alors qu'en 1988, la cybercriminalité restait contingentée aux hackers, « bidouilleurs » plus que criminels. La loi Godfrain montre qu'une loi « générique », non restrictive et non liée à la technique utilisée demeure plus efficace dans un environnement mouvant qu'une loi basée sur l'utilisation de techniques particulières. Elle permet à la jurisprudence d'interpréter des notions telles que « système de traitement automatisé de données » non défini dans la loi. Ont été interprétés comme STAD par la jurisprudence, le réseau de transmissions d'ORANGE, le réseau carte bancaire, un disque dur ou un téléphone portable[2217].

[2216] Jacques Godfrain, « Loi Godfrain : La loi du 5 janvier sur la fraude informatique », Irène Bouhadana, William Gilles (dir.), *Cybercriminalité cybermenaces & cyberfraudes,* Mars 2012, Les éditions IMODEV, pp.92-94.
[2217] Ibid.

Section 1. Vers une réglementation interprétative et pragmatique

La difficulté de promulguer des lois s'attachant aux techniques plus qu'aux conséquences des actes délictueux est démontrée par les lois HADOPI[2218]. L'objectif des lois HADOPI était de lutter contre les copies illégales des œuvres artistiques[2219] donc de protéger les auteurs de ces œuvres ou leurs ayants droit[2220]. Une première loi[2221] est promulguée en août 2006 pour transposer en droit français une directive européenne d'harmonisation des droits d'auteur et des droits voisins dans la société de l'information[2222]. Cette loi modifie le code de la propriété intellectuelle. Elle comporte un chapitre IV très technique intitulé « Mesures techniques de protection et d'information », ces mesures de protection ne doivent pas entraver l'interopérabilité ni s'opposer au libre usage de l'œuvre. Ces mesures concernent la gestion numérique des droits ou en anglais *Digital Rights Management* (DRM)[2223]. Ces dispositifs concernent principalement les CD et DVD, et sont utilisés pour empêcher les copies illicites, voire pour les DVD leur utilisation en dehors de certaines zones géographiques. À l'époque, dès l'apparition des graveurs de CD ou de DVD, des logiciels de copie contournant les protections ont été mis à disposition sur Internet. Certains de ces logiciels fournissent automatiquement des mises à jour permettant de contourner les nouvelles techniques de protection. La fourniture de tels logiciels est interdite par la loi ainsi que leur utilisation[2224], mais les fournisseurs étant hors de l'Union européenne ne peuvent être poursuivis et

[2218] La loi nº 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur Internet*, dite loi HADOPI 1 ou loi création et Internet et la loi nº 2009-1 311 du 28 octobre 2009 *relative à la protection pénale de la propriété littéraire et artistique sur Internet* dite loi HADOPI 2.
[2219] Nicolas Curien, « IV. Révolution numérique et piratage », dans *L'industrie du disque.* Paris, La Découverte, « Repères », 2006, pp. 58-72. URL : https://www.cairn.info/l-industrie-du-disque--9782707148582-page-58.htm consulté le 30 janvier 2018.
[2220] Marin Dacos, Pierre Mounier, « I. Le droit d'auteur à l'épreuve du numérique », dans *L'édition électronique.* Paris, La Découverte, « Repères », 2010, pp. 8-25. URL : https://www.cairn.info/l-edition-electronique--9782707157294-page-8.htm consulté le 30 janvier 2018.
[2221] Loi nº 2006-961 du 1er août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information* publiée au JORF nº178 du 3 août 2006 p. 11529.
[2222] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 *sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.*
[2223] Anne-Gaëlle Geffroy, « Les DRMs : entre protection légale et protection technique des biens culturels à l'ère numérique », *Reflets et perspectives de la vie économique*, 2006/4 (Tome XLV), pp. 75-82. URL : https://www.cairn.info/revue-reflets-et-perspectives-de-la-vie-economique-2006-4-page-75.htm consulté le 30 janvier 2018.
[2224] Loi n° 2006-961 du 1er août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information* Art. 22.

condamnés[2225] et il est impossible de vérifier l'installation de tels outils sur un ordinateur personnel sans tomber dans les délits prévus par la loi Godfrain et la protection du domicile. De plus, ces logiciels permettaient de créer une copie de sauvegarde « privée », l'exception de « copie privée » est autorisée et donne lieu à perception d'un droit[2226].

Quelques années plus tard, la copie illicite s'est déportée des supports physiques vers des supports immatériels à travers Internet et des sites de téléchargement. Aussi en 2009, une nouvelle loi est nécessaire pour combattre le téléchargement illégal[2227]. Cette nouvelle loi sera la loi HADOPI du nom de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet, autorité administrative indépendante chargée de lutter contre le téléchargement illégal, créée par cette loi. Elle permet de surveiller le téléchargement illégal des œuvres sur les réseaux point à point (en anglais : *peer to peer*). Après une adoption difficile par le Parlement, cette loi sera en partie déclarée non conforme à la constitution par le Conseil constitutionnel[2228] et nécessitera l'adoption d'une seconde loi, la loi HADOPI 2, pour réintroduire un volet répressif. Mais cette loi a été critiquée dès son adoption, car elle ne visait que le téléchargement en point à point alors que la technique du *streaming*[2229] n'était pas concernée et devenait ainsi la nouvelle technique de lecture illégale des œuvres artistiques. Des logiciels permettant de sauvegarder localement des œuvres obtenues par *streaming* sont apparus, permettant ainsi une diffusion ultérieure illégale, mais difficilement décelable. Devant les critiques, le gouvernement envisageait une loi HADOPI 3[2230], loi qui ne vit pas le jour compte tenu du changement de majorité.

Cette loi HADOPI repose sur la jurisprudence du Conseil constitutionnel[2231]. Elle a pu être rendue opérationnelle parce que le Conseil constitutionnel[2232] a eu à se prononcer sur

---

[2225] En particulier, les fournisseurs nord-américains qui invoquent le précédent YAHOO!

[2226] Code de la propriété intellectuelle, art. L.311-1 à L.311-8.

[2227] Gilles Boenisch, « Juan Branco, *Réponses à Hadopi* », *Questions de communication* [En ligne], 24 | 2013, mis en ligne le 01 février 2014, consulté le 30 janvier 2018. URL : http://journals.openedition.org/questionsdecommunication/8838.

[2228] Conseil constitutionnel, Décision nº 2009-580 DC du 10 juin 2009, *loi favorisant la diffusion et la protection de la création sur Internet*.

[2229] Le streaming est une technique d'écoute ou de visualisation en temps réel sur un ordinateur personnel sans enregistrer l'œuvre sur ce terminal.

[2230] « Hadopi 3 pourrait avoir la peau du streaming et du direct download », 26 février 2013, *Rue 89*, URL : https://www.nouvelobs.com/rue89/rue89-internet/20130226.RUE4499/hadopi-3-pourrait-avoir-la-peau-du-streaming-et-du-direct-download.html consulté le 28 février 2018.

[2231] Irène Bouhadana, « La jurisprudence constitutionnelle en matière de cybercriminalité », Irène Bouhadana, William Gilles, *Cybercriminalité cybermences & cyberfraudes,* Mars 2012, Les éditions IMODEV, pp.106-113.

[2232] Conseil constitutionnel, Décision n° 2004-499 DC du 29 juillet 2004 *Loi 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*.

l'autorisation donnée aux sociétés de perception et de gestion des droits d'auteurs et les organismes professionnels de mettre en œuvre des traitements de données à caractère personnel en mutualisant les données de connexion, mais les Sages ont refusé[2233] de donner un pouvoir de sanction à la commission de la Haute autorité pour la diffusion des œuvres et de protection des droits sur Internet. Seul le juge peut prononcer une interruption de l'accès à Internet, cet accès étant nécessaire à l'exercice de la liberté d'expression[2234].

Cet exemple montre la difficulté pour une loi trop technique de pouvoir s'adapter aux évolutions techniques sans nécessiter une réécriture, donc la nécessité de conceptualiser l'objectif à atteindre ou l'objet de droit protégé indépendamment des techniques utilisées[2235]. L'applicabilité d'une loi ne doit pas dépendre de l'utilisation d'une technique, technique courant le risque de devenir rapidement obsolète et ainsi d'entraîner la nécessité pour ladite loi de devoir être réécrite ou de devenir inefficace et inutile.

Ainsi, l'étude d'impact concernant le projet de loi sur le renseignement, constate que le fait que la législation du Royaume-Uni sur le renseignement ne réglemente pas en tant que tel l'usage de telle ou telle technique, mais raisonne davantage par rapport à la nature de l'atteinte à la vie privée qu'elle représente, a permis à la législation anglaise de s'adapter aux évolutions technologiques, sans qu'il soit nécessaire de mettre à jour les textes trop fréquemment[2236].

Sous-section 1. Une législation énonçant des principes généraux

La protection des libertés dans une société numérique doit tenir compte des spécificités liées à la numérisation, mais les textes protecteurs doivent énoncer simplement les principes liés à cette protection sans devenir des manuels techniques. La précision technique peut devenir un frein à la protection compte tenu de l'évolution constante de la numérisation.

Les révolutionnaires français en élaborant la Déclaration des droits de l'homme et du citoyen de 1789 ont énoncé de grands principes, laissant aux constituants et aux législateurs le soin de

[2233] Conseil constitutionnel, Décision n° 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur Internet*.
[2234] Séverine Brondel, « Une autorité administrative ne peut pas suspendre l'accès à Internet », *Actualité juridique. Droit administratif,* 2009, n° 21, p. 1132.
[2235] Jacques Godfrain, « Loi Godfrain : La loi du 5 janvier sur la fraude informatique », Irène Bouhadana, William Gilles (dir.), *Cybercriminalité cybermenaces & cyberfraudes,* Mars 2012, Les éditions IMODEV, pp.92-94.
[2236] Extrait de Projet de loi *relatif au renseignement – Étude d'impact*, Assemblée nationale, 18 mars 2015.

décliner la protection de ces droits énoncés. La Déclaration des droits de l'homme[2237] apparaît comme un texte dogmatique qui affirme des principes généraux sans les définir, alors que la Déclaration des droits ou « *Bill of Rights*[2238] » des États-Unis d'Amérique ressort d'une dialectique pragmatique. Les droits des citoyens dérivent de situations précises, par exemple, le droit de porter une arme est lié à l'existence de milices, mais il n'est pas nécessaire d'appartenir à une milice pour détenir une arme. L'objectif et le contexte de l'élaboration de ces deux textes contemporains différaient, les États-Unis libéraient une nation du colonialisme, la France édifiait une société nouvelle[2239] avec de nouveaux droits.

Aux États-Unis d'Amérique, les droits sont d'essence pragmatique, leur objet est de protéger l'individu contre les pouvoirs publics, suivant en cela la tradition anglaise qui préfère à la proclamation de principes solennels la mise en place de garanties procédurales permettant au citoyen de se défendre lorsque ses libertés sont mises en cause par le pouvoir central[2240]. La protection des attaques non gouvernementales est d'essence contractuelle ou prétorienne. Pour les rédacteurs de la Déclaration des droits de l'homme et du citoyen, ce texte est conçu comme un texte politique de nature à guider les Constituants[2241]. La Déclaration des droits de l'homme et du citoyen est une œuvre intellectuelle, elle édicte des principes et elle nécessite une constitution qui doit respecter ces principes, et des lois pour encadrer et préciser son application pratique. La protection des intérêts individuels est normative et d'origine civiliste. Les nombreux codes de notre législation prévoient les diverses protections de l'individu : code monétaire et financier, code des postes et télécommunications, code de la construction, code de la protection intellectuelle, code du travail, etc.

Mais la législation française normative contient des lois « génériques », des lois décrivant des grands principes et non des cas pragmatiques et techniques, ainsi la loi Godfrain[2242], promulguée en 1988, permet de définir les délits concernant les accès et les altérations des

[2237] La Déclaration des droits de l'homme et du citoyen de 1789 dont les derniers articles ont été adoptés le 26 août 1789, énonce un ensemble de droits naturels individuels et les conditions de leur mise en œuvre.
[2238] La déclaration des droits ou « *Bill of Rights* » fut adoptée le 25 septembre 1789 par le premier congrès fédéral sous la forme des dix premiers amendements de la Constitution et trouve son origine dans la volonté e Madison de rallier les suffrages des antifédéralistes peu enclins à ratifier la Constitution.
[2239] Roseline Letteron, « L'idéologie des Droits de l'Homme en France et aux États-Unis » in *L'Universalité des Droits de l'Homme : apparences et réalités*, at http://www.diplomatie.gouv.fr/fr/IMG/pdf/FD001351.pdf consulté le 4 janvier 2017 .
[2240] Terence Marshall, « Épistémologie, ontologie, philosophie politique », *Droits*, 2007/2 (n° 46), pp. 213-276. URL : https://www.cairn.info/revue-droits-2007-2-page-213.htm consulté le 30 janvier 2018.
[2241] Cf. DDHC Art. 16. Toute Société dans laquelle la garantie des Droits n'est pas assurée, ni la séparation des Pouvoirs déterminée, n'a point de Constitution.
[2242] Loi nº 88-19 du 5 janvier 1988 *relative à la fraude informatique*.

systèmes de traitement automatique des données sans définir ni décrire les moyens utilisés pour ce faire. À l'opposé des lois modernes, cette loi est concise, générique et bien que conçue en 1988 reste directement applicable aujourd'hui malgré les évolutions de la technique disponible lors de son élaboration et l'apparition de nouvelles techniques.

D'autres exemples existent. Des textes très normés peuvent être révélés par une interprétation des juges. En droit civil, les sens successivement donnés à l'article 1384 al. 1 du Code civil[2243], selon lequel « *on est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde* », conçu, en 1804, comme une introduction aux alinéas et articles suivants, puis fondant, du fait d'interprétations successives de la Cour de cassation, à partir de 1896, une responsabilité autonome « *du fait des choses* » puis, à partir de 1991, « *du fait des personnes dont on doit répondre* »[2244]. Le même énoncé de l'article 1384 al. 1 a donc été successivement doté de trois sens différents. La « réalité » du sens de cet article réside dans son sens tel qu'interprété à différents moments de son histoire, et non dans sa lettre ou dans son sens « originel »[2245]

Dans le code pénal, le vol est défini des articles 311-1 à 311-11. Si les trois premiers articles définissent le vol et la peine associée, les articles suivants définissent les cas de vol aggravé et les possibilités de passer d'un délit à un crime soit en fonction du mode d'exécution (accompagné de violences, en bande, par intrusion dans une habitation, etc.), soit en fonction de la qualité de l'objet volé (objet archéologique, bien culturel dans un musée, etc.). Le vol y est décrit comme « la soustraction frauduleuse de la chose d'autrui », et nécessite donc de soustraire concrètement une chose, donc un objet concret. La soustraction d'énergie, objet immatériel, au préjudice d'autrui y a été assimilée à un vol par un article spécifique. Le juge devra qualifier l'infraction et prononcer la peine[2246]. Mais le vol d'informations dans un système de traitement automatisé n'existe pas pénalement au travers de ces articles, et ce sont bien les articles créés par la loi Godfrain qui peuvent être utilisés pour définir et sanctionner ces faits, ou subsidiairement les articles sanctionnant la violation du secret des affaires, les informations dévoilées par ces intrusions pouvant relever du domaine des secrets industriels voire secrets d'État.

[2243] Devenu l'article 1242 dans la rédaction du Code civil issue de l'ordonnance n° 2016-131 du 10 février 2016.
[2244] Cour de cassation, Assemblée Plénière, 29 mars 1991, n° 89-15231, *Blieck.*
[2245] Joël Moret-Bailly, « Esquisse d'une théorie pragmatiste du droit », *Droits* 2012/1 (n°55), pp. 177-212. URL : https://www.cairn.info/revue-droits-2012-1-page-177.htm consulté le 30 janvier 2018.
[2246] Ibid.

Le contraste existe entre la loi Godfrain et les lois actuelles protégeant les données à caractère personnel et la vie privée, détaillées, précises, mais trop techniques et donc rapidement contournées par les évolutions de la technique. La loi HADOPI, déjà citée, en est un exemple. Mais d'autres lois récentes connaissent cette inflation d'articles[2247].

Le texte initial de la loi n° 78-17 définit les grands principes de la protection des données à caractère personnel et donne pouvoir à la Commission de l'informatique et des libertés d'édicter des règles propres à certains traitements ou à certaines techniques, les délits y sont décrits respectant la nécessité de légalité des incriminations et des peines. Cette loi promulguée en 1978 et remaniée en 2004 pour transposer la directive 95/46/CE ne connaissait pas, lors de cette promulgation et révision, le WEB 2.0, les smartphones, la géolocalisation et le GPS ou les objets connectés. Dans ses recommandations sur la sécurité des systèmes de vote par voie électronique[2248] ou sur la géolocalisation des véhicules automobiles utilisés par les employés d'un organisme privé ou public[2249], la Commission de l'informatique et des libertés définit de manière concrète les implications de la loi du 6 janvier 1978 pour des problématiques émergentes, reprenant ici le rôle de la Cour de cassation sur l'article 1384 al. 1 du Code civil. L'usage du droit souple par les Autorités administratives indépendantes s'apparente à la notion de directive, ou lignes directrices, tel qu'elle a été dégagée par le Conseil d'État[2250] : « *Une autorité administrative peut, alors qu'elle ne dispose pas en la matière du pouvoir réglementaire, encadrer l'action de l'administration, dans le but d'en assurer la cohérence, en déterminant, par la voie de lignes directrices, sans édicter de condition nouvelle, des critères permettant de mettre en œuvre un texte qu'elle est chargée d'appliquer, sous réserve de motifs d'intérêt général conduisant à y déroger et de l'appréciation particulière de chaque situation. À l'occasion d'un recours formé contre une décision individuelle qui fait application de telles lignes directrices, leurs orientations et l'application qui en est faite peuvent être contestées* ».

[2247] 48 articles dans la version initiale de la loi n° 78-17 du 6 janvier 1978, 72 articles dans la version en vigueur au 4 janvier 2017, 113 articles dans 4 Titres pour la loi n° 2016-1 321 du 7 octobre 2016 *pour une République numérique* et plus de 60 décrets d'application prévus parus ou à paraitre.

[2248] Commission nationale de l'informatique et des libertés, *Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.*

[2249] Commission nationale de l'informatique et des libertés, *Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public.*

[2250] Conseil d'État, Section, *Crédit foncier de France c/ demoiselle Gaupillat et dame Ader*, Arrêt du 11 décembre 1970, requête n° 78880, Recueil Lebon p. 750.

L'objet de droit est créé par la loi, une Autorité administrative est chargée d'édicter les règles liées aux différentes techniques utilisées et d'en contrôler leur respect, créant ainsi un « droit mou » ou « droit souple », dénommé « *Soft law* » en anglais.

Sous-section 2. Des lignes directrices et des recommandations adaptées au contexte

Le Conseil d'État a consacré une de ces études annuelles[2251] à ce droit souple. En avant-propos de cette étude, Jean-Marc Sauvet, vice-président du Conseil d'État, écrit : « *Il semble, […], que le droit souple puisse être l'oxygénation du droit et favoriser sa respiration dans les interstices du corset parfois un peu trop serré des sources traditionnelles de la règle. Il peut accompagner la mise en œuvre du "droit dur", comme il peut dans certains cas s'y substituer pour la mise en œuvre de politiques publiques suffisamment définies et encadrées par la loi* ». Son emploi raisonné contribue à une simplification des normes et à la qualité des normes.
Avec la Commission nationale de l'informatique et des libertés, ce droit souple est utilisé pour définir les normes et l'état de l'art pour la protection des données à caractère personnel donc de la vie privée dans une société numérique.

§ 1 - Le droit souple dans un contexte non figé ou émergent

Le droit souple est apparu en droit international dès 1930 pour tenir compte des difficultés à tenir des engagements interétatiques. Il est utilisé dans le cadre de l'Union européenne, certaines directives renvoyant à des normes techniques.

A) Le droit souple utilisé en droit international

Le terme de *soft law* est apparu en 1930 pour la première fois[2252]. Le concept de *soft law* est apparu dans le droit international public au début des années mil neuf soixante-dix. À l'époque, la réflexion sur les sources du droit international public s'est accélérée en prenant en compte

[2251] Conseil d'État, *Le Droit souple*, Les rapports du Conseil d'État, 2013.
[2252] Lord A. McNair, « The Functions and Differing Legal Character of Treaties », *British Yearbook of International Law*, 1930.

deux problèmes, la place des résolutions dans les organisations internationales et le caractère inapproprié du droit coutumier. La coutume est une source de droit international dans la mesure où son non-respect peut entraîner une sanction[2253]. Concernant le droit souple, également appelé « droit mou », il était malaisé de qualifier juridiquement des actes non obligatoires adoptés d'un commun accord par la collectivité de certains États en vue de définir des principes et des orientations politiques. Les actes du droit souple sont applicables en vertu des engagements réciproques pris par les parties contractantes. Ils incorporent des règles de conduite, sans pour autant impliquer la création, la préservation, le renforcement, la modification ou l'extinction des droits et des obligations, selon les règles classiques du droit international public. Aux côtés des actes conventionnels à caractère contraignant du droit international qui produisent des droits et des obligations pour les parties, ce type d'actes n'a pas nécessairement ni immédiatement un caractère juridique, et, par conséquent, n'est pas forcément contraignant[2254].

Cet aspect contraignant du droit international peut être l'objet d'analyses divergentes. Récemment, en 2015, l'« Accord de Paris » concernant la lutte contre le réchauffement climatique énonce des principes acceptés et approuvés par l'ensemble des 195 délégations le 12 décembre 2015. Cet accord a été annoncé comme contraignant par M. Fabius, président de la COP 21, et non contraignant par certains participants et par les responsables de Greenpeace[2255] faute de sanctions prévues.

Comme l'écrit le Conseil d'État dans son étude[2256], le droit souple se manifeste dans les relations internationales sous de multiples formes : les déclarations des conférences intergouvernementales, les résolutions de l'Assemblée générale des Nations unies, les recommandations des organisations internationales, les dispositions souples dans un traité, les conventions non ratifiées, les actes concertés non conventionnels, les avis consultatifs, voire les opinions individuelles et dissidences des juges de la Cour internationale de justice[2257].

[2253] Guillaume Le Floch. « La coutume dans la jurisprudence de la Cour Internationale de Justice en Droit de la Mer », *Revue juridique de l'Ouest*, 2001-4. pp. 535-573.

[2254] Filippa Chatzistavrou, « L'usage du *soft law* dans le système juridique international et ses implications sémantiques et pratiques sur la notion de règle de droit », *Le Portique* [En ligne], 15 | 2005, mis en ligne le 15 décembre 2007, consulté le 30 septembre 2016. URL : http://leportique.revues.org/591.

[2255] Audrey Garric, « L'accord obtenu à la COP210 est-il vraiment juridiquement contraignant ? », 14 décembre 2016, *Le Monde.fr,* URL : http://www.lemonde.fr/cop21/article/2015/12/14/l-accord-de-paris-sur-le-climat-est-il-vraiment-juridiquement-contraignant_4831255_4527432.html consulté le 30 janvier 2018.

[2256] Conseil d'État, *Le Droit souple*, Les rapports du Conseil d'État, 2013.

[2257] Isabelle Duplessis, « Le vertige et la *soft law* : réactions doctrinales en droit international », *Revue québécoise de droit international,* hors-série, 2007, pp. 246-268. Article disponible en ligne à l'URL : http://www.crimt.org/PDF/hs07_duplessis.pdf consulté le 30 janvier 2018.

Le droit souple peut constituer une étape avant sa transformation en convention internationale. Ainsi la Déclaration universelle des droits de l'homme (DUDH), adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948 proclame, selon le préambule, « *la présente Déclaration universelle des droits de l'homme comme l'idéal commun à atteindre par tous les peuples et toutes les nations* ». La DUDH a ainsi une valeur de référence sans caractère contraignant pour les États, sauf lorsque certaines de ses dispositions sont considérées comme la reprise d'un principe général du droit international ou d'une coutume. En France, le Conseil d'État a jugé que la Déclaration universelle des droits de l'homme n'avait pas l'autorité donnée aux traités dans l'ordre interne par la Constitution[2258]. Mais la Déclaration, instrument de droit souple, a inspiré deux textes de droit dur, les pactes internationaux des Nations unies du 16 décembre 1966, l'un relatif aux droits civils et politiques et l'autre aux droits économiques, sociaux et culturels.

D'autres exemples de résolutions de l'Assemblée générale dont le contenu a été repris ultérieurement dans des conventions peuvent être mentionnés : déclaration universelle des droits de l'enfant du 20 novembre 1959, suivie par la convention internationale des droits de l'enfant du 20 novembre 1989 ; déclaration sur la protection de toutes les personnes contre les disparitions forcées du 18 décembre 1992 et convention internationale contre les disparitions forcées du 20 décembre 2006 ; règles pour l'égalisation des chances des personnes handicapées du 20 décembre 1993 et convention relative aux droits des personnes handicapées du 13 décembre 2006[2259].

B) Le droit souple proposé par le Conseil d'État

Dans son étude[2260], le Conseil d'État propose une définition du droit souple qui regroupe des instruments répondant à trois critères cumulatifs[2261] : ils modifient ou orientent les comportements de leurs destinataires en suscitant leur adhésion, ils ne créent pas par eux-mêmes de droits ou d'obligations pour leurs destinataires, ils présentent un degré de formalisation et de structuration les apparentant aux règles de droit. Pour le Conseil d'État, « *le droit souple permet d'appréhender les phénomènes émergents qui se multiplient dans le monde*

[2258] Cité par Gilles Lebreton, « Critique de la Déclaration universelle des Droits de l'homme », *CRIDF*, n°7, 2009, pp.17-22. URL : https://www.unicaen.fr/puc/images/crdf0702lebreton.pdf consulté le 31 janvier 2018.
[2259] Exemples cités dans l'étude du Conseil d'État sur le droit souple de 2013, p.25.
[2260] Conseil d'État, *Le Droit souple*, Les rapports du Conseil d'État, 2013, déjà cité.
[2261] Ibid. p. 9.

contemporain, soit en raison d'évolutions technologiques, soit de mutations sociétales. […] Il joue un rôle prédominant dans le fonctionnement d'Internet et est abondamment utilisé par la CNIL »[2262]. Il ajoute : « *Les recommandations des AAI sont d'autant plus suivies par leurs destinataires que ces autorités sont dotées par ailleurs de pouvoirs de sanction »*[2263].

L'étude du Conseil d'État vise à donner aux pouvoirs publics une doctrine et des outils et elle contient 25 propositions d'utilisation du droit souple. Parmi ces propositions, certaines s'appliquent directement à la société numérique et à la protection des données à caractère personnel. Dans le cas de phénomènes émergents, le Conseil d'État recommande d'utiliser le « droit souple » si le « droit dur » ne peut être utilisé du fait de la non-stabilité du phénomène émergent ou en complément du droit comme outil de régulation d'un domaine d'activité[2264]. Il recommande aussi leur utilisation en accompagnement du droit[2265], ce qui est assuré tant par la CNIL que par l'ARCEP dans leurs domaines respectifs, les lignes directrices ainsi édictées doivent par ailleurs être encadrées par le législateur et ne pas se substituer à cet encadrement législatif pour respecter les contraintes constitutionnelles[2266]. Ces lignes directrices doivent se substituer aux dispositions réglementaires trop détaillées en recentrant la législation sur les dispositions qui doivent nécessairement relever de la loi. Le législateur, sous réserve de ne pas commettre d'incompétence négative et d'épuiser la compétence qu'il tient de l'article 34 de la Constitution, peut s'en tenir à l'énoncé de principes généraux que l'autorité publique chargée de leur mise en œuvre pourra expliciter, par la voie de recommandations ou de lignes directrices[2267]. Le Conseil d'État relève qu'une telle configuration est observée avec la protection des données personnelles, la loi définissant les principes fondamentaux : nécessité de la collecte, proportionnalité et loyauté, la Commission nationale de l'informatique et des libertés précise comment il faut interpréter les principes énoncés par le législateur, mais en s'adaptant aux circonstances particulières de chaque cas d'espèce. Le Conseil préconise d'éclaircir les règles de compétences et de garantir lors de leur élaboration la sécurité juridique

[2262] Ibid. Page 10.
[2263] Ibid.
[2264] Conseil d'État, *Le Droit souple*, Les rapports du Conseil d'État, 2013, déjà citée, proposition n° 1, test d'utilité
[2265] Ibid. proposition n° 2.
[2266] Conseil constitutionnel, Décision n° 2011-639 DC du 28 juillet 2011, *Loi tendant à améliorer le fonctionnement des maisons départementales des personnes handicapées et portant diverses dispositions relatives à la politique du handicap*,.
[2267] Conseil d'État, *Le Droit souple*, Les rapports du Conseil d'État, 2013, déjà citée, proposition n° 4.

afin d'éviter des annulations pour incompétences[2268], et de publier, notamment sur Internet, les instruments de droit souple pour une diffusion large[2269].

§ 2 - Le droit souple dans la société numérique

Depuis sa création, le réseau Internet a fait l'objet de recommandations[2270] objets d'un consensus. Il y existe des instances normatives comme le W3C. Le respect des recommandations permet le fonctionnement du réseau et l'intercommunication des applications.

A) Les instances de gouvernance du WEB

Dans le monde numérique où les acteurs principaux ne sont pas européens, mais américains, l'utilisation de principes, de recommandations et de lignes directrices permet de contourner les différentes législations intervenant sur le WEB. De plus, le monde numérique est habitué à fonctionner avec ces concepts, le World Wide WEB Consortium (W3C) est une communauté internationale qui développe des standards ouverts assurant la croissance et la pérennité du WEB. Le W3C opère au travers d'un code éthique et de conduite. Parmi les membres du W3C figurent nombre d'acteurs principaux du développement du WEB : Google, Microsoft, Facebook, Apple, Adobe, mais aussi des organismes de recherche comme le CERN, ou des opérateurs de télécommunications : AT&T, ORANGE, ou des industriels comme Samsung, Nokia, Ericsson, voire des fournisseurs de logiciel libre comme Mozilla. Dès l'origine d'Internet, les RFC ou *Requests for comment*, ont été utilisées pour définir le fonctionnement du réseau. Ces RFC sont plutôt stables, malgré leur dénomination, et classées de « obligatoire » à « non recommandé » et se différencient des standards techniques internationaux, contraignants et gérés par l'Organisation internationale de normalisation plus connue sous son sigle anglais ISO pour *International Organization for Standardization*.

[2268] Ibid. proposition n° 10.
[2269] Ibid. proposition n° 15.
[2270] Les *requests for comment* ou RFC, en français littéralement demandes de commentaires, sont une série de documents décrivant les aspects techniques d'Internet ou de différents matériels informatiques utilisés dans le réseau (routeurs, serveurs DHCP). Les RFC sont élaborées par des experts techniques avant d'être soumises à la communauté Internet. Ces RFC rédigées en anglais utilisent les termes *must, must not, should, may, etc.* pour définir les exigences (obligation, interdiction, recommandation, etc.).

Malgré la prévalence du droit souple dans la gouvernance d'Internet, le passage vers le droit dur est réalisé pour certains aspects de la régulation d'Internet. En France, il en est ainsi de l'attribution des noms de domaine, selon un processus qui a connu trois étapes. La première étape a été caractérisée par un fonctionnement informel. L'Institut national de recherche en automatique et en informatique (INRIA), établissement public, s'est vu confier en 1986 par le prédécesseur de l'ICANN, l'*Internet Assigned Numbers Authority* (IANA), la gestion du « registre » du .fr. Une « charte du nommage », définissant les règles d'ouverture et de retrait des noms de domaine, en dehors de tout cadre juridique a été établie en 1996, la charte prend en compte, les problèmes de propriété intellectuelle. Ce n'est qu'en 2004 que le législateur est intervenu, en disposant que le ministre chargé des communications électroniques est compétent pour désigner, après consultation publique, les organismes « chargés d'attribuer et de gérer les noms de domaine » de l'extension .fr. L'Association française pour le nommage Internet en coopération (AFNIC), association créée en 1998 par l'État et l'INRIA pour reprendre la mission de gestion du .fr assurée précédemment par l'INRIA, s'est vue confirmée sur le fondement de ce nouveau cadre légal par un arrêté du 19 février 2010 pour une durée de 7 ans, arrêté annulé pour vice de procédure par deux arrêts du Conseil d'État du 10 juin 2013[2271]. Le Conseil d'État a fait droit à la requête demandant l'annulation d'un arrêté du 19 février 2010 désignant l'office d'enregistrement du domaine .fr, la convention qui le complète, ainsi que les chartes de nommage et la procédure de résolution des litiges « PREDEC » en vigueur de 2009 à 2011. Ces arrêts n'ont pas eu de conséquences pratiques, car par une décision du 6 octobre 2010, le Conseil constitutionnel[2272] a ouvert une troisième étape impliquant un encadrement législatif plus précis. Considérant « *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 dans la vie économique et sociale, notamment pour ceux qui exercent leur activité en ligne, l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur Internet affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre* » et en a déduit que la loi était entachée d'incompétence négative, car elle avait « *entièrement délégué le pouvoir d'encadrer les conditions dans lesquelles les noms de domaine sont attribués ou peuvent être renouvelés, refusés ou retirés* ». Au terme de cette évolution, l'attribution des noms

[2271] Conseil d'État, 10ème et 9ème sous-sections réunies, 10/06/2013, 327 375 et Conseil d'État, 10ème et 9ème sous-sections réunies, 10/06/2013, 337 320.
[2272] Conseil constitutionnel, Décision nº 2010-45 QPC, *M. Mathieu P. [Noms de domaine Internet]*.

de domaine est régie par des dispositions plus détaillées issues d'une loi du 22 mars 2011[2273], qui énoncent désormais les principes présidant à l'attribution (règle du « premier arrivé, premier servi », attribution sur la base des déclarations faites par le demandeur et sous sa responsabilité). Le droit souple a ainsi permis d'accompagner le développement d'Internet et de ne passer au droit dur que lorsque le phénomène et la réflexion à son sujet avaient acquis une maturité suffisante et que le législateur pouvait se saisir du phénomène.

Mais, ce droit souple élaboré par consensus américano-européen régit un réseau où la majorité des acteurs est aujourd'hui asiatique et où la protection des libertés n'a pas la résonnance connue en occident[2274]. Ce droit souple ne protège pas les données à caractère personnel qui font l'objet de réglementation au niveau de l'Union européenne et des États. En France, la CNIL a la responsabilité de cette protection. Elle complète la réglementation par des lignes directrices ou des recommandations.

B) Les lignes directrices de la CNIL

En France, le droit souple est utilisé par les Autorités administratives indépendantes au travers de recommandations ou de lignes directrices dans le cadre de leur rôle de régulation. Sur le site de la CNIL, une recherche avec le mot clé « Recommandations » donne 141 résultats[2275] et 78 délibérations concernant des recommandations. Ces recommandations portent sur des aspects divers de la protection des données à caractère personnel, il est possible d'y trouver : publication d'une méthode pour mener des études d'impact sur la vie privée (*Privacy Impact Assessment*) ; publication d'un avis du groupe de l'article 29 sur les techniques d'anonymisation ; adoption d'une recommandation sur les coffres-forts électroniques ; mise en demeure d'une vingtaine d'éditeurs de sites Internet qui ne respectent pas les règles encadrant l'utilisation des cookies et autres traceurs, etc.

[2273] Loi n° 2011-302 du 22 mars 2011 *portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques,* publiée au JORF n°0069 du 23 mars 2011 p. 5186.

[2274] La Chine a promulgué une loi sur la cybersécurité, entrée en application le 1er juin 2017. Cette loi réglemente la protection des données de la Chine assez similaire au RGPD de l'Union européenne, sans droit à l'oubli. Mais le pricipe concernant le traitement des données est un traitement sur le territoire chinois sans transfert interfrontalier de ces données (Emmanuel Pernot, « Loi sur la cybersécurité chinoise : Protection des données personnelles », 18 novembre 2017, URL : https://epernot.com/fr/loi-cybersecurite-chine-protection-donnees-personnelles/ consulté le 31 janvier 2018).

[2275] Recherche effectuée le 13 septembre 2017.

Après l'arrêt de la Cour de justice de l'Union européenne du 13 mai 2014[2276] concernant le déréférencement des moteurs de recherche, le groupe de l'Article 29 a adopté et publié des lignes directrices pour assurer une application harmonisée de l'arrêt de la Cour de justice de l'Union européenne[2277], lignes directrices qui contiennent une interprétation commune de l'arrêt ainsi que des critères que les autorités utiliseront dans le cadre de l'instruction des plaintes leur parvenant suite à des refus de déréférencement par les moteurs de recherche. L'objectif de ces lignes directrices est d'éviter le contournement des décisions de déréférencement. Elles contiennent une liste de 13 critères communs que les autorités de protection des données appliqueront pour traiter les plaintes qu'elles reçoivent suite à des refus de déréférencement par les moteurs de recherche. Ces 13 critères permettent d'harmoniser les décisions, mais doivent être considérés comme des outils de travail flexibles aidant les autorités dans la prise de décision.

Mais les parlementaires critiquent le droit souple, car il leur échappe. En 2007, le Parlement européen a adopté une résolution critiquant le recours aux « instruments juridiques non contraignants »[2278]. Dans les considérants de la proposition de résolution, il est écrit entre autres : « *la notion de soft law, qui est fondée sur la pratique courante, est ambiguë et pernicieuse et ne devrait être utilisée dans aucun document des institutions communautaires*, » et « *les prétendus instruments de soft law, tels que recommandations, livres verts et blancs ou conclusions du Conseil, n'ont aucune valeur juridique ni aucun caractère contraignant* », en conséquence, les Parlementaires demandent « *à la Commission de développer, en coopération avec le Parlement, un modus operandi qui garantisse la participation des organismes démocratiquement élus, y compris, éventuellement, au moyen d'un accord interinstitutionnel et, donc, un contrôle plus efficace de l'opportunité d'adopter des instruments juridiques non contraignants* ».

Dans un monde technique fortement et rapidement évolutif, la notion de « soft law » s'est imposée dès l'origine d'Internet, car elle permet une évolution rapide et pragmatique des

[2276] Cour de justice de l'Union européenne, arrêt du 13 mai 2014 *Google Spain SL et Google Inc. v Agencia Española de Protección de Datos (AEPD) et Mario Costeja González* (C-131/12).

[2277] Article 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12*, adoptées le 26 novembre 2014, en ligne à http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, consultées le 21 aout 2017.

[2278] Parlement européen, Rapport *sur les implications juridiques et institutionnelles du recours aux instruments juridiques non contraignants (soft law)* (2007/2028 (INI)) A6-0259/2007 du 28 juin 2007.

principes directeurs. Le monde juridique du droit « dur » est un monde à évolution lente d'où une possible inadéquation entre les lois et les techniques qui les contournent avant leur promulgation. La société numérique nécessite des lois pour créer des objets de droit et des contraintes fortes, ces lois créent une stabilité juridique et énoncent et définissent les grands principes du droit. Ces lois doivent être complétées par des règles élaborées plus rapidement, pragmatiques et décrivant ou fournissant les moyens de respecter les obligations légales. Ces moyens peuvent être divers et doivent s'adapter aux techniques visées. Ces règles et principes doivent être validés et contrôlés par des organismes indépendants ayant un pouvoir de sanction si leur non-respect entraîne une violation de la législation.

Dans deux décisions, rendues en assemblée plénière du 21 mars 2016[2279], le Conseil d'État accepte d'être saisi de recours en annulation contre des actes de droit souple, lorsqu'il s'agit d'avis, de recommandations, de mises en garde et de prises de position qui pourraient ensuite justifier des sanctions de la part des autorités ; ensuite, et sur ce point de manière novatrice, lorsque l'acte contesté est de nature à produire des effets notables, notamment de nature économique, ou lorsqu'il a pour objet d'influer de manière significative sur les comportements des personnes auxquelles il s'adresse. De tels actes n'étaient jusqu'alors pas susceptibles de recours juridictionnels dès lors qu'ils n'ont aucun effet juridique[2280]. La protection des données à caractère personnel entre dans les critères retenus par le Conseil d'État dans ses deux décisions. Elles placent le droit souple dans un continuum de normativité.

De plus, dans un univers numérique qui se joue des frontières, il semble, de par l'expérience du droit international, possible d'édicter des règles et principes acceptés par plusieurs États évitant ainsi une « Babélisation » du droit. Par ailleurs, les entreprises américaines sont habituées à exister dans un État où le droit souple est largement utilisé au travers des clauses contractuelles et de l'autorégulation. Mais la prédominance du droit nord-américain moins protecteur de l'individu que le droit de l'Union européenne peut fragiliser les protections mises en place.

[2279] Conseil d'État, Assemblée, Arrêt du 21 mars 2016, décision n° 368082, *Fairvesta international GMBH*, Publié au recueil Lebon et Conseil d'État, Assemblée, Arrêt du 21 mars 2016, décision n° 390023, *Société NC Numéricable*, Publié au recueil Lebon.

[2280] Conseil d'État, « Droit souple », communiqué du 21 mars 2016, URL : http://www.conseil-etat.fr/Actualites/Communiques/Droit-souple consulté le 31 janvier 2018.

Section 2. Vers une juridiction protectrice de l'individu

Dans un univers où les frontières semblent disparaître, l'individu peut communiquer sans limites territoriales et sans délai de transmission. L'individu se retrouve au sein d'un réseau dense et performant qui relie les individus entre eux. Cette densité de communications a un revers, des informations préjudiciables pour certaines personnes physiques ou morales peuvent circuler sur le réseau et nuire à l'image ou la réputation de ces personnes[2281]. De plus en plus d'informations à caractère personnel sont captées par des sociétés ou des États, dans un but de fichage ou de scoring[2282] voire de simple surveillance. Cette évaluation peut être utilisée pour une campagne de promotions et affiner la cible visée, elle peut être aussi utilisée par une compagnie d'assurance pour évaluer le risque associé à un assuré ou potentiel assuré[2283], voire par les forces de police pour évaluer la dangerosité d'un individu[2284].

Si certaines de ces techniques sont licites, elles peuvent aussi sortir du cadre légal. Il peut être alors difficile de pénaliser les fautifs faute de juridiction compétente, le délit étant réalisé dans un État, la victime résidant dans un autre État et le délinquant dans un troisième. Les règles applicables en droit international public ne sont pas toujours mises en œuvre compte tenu des difficultés d'accès par une personne physique et des faibles réparations potentielles ou des délais nécessaires pour aboutir à un jugement définitif. La sécurité juridique internationale n'est pas réellement garantie[2285]. Le problème de la compétence des instances judiciaires locales compte tenu des localisations ou de l'implication des États eux-mêmes nécessite de simplifier les règles de compétences.

[2281] Lionel Barbe, Michel Arnaud, Milad Doueihi *et al.*, « Un enjeu de société », *Documentaliste-Sciences de l'Information*, 2010/1 (Vol. 47), pp. 56-67. URL : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2010-1-page-56.htm consulté le 2 février 2018.

[2282] Technique permettant en marketing direct de mesurer via l'attribution de notes, la probabilité qu'un individu appartienne à la cible visée. Les critères retenus seront par exemple : la réponse au mailing, le nombre de relances, le nombre de commandes passées, le montant moyen d'une commande, les modalités et les délais de paiement, la sensibilité aux promotions... Ces notes permettent d'évaluer la valeur marchande d'un fichier de prospects.

[2283] Pierre-Alain de Malleray, « Le marketing dans l'assurance : le tournant du digital », *Revue d'économie financière*, 2017/2 (N° 126), pp. 145-168. URL : https://www.cairn.info/revue-d-economie-financiere-2017-2-page-145.htm consulté le 1er février 2018.

[2284] Virginie Gautron, David Monniaux, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », *Archives de politique criminelle*, 2016/1 (n° 38), pp. 123-135. URL : https://www.cairn.info/revue-archives-de-politique-criminelle-2016-1-page-123.htm consulté le 2 février 2018.

[2285] Samuel Fulli-Lemaire, « Affaire PIP : quelques réflexions sur les aspects de droit international privé », *Revue internationale de droit économique*, 2015/1 (t. XXIX), pp. 99-122. URL : https://www.cairn.info/revue-internationale-de-droit-economique-2015-1-page-99.htm consulté le 1er février 2018.

Sous-section 1. Compétence des instances de défense des libertés

En matière de compétence numérique, deux types d'instances peuvent être sollicitées : les instances judiciaires et les autorités administratives indépendantes. Les instances judiciaires ont compétence pour les fautes pénales et les réparations civiles, les autorités administratives n'ont compétence que dans le cadre de la loi qui les a créées : protection des données à caractère personnel pour la CNIL ; diffusion des données administratives pour la CADA, cette compétence pouvant être limitée de par la loi.

§ 1 - Les instances judiciaires

En matière judiciaire, la mondialisation des acteurs rend délicat le contrôle du respect des normes, celles-ci pouvant dépendre de la localisation des différents acteurs. De plus, cette compétence peut dépendre de l'activité répréhensible : activité commerciale ou assimilée et actes d'origine pénale d'atteinte à la personne. Selon les États, le choix de la procédure peut différer[2286].

A) La compétence en matière commerciale ou industrielle

Le cyberespace ne remet pas en question l'applicabilité des lois nationales. Le problème ne réside pas tellement dans la dimension internationale d'Internet, mais plutôt dans le fait que des lois nationales divergentes règlent une situation internationale. Le défi qui se présente au droit est celui de jeter un pont entre le droit national et la réalité globale du cyberespace[2287]. En droit international privé, se pose d'abord la question du juge compétent puis dans un deuxième temps celle de la loi applicable. Il peut y avoir une dissociation des compétences. La partie du préjudice subie à l'étranger doit être plutôt soumise à l'appréciation du droit étranger. Il n'en va pas ainsi en droit pénal international. Un juge français n'applique pas les lois pénales

[2286] Samuel Fulli-Lemaire, « Affaire PIP : quelques réflexions sur les aspects de droit international privé », *Revue internationale de droit économique*, 2015/1 (t. XXIX), pp. 99-122. Op. cit.
[2287] Josef Drexl, « Le commerce électronique et la protection des consommateurs », *Revue internationale de droit économique*, 2002/2 (t. XVI), pp. 405-444. URL : https://www.cairn.info/revue-internationale-de-droit-economique-2002-2-page-405.htm consulté le 1er février 2018.

étrangères : il n'applique que la loi pénale française. Il n'est compétent que parce que la loi pénale française a été violée[2288].

En matière d'atteinte en contrefaçon au droit d'auteur, la Cour de cassation a reconnu en 2014, au travers de trois arrêts, la compétence du juge français dès lors que la diffusion des contenus litigieux par des sites Internet ou par un réseau de télécommunication est accessible en France[2289]. La première affaire opposait un auteur-compositeur résidant en France à une société autrichienne ayant reproduit son album sur des supports CD sans autorisation, lesdits supports litigieux avaient par la suite été commercialisés par des sociétés situées en Angleterre, par l'intermédiaire d'un site Internet accessible depuis la France et pouvaient être acquis depuis la France. La Cour d'appel de Toulouse s'était déclarée incompétente au motif que tant le domicile du défendeur que le lieu de réalisation du dommage allégué n'étaient pas situés en France, mais en Autriche ou au Royaume-Uni. La Cour de cassation avait saisi l'opportunité de ce pourvoi pour soumettre plusieurs questions préjudicielles à la Cour de Justice de l'Union européenne, afin, notamment, de déterminer si, au sens de l'article 5-3 du Règlement (CE) n°44/2001[2290] en matière de compétence judiciaire, les juridictions françaises étaient compétentes, dès lors que le site Internet commercialisant les supports prétendument contrefaisants était accessible en France, sans pour autant être destiné au public français. Dans son arrêt[2291], la Cour de justice de l'Union européenne a arrêté que : « *L'article 5, point 3, du règlement (CE) n° 44/2001 du Conseil, du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution de décisions en matière civile et commerciale, doit être interprété en ce sens que, en cas d'atteinte alléguée aux droits patrimoniaux d'auteur garantis par l'État membre de la juridiction saisie, celle-ci est compétente pour connaître d'une action en responsabilité introduite par l'auteur d'une œuvre à l'encontre d'une société établie dans un autre État membre et ayant, dans celui-ci, reproduit ladite œuvre sur un support matériel qui est ensuite vendu par des sociétés établies dans un troisième État membre, par l'intermédiaire d'un site*

[2288] David Chilstein, « Le droit de la communication à l'épreuve du droit pénal international », *LEGICOM*, 2014/1 (n° 52), pp. 51-58. URL : https://www.cairn.info/revue-legicom-2014-1-page-51.htm consulté le 1er février 2018.
[2289] Cour de cassation, chambre civile 1, arrêt du 22 janvier 2014, pourvoi n°10-15.890, *M. Pinckney c/ KDG Mediatech* ; Cour de cassation, chambre civile 1, arrêt du 22 janvier 2014, pourvoi n°11-24019, *Samuel X. C. BBC* ; Cour de cassation, chambre civile 1, arrêt du 22 janvier 2014, pourvoi n°11-26822, *Korda c/ Onion/The Onion*.
[2290] Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 *concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale* publié au Journal officiel n° L 012 du 16/01/2001 pp. 1-23.
[2291] Cour de justice de l'Union européenne, quatrième chambre, Arrêt du 3 octobre 2013, *Peter Pinckney contre KDG Mediatech AG,* Demande de décision préjudicielle, introduite par la Cour de cassation (France), Affaire C-170/12.

Internet accessible également dans le ressort de la juridiction saisie. Cette juridiction n'est compétente que pour connaître du seul dommage causé sur le territoire de l'État membre dont elle relève ». S'appuyant sur cet arrêt, la Cour de cassation en a déduit la compétence des tribunaux français pour les dommages subis sur le territoire français en matière de contrefaçon du fait de l'accessibilité au site Internet depuis la France, même si ce site n'est pas dirigé vers un public français.

Dans les deux autres arrêts, elle a élargi sa compréhension de l'arrêt de la Cour de justice de l'Union européenne. Dans la seconde affaire qui opposait l'ayant droit d'un photographe français à la BBC, suite à la diffusion, sur l'une des chaînes du groupe britannique et sur Youtube, d'un documentaire reproduisant plusieurs de ses œuvres. Alors que la Cour d'appel s'était déclarée incompétente du fait que le documentaire de la BBC n'était pas destiné à un public français, car nécessitant un abonnement et une domiciliation au Royaume-Uni, la Cour de cassation a décidé d'étendre la solution dégagée par la Cour de justice de l'Union européenne à la mise à disposition de contenus dématérialisés, par voie hertzienne ou via Internet, dès lors qu'ils étaient accessibles en France. Dans le troisième arrêt, l'affaire opposait les ayants droit d'Alberto Korda, auteur de la célèbre photographie du « Che au béret et à l'étoile », à une société américaine qui proposait à la vente, sur son site Internet, des tee-shirts reproduisant ladite photographie. L'arrêt de la Cour de justice de l'Union européenne ne pouvait être directement évoqué puisque la société qui vendait l'article litigieux était américaine et non européenne. La Cour de cassation a, dans des termes proches de l'arrêt de la Cour de justice de l'Union européenne, statué que « *l'accessibilité, dans le ressort de la juridiction saisie, d'un site Internet commercialisant les produits argués de contrefaçon suffit à retenir la compétence de cette juridiction [la juridiction française], prise comme celle du lieu de la matérialisation du dommage allégué* ».

Ainsi, en matière de contrefaçon, dès lors que le site Internet proposant des objets contrefaits protégés par la législation française est accessible en France, les tribunaux français sont compétents pour en connaître. Il n'en est pas toujours aussi simple en matière délictuelle.

B) La compétence en matière contractuelle ou délictuelle

Sur Internet, compte tenu du réseau international, les acteurs d'un fait délictueux peuvent être localisés dans différents États. Le législateur communautaire a harmonisé le droit des États

membres par des règles strictes attribuant des droits individuels aux consommateurs, avec la directive 97/7/CE[2292] sur les contrats à distance et la directive 2000/31/CE[2293] sur le commerce électronique. Cette harmonisation a pour but d'inciter le consommateur à acheter à l'étranger, en lui garantissant un certain niveau de protection dans l'ensemble de l'Union européenne[2294].
L'Union européenne a réglé les conflits de compétence entre les juridictions des États membres. La disparité des localisations des acteurs est réglée dans l'Union européenne par la convention de Bruxelles[2295] et la convention de Rome[2296], remplacées par les règlements Bruxelles 1[2297], Bruxelles II[2298], Rome I[2299], Rome II [2300]et Rome III[2301], soit deux conventions et leurs protocoles remplacés par cinq règlements nécessaires pour régler la loi applicable et la compétence des juridictions, établis entre 1980 et 2016.
En matière de vente sur Internet, dans un arrêt de 2013, la Cour de justice de l'Union européenne[2302], reconnaissant le caractère international de la transaction, décide de l'application de Bruxelles I dans l'achat en Autriche, d'un séjour proposé sur le site lasteminute.com dont le siège social est en Allemagne, séjour réalisé et vendu par TUI Österreich. Le règlement prévoit que les règles de compétence doivent présenter un haut degré de prévisibilité et s'articuler autour de la compétence de principe du domicile du défendeur,

[2292] Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 *concernant la protection des consommateurs en matière de contrats à distance.*
[2293] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »).*
[2294] Josef Drexl, « Le commerce éléctronique et la protection des consommateurs », *Revue internationale de droit économique*, 2002/2 (t. XVI), pp. 405-444. URL : https://www.cairn.info/revue-internationale-de-droit-economique-2002-2-page-405.htm Op. cit.
[2295] Convention du 27 septembre 1968 *concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale*, publiée au Journal officiel nº L299, p. 32.
[2296] Convention *sur la loi applicable aux obligations contractuelles* ouverte à la signature à Rome le 19 juin 1980 (80/934/CEE) publiée au Journal officiel nº L 266 du 09/10/1980 pp. 1-19.
[2297] Règlement (CE) nº 44/2001 du Conseil du 22 décembre 2000 *concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale* publié au Journal officiel nº L 012 du 16/01/2001 pp. 1–23.
[2298] Règlement (CE) nº 2201/2003 du Conseil du 27 novembre 2003 *relatif à la compétence, la reconnaissance et l'exécution des décisions en matière matrimoniale et en matière de responsabilité parentale abrogeant le règlement (CE) nº 1347/2000* publié au Journal officiel nº L 338 du 23/12/2003 pp. 1-29
[2299] Règlement (CE) nº 593/2008 du Parlement européen et du Conseil du 17 juin 2008 *sur la loi applicable aux obligations contractuelles (Rome I),* publié au Journal officiel n° L 177/6 du 4.7.2008, pp. 6–16.
[2300] Règlement (CE) nº 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 *sur la loi applicable aux obligations non contractuelles (Rome II)*.
[2301] Règlement (UE) nº 1259/2010 du Conseil du 20 décembre 2010 *mettant en œuvre une coopération renforcée dans le domaine de la loi applicable au divorce et à la séparation de corps*, publié au JO L 343 du 29.12.2010, pp. 10-16.
[2302] Cour de justice de l'Union européenne, Arrêt du 14 novembre 2013, *Armin Maletic et Marianne Maletic contre lastminute.com Gmbh et TUI Österreich GmbH. (C-478/12)*

mais qu'en matière de contrats d'assurance, de consommation ou de travail, il est opportun de protéger la partie la plus faible, au moyen de règles de compétence plus générales. Ce même règlement précise dans son article 5 que le demandeur à l'action en responsabilité délictuelle peut saisir les tribunaux de l'état dans lequel le défendeur à son domicile ou le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire. En ce sens, la Cour de justice de l'Union européenne[2303] considère qu'en cas d'atteinte alléguée aux droits de la personnalité par un site Internet, la personne qui s'estime lésée peut saisir d'une action en responsabilité, soit les juridictions de l'État membre du lieu d'établissement de l'émetteur des contenus, soit les juridictions de l'État membre où se trouve le centre de ses intérêts pour l'intégralité du préjudice, ou en lieu et place d'une action en responsabilité au titre de l'intégralité du préjudice, introduire une action devant les juridictions de chaque État membre sur le territoire duquel le contenu en ligne est accessible ou l'a été, dans ce cas, les juridictions saisies n'étant compétentes que pour connaître du seul dommage causé sur le territoire de leur État membre.

Plus récemment, la Chambre criminelle de la Cour de cassation[2304] a rappelé les éléments attribuant la compétence au juge français lorsqu'une infraction est commise au travers d'une publication sur Internet : la compétence du juge français ne saurait être universelle et ne peut être retenue que si les pages du site les contenant sont à destination du public français, leur accessibilité par les internautes français n'étant pas suffisante pour rattacher l'infraction au territoire français, contrairement aux délits de contrefaçon.

La juridiction française a considéré que les clauses attributives de compétences exclusives à des tribunaux américains étaient abusives et donc nulles et non avenues[2305], respectant en cela le règlement Bruxelles I qui prévoit que l'action intentée par un consommateur contre l'autre partie au contrat peut être portée soit devant la juridiction de l'État membre sur lequel est domicilié cette partie, soit la juridiction du lieu où le consommateur est domicilié, et considérant que ces clauses créent un déséquilibre significatif entre les droits et obligations des parties au contrat d'adhésion[2306] et suppriment et entravent l'exercice d'actions en justice ou des voies de recours par le consommateur[2307]. De cette décision, il résulte que les juridictions étrangères sont incompétentes pour connaître de manière systématique des litiges avec les utilisateurs et, ce,

[2303] Cour de justice de l'Union européenne, Arrêt du 25 octobre 2011, affaires jointe C-509/09 et C-161/10.
[2304] Cour de cassation, Chambre criminelle, arrêt du 12 juillet 2016 nº15-86645, publié au bulletin.
[2305] Cour d'appel de Paris, Pôle 2 - Chambre 2, arrêt du 12 février 2016.
[2306] Code de la consommation, article L.132-1.
[2307] Code la consommation, article R.132-2.

même si la clause de compétence territoriale des conditions générales d'utilisation acceptées par ces derniers leur attribuerait expressément compétence[2308].

C) La compétence en matière de protection des libertés ou des personnes

En matière de protection des libertés sur Internet, la juridiction française retient deux critères : le site Internet est orienté vers le public français, par exemple pages écrites ou traduites en français ou site avec une URL possédant une extension française en .fr ou autre ; un justiciable a subi un dommage sur le territoire français. Cette approche semble respecter le principe de subsidiarité européen ou de proximité. Les attaques contre les personnes, diffamation, injure, sont de la compétence du juge judiciaire et le juge français est compétent dès que cette attaque concerne un citoyen français, un résident français ou s'est produite sur le territoire français. Les tribunaux de grande instance sont compétents pour les actions civiles pour diffamation ou injures publiques ou non publiques, verbales ou écrites[2309]. Cette compétence du tribunal de grande instance a été confirmée dans un arrêt du 5 mai 2004 de la Cour d'appel de Paris en disposant que l'émission de propos sur un site Internet constitue une communication audiovisuelle et non une communication par voie de presse.

Cette proximité des instances judiciaires, garantie en cas de délits de presse ou de délits commerciaux ou contractuels, ne semble pas retenue en cas de non-respect de la protection des données personnelles. La protection des données personnelles est de la compétence de la Commission nationale de l'informatique et des libertés[2310]. Le Règlement général sur la protection des données prévoit que l'autorité de contrôle du lieu de l'établissement permanent est compétente dans ce cas[2311]. L'autorité de l'État qui a traité initialement la réclamation n'est compétente qu'en cas de refus de traiter la réclamation de l'autorité du lieu de l'établissement principal.

[2308] Anthony Biem, *Facebook : illicéité de la clause attributive compétence du tribunal californien de ses CGU*, article publié le 28 juin 2016, at http://www.legavox.fr/blog/maitre-anthony-bem/facebook-illiceite-clause-attributive-competence-21407.htm, consulté le 6 janvier 2017.
[2309] Code de l'organisation judiciaire, Art. R211-4.
[2310] Loi n° 78/17, Art. 11.
[2311] Règlement général sur la protection des données, Art. 56.

§ 2 - Les autorités de contrôle

Les textes de protection des données à caractère personnel prévoient que les autorités de contrôle peuvent être saisies et agir en cas de non-respect des règles de protection. Dans la loi informatique et libertés promulguée le 7 janvier 1978, les dispositions pénales sont définies sans indiquer de compétence particulière de territorialité, à l'époque les délits visés sont réalisés sur le territoire français, il n'existe pas encore de réseaux concernant les particuliers, la télématique ne verra le jour qu'à partir des années 1980. Le chapitre III de la directive 95/46/CE intitulé « Recours juridictionnels, responsabilité et sanctions » prévoit que dans chaque État membre, toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis. Mais aucune compétence de territorialité n'est précisée, en effet en 1995 le réseau Internet est encore en gestation et les principaux acteurs de l'Internet n'existent pas encore. Le premier navigateur WEB est apparu en 1993.

Lors de la révision de 2004 de la loi informatique et libertés, aucune compétence territoriale des instances judiciaires ou de contrôle n'est prévue. Les autorités de contrôle doivent coopérer entre elles. Seuls les transferts de données hors de l'Union européenne peuvent être interdits, sans qu'il soit fait état de sanctions particulières.

Avec le règlement général sur la protection des données[2312], les principes de compétence territoriale sont précisés. Toute autorité de contrôle est « *compétente pour traiter une réclamation introduite auprès d'elle ou une éventuelle violation du règlement, si son objet concerne uniquement un établissement dans l'État membre dont elle relève ou affecte essentiellement des personnes concernées dans cet État membre uniquement* »[2313]. Mais si cette autorité de contrôle n'est pas l'autorité chef de file, c'est-à-dire l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement, l'autorité de contrôle saisie doit en avertir l'autorité chef de file qui peut ou non se saisir de la réclamation ou de la violation.

Chaque État membre prévoit, par la loi, que son autorité de contrôle peut porter toute violation du règlement devant les autorités judiciaires et ester en justice. Toute personne a également droit à un recours juridictionnel si elle considère que les droits conférés par le règlement ont été

[2312] 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).*
[2313] RGPD, Alinéa 2 de l'article 56.

violés du fait d'un traitement de ses données à caractère personnel. Toute action, contre un responsable du traitement ou un sous-traitant, est intentée soit devant la juridiction de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement, soit devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle[2314]. Le règlement reprend ainsi la jurisprudence existante issue du règlement Bruxelles I.

Mais le règlement s'applique lorsqu'un responsable d'un traitement dispose d'un établissement sur le territoire de l'Union européenne[2315] ou lors de la fourniture d'une offre de service payante ou non quelle que soit la localisation du traitement. L'usager est protégé dans le cadre de ce Règlement général sur la protection des données en cas de fourniture de service ou d'acte commercial, quel que soit le lieu de résidence du responsable du traitement. La notion de fourniture d'une offre de service doit être précisée, car le responsable de traitement non fournisseur d'une offre de service semblerait hors de portée légale du règlement. Ainsi, un responsable de traitement qui collationnerait des données à caractère personnel par quelque moyen que ce soit, achat de fichiers ou rapprochement de fichiers, afin d'en déduire des données à valeur ajoutée destinées à être revendues à d'autres prestataires, ne fournit pas d'offre de service pour l'usager et serait hors de portée du règlement s'il était domicilié hors de l'Union européenne sans disposer d'un établissement fixe dans l'Union européenne. La seule protection existant dans ce cas est la protection liée à la transmission des données hors de l'Union européenne, protection existante, mais qui restera difficile à mettre en œuvre, d'autant plus que des dérogations existent. Les États membres doivent compléter le règlement sur certains points laissés à leur discrétion. Il appartient donc aux États de compléter la protection apportée par la règlement, en particulier pour les activités que ne relèvent pas du champ d'application du droit de l'Union.

Sous-section 2. L'immunité apparente des États en matière de protection des données dans le cadre de leurs missions régaliennes

Dans son considérant n° 16, le Règlement général sur la protection des données précise : « *Le présent règlement ne s'applique pas à des questions de protection des libertés et droits*

[2314] Article 79 du Règlement général sur la protection des données.
[2315] RGPD, Considérant n° 23.

fondamentaux ou de libre flux des données à caractère personnel concernant des activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale. Le présent règlement ne s'applique pas au traitement des données à caractère personnel par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union ». Ainsi les États ne relèvent pas de ce règlement pour tous les problèmes de politique étrangère et de sécurité alors que les États sont des acteurs de la protection et de la sauvegarde des libertés. Mais les lois de lutte contre le terrorisme et les révélations des lanceurs d'alerte, et en particulier celles de Edward Snowden, montrent que ces États utilisent parfois les moyens des techniques numériques pour surveiller les individus, intercepter les communications, voire tenter d'agir dans les processus démocratiques d'un autre État[2316], en violation des traités internationaux et de l'autodétermination des États. Par ailleurs, avec l'instauration d'États d'urgence pour faire face et lutter contre les risques de terrorisme, certaines libertés individuelles sont suspendues par les États : violation du domicile, violation des correspondances, limitation de la liberté d'aller et venir, etc. La protection des libertés individuelles n'est plus assurée par les instances juridictionnelles judiciaires, mais par les instances juridictionnelles administratives, rompant ainsi avec le principe de la séparation des pouvoirs. Ces atteintes aux libertés sont facilitées par les techniques de la société numérique, chaque individu ne pouvant se protéger efficacement contre les risques d'intrusion dans sa vie privée.

Le règlement européen de protection des données à caractère personnel prévoit des dérogations pour les besoins des États, le seul recours des individus restant alors la saisine des cours suprêmes et au niveau européen la saisine de la Cour européenne des droits de l'homme, mais ces saisines ne sont généralement activables qu'après épuisement des recours juridictionnels traditionnels, donc nécessitent des délais longs pour les activer alors qu'une réponse immédiate est parfois nécessaire.

[2316] Barack Obama et son administration ont accusé la Russie d'avoir interférer dans les élections présidentielles de 2016 par des cyberattaques et vol de documents démocrates.

§ 1 - Le besoin d'une construction efficace pour la protection de la vie privée et des données personnelles

La protection de la vie privée en France est une protection législative depuis 1970[2317]. En 1999, le Conseil constitutionnel a déduit le principe du respect de la vie privée de l'article 2 de la Déclaration des droits de l'homme et du citoyen[2318], la hissant au niveau des droits fondamentaux protégés par la Constitution, mais sans la constitutionnaliser[2319]. La protection des données personnelles est, quant à elle, garantie par la loi informatique et libertés[2320], et à partir de 2018 par le règlement général sur la protection des données[2321].

A) Une protection prétorienne

En droit français, il est possible de saisir le Conseil constitutionnel afin de vérifier la conformité constitutionnelle d'une loi ou de certaines de ses dispositions. Cette saisine, d'office pour les lois organiques, peut être réalisée soit avant la promulgation des lois, par le Président de la République, le Premier ministre, les Présidents du Sénat et de l'Assemblée nationale ou par un ensemble de parlementaires[2322], soit après la promulgation de la loi, par tout justiciable qui soutient qu'une disposition législative porte atteinte aux droits et libertés garantis par la Constitution, et la conteste par le moyen d'une Question préjudicielle de constitutionnalité ou QPC sur renvoi du Conseil d'État ou de la Cour de cassation[2323]. Le droit au respect de la vie privée figure depuis 1970 à l'article 9 du Code civil, à l'article 8 de la Convention européenne des droits de l'homme et à l'article 7 de la Charte des droits fondamentaux de l'Union européenne. Cette protection existe dans de nombreuses Constitutions d'États européens, mais

[2317] Modification de l'article 9 du Code civil par l'article 22 de la loi n° 70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens.*
[2318] Conseil constitutionnel, Décision nº 99-416 du 23 juillet 1999, *Loi portant création d'une couverture médicale universelle*, JO du 28 juillet 1999, p. 11250, considérant nº 45.
[2319] Cf. Partie 2. Titre 2. Chapitre 1. Section 2. Sous-section 2. Le refus français de la protection directe des données personnelles et de la vie privée par la Constitution.
[2320] Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* modifiée par la Loi nº 2004-801 du 6 août 2004 déjà citée.
[2321] 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).*
[2322] Constitution, Article 61 complété par la loi constitutionnelle du 29 octobre 1974.
[2323] Constitution, Article 61-1 créé par la loi constitutionnelle du 4 février 2008.

en France, la jurisprudence du Conseil constitutionnel a comblé cette lacune et lui a conféré une valeur constitutionnelle en 1999.

Il semble que ce soit la Cour européenne des droits de l'homme qui protège in fine l'individu contre les intrusions des États au travers de sa jurisprudence concernant les surveillances, les visites domiciliaires et autres intrusions des pouvoirs publics dans la vie privée[2324]. Avant les récentes lois de lutte contre le terrorisme, la Cour européenne des droits de l'homme a eu à connaître des problèmes de conciliation de la protection de la vie privée avec la prévention des infractions pénales. La protection du respect de la vie privée, du secret des correspondances et du domicile garantie par l'article 8 de la Convention européenne des droits de l'homme, encadre les pouvoirs de la police, des douanes ou du fisc à enquêter, géolocaliser ou suivre un individu, intercepter les communications, courriers ou autres échanges privés, à pénétrer dans les domiciles. Les progrès technologiques continus ainsi que les préoccupations sécuritaires des États, dans un contexte de lutte contre le terrorisme auquel doivent faire face les pays, obligent le juge européen à continuellement actualiser ses grilles d'analyse et à rappeler les limites conventionnelles des ingérences dans la vie privée. Ces ingérences dans la vie privée doivent être encadrées par la loi[2325] et offrir des garanties contre les abus et l'arbitraire administratif[2326]. En décembre 2015[2327], la Grande chambre de la Cour a précisé les exigences relatives à une législation autorisant une interception secrète des communications effectuées à partir d'un téléphone mobile. En octobre 2015[2328], la Cour de justice de l'Union européenne a invalidé la décision 200/520/CE relative au transfert de données à caractère personnel vers les États-Unis d'Amérique arguant d'une insuffisance de protection et d'une impossibilité de recours ou de contrôle par les personnes physiques concernées. Les motifs et les dispositifs de cette décision ont pour conséquence une élévation du niveau d'exigence en matière de protection des données personnelles des citoyens européens dont les données sont transférées vers les États-Unis. Puisque la décision Safe Harbor se contentait de reprendre des dispositions de droit américain, ses considérants constituent un constat officiel de non-conformité du système de surveillance

[2324] Frédéric Sudre, Gérard Gonzalez, Katarzina Blay-Grabarczyk, Laure Milano, Hélène Surrel, « Chronique de la jurisprudence de la Cour européenne des droits de l'homme (2015) » dans *Revue du Droit public*, n°3 du 1 mai 2016, p. 1013.

[2325] Cour européenne des droits de l'homme, Arrêt du 6 septembre 1978, Affaire n° 529/71, *Klass et autres c/ Allemagne.*

[2326] Cour européenne des droits de l'homme, Arrêt du 24 avril 1990, Affaire n° 1180/95, *Kruslin c/ France*.

[2327] Cour européenne des droits de l'homme, Arrêt du 4 décembre 2015, Affaire n° 47143/06, *Roman Zakharov c/ Russie.*

[2328] Cour de justice de l'Union européenne, Arrêt du 6 octobre 2015, Affaire C-362/14, *Maximillian Schrems / Data Protection Commissioner.*

de masse mis en place aux États-Unis. Ses considérants constituent également un avertissement clair à l'égard des États membres. Les arrêts Zakharov et Szabo[2329] rendus par la Cour européenne des droits de l'homme vont dans le même sens, vers une condamnation de la surveillance de masse[2330]. En effet, alors que la Cour[2331] a estimé que les crimes terroristes entrent dans une « catégorie spéciale » justifiant une atténuation des droits au nom de la lutte contre le terrorisme, dans les arrêts Zakharov et Szabo, la Cour s'est référée à sa jurisprudence Klass c/ Allemagne, pour juger qu'une législation autorisant des mesures secrètes de surveillance affecte tous les usagers des services de télécommunications en instituant un système où toute personne peut voir ses communications interceptées sans qu'en outre aucun recours ne soit possible. Même si la base légale de telles interceptions secrètes existe, la Cour analyse la prévisibilité de telles mesures afin d'en éviter l'arbitraire administratif[2332]. Le juge de la Cour européenne des droits de l'homme a emprunté son raisonnement au juge de la Cour de justice de l'Union européenne qui, depuis l'avènement de la Charte des droits fondamentaux de l'Union européenne, est devenu le gardien de ces derniers. En s'interrogeant sur l'existence concomitante de garanties légales assurant le respect des droits des individus, la Cour fait en effet référence à la jurisprudence de la Cour de justice de l'Union européenne[2333].

Les trois décisions Schrems, Sakharov et Szabo, placent l'ensemble des cours européennes, ainsi que les cours nord-américaines, face à leur responsabilité quant au contrôle des législations instaurant ou encadrant une surveillance pouvant être considérée comme abusive. S'agissant de la condamnation de la surveillance « de masse », la décision Schrems, mise en perspective avec la décision Zakharov du 4 décembre 2015 et la décision Szabo du 12 janvier 2016, renforce en effet de manière inédite les garanties accordées aux citoyens européens contre les abus de la surveillance secrète. Elle fonde la prohibition de la surveillance de masse sur une double

[2329] Cour européenne des droits de l'homme, Arrêt du 12 janvier 2016, Affaire nº 37138/14, *Szabo et Vissy c/ Hongrie.*

[2330] Jean-Philippe Foegle, *« Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse »*, La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés, mis en ligne le 30 mars 2016, consulté le 30 septembre 2016. URL : http://revdh.revues.org/2074.

[2331] Cour européenne des droits de l'homme, Arrêt du 20 octobre 2015, Affaire nº 5201/11, *Sher et autres c/ Royaume-Uni.*

[2332] Sylvie Peyrou, *Surveillance de masse : un coup d'arrêt aux dérives de la lutte antiterroriste (CEDH, Szabo et Vissy c/ Hongrie, 12 janvier 2016)*, 30 janvier 2016, articles en ligne sur http://www.gdr-elsj.eu/2016/01/30/droits-fondamentaux/surveillance-de-masse-un-coup-darret-aux-derives-de-la-lutte-antiterroriste-cedh-szabo-et-vissy-c-hongrie-12-janvier-2016/ consulté le 12 janvier 2017.

[2333] Cour de justice de l'Union européenne, Arrêt du 8 avril 2014, Affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlande, et Kärntner Landesregierung.*

garantie tirée d'une part du droit à la protection des données personnelles et, de manière plus novatrice, sur le droit à un recours effectif.

Après ces décisions européennes, le Conseil constitutionnel a considéré qu'une surveillance de masse était non conforme à la Constitution. Alors qu'en novembre 2015, le Conseil constitutionnel avait déclaré conforme à la Constitution l'ensemble de la loi sur la surveillance internationale des communications électroniques[2334], qui remplace la seule partie censurée de la loi sur le renseignement de juillet 2015, les Sages ont considéré que les mesures de surveillance de masse et de contrôle des communications par voie hertzienne, sans exclure que puissent être interceptées des communications ou recueillies des données individualisables, portent atteinte au droit au respect de la vie privée et au secret des correspondances et les a déclarées non conformes à la Constitution[2335]. De plus, en août 2017, les Sages jugent que la surveillance électronique de l'entourage de personnes suspectées d'être en lien avec une activité terroriste viole le droit à la vie privée[2336].

Mais les lois de lutte contre le terrorisme ont toutes réduit les libertés individuelles au nom de l'efficacité de ces luttes. Si jusqu'en novembre 2017, la France connaît un état d'urgence, le gouvernement prépare une nouvelle loi pour permettre l'utilisation des techniques d'investigation autorisées par l'état d'urgence dans la loi ordinaire. Le recours au Conseil constitutionnel ou à la Cour européenne des droits de l'homme est donc la voie que l'individu pourra utiliser pour espérer sauvegarder et protéger une part de sa vie privée contre les intrusions administratives et policières.

B) Une protection administrative et réglementaire

La protection des données à caractère personnel est encadrée par la loi n° 78-17 dite informatique et libertés, modifiée en 2004 pour transposer la directive européenne 95/46/CE. En France, la Commission nationale de l'informatique et des libertés est chargée de veiller au respect de cette loi. À ce titre, elle reçoit les plaintes des personnes physiques et les demandes

[2334] Conseil constitutionnel, Décision nº 2015-722 DC du 26 novembre 2015, *Loi relative aux mesures de surveillance des communications électroniques internationales*.
[2335] Conseil constitutionnel, Décision nº 2016-590 QPC du 21 octobre 2016, *La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne]*,.
[2336] Conseil constitutionnel, Décision nº 2017-648 QPC du 4 août 2017, *L Quadrature du Net et autres [Accès administratif en temps réel aux données de connexion]*.

d'accès indirect et depuis 2014, les plaintes en refus de déréférencement. Elle a également un rôle de contrôle et de sanction.

	2016	2015	2014	2013	2012	2011	2010	2009	2008	2007
Protéger										
Plaintes	7703	7908	5825	5640	6017	5738	4821	4265	4244	4455
Demandes d'accès indirect	4379	5890	5246	4305	3682	2099	1877	2217	2516	2660
Refus de déréférencements	410	450								
Contrôler et sanctionner										
Contrôles	430	510	421	414	458	385	308	270	218	164
Mises en demeure	82	93	62	57	43	65	111	91	126	101
Sanctions financières	4	3	8	14	4	5	5	5	9	9
Avertissements	9	7	7	5	9	13	3	4	1	5

Figure 5 —La CNIL en chiffres (source Rapports annuels)

Le rôle de la CNIL est encadré par la loi. En préparation des textes réglementaires concernant les traitements automatiques des administrations et des établissements de service public, ses avis ne sont pas contraignants et sont annexés au texte lors de sa publication, que cet avis soit favorable ou défavorable. Ainsi la Commission de l'informatique et des libertés joue pleinement son rôle de protection face aux entreprises privées, mais le gouvernement s'en est partiellement exclu[2337].

Le Règlement général sur la protection des données[2338] a défini de nouveaux droits pour les personnes physiques. Dans son considérant nº 11, le règlement général sur la protection des données indique : « *Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel, ainsi que de prévoir, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations* ». Les nouveaux droits accordés par le Règlement général sur la protection des données aux personnes physiques concernant les traitements des données à caractère personnel reposent sur l'acceptation et le droit à l'oubli. Le consentement doit être volontaire, libre, éclairé et donné de façon explicite, ce qui semble exclure le consentement par défaut ou opt-out, et rappelle les principes du consentement à un contrat en droit civil, les vices du consentement y étant l'erreur, le dol et la violence[2339]. Il peut être révoqué plus simplement qu'aujourd'hui puisqu'il peut être retiré à

[2337] Cf. Partie 1. Titre 1. Chapitre 2. Section 1. Sous-section 1. § 1 -B)1) L'assouplissement de la loi informatique et libertés

[2338] 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).*

[2339] *Code civil*, art. 1130-1149.

tout moment[2340] et il doit être aussi simple de retirer son consentement que de le donner. Le consentement peut être retiré dès que le traitement effectué ne correspond plus à la cause initiale de la collecte ayant permis d'obtenir le consentement, il peut aussi être retiré par une personne qui a donné son consentement en tant que mineur et par ailleurs le consentement n'est plus donné *ad vitam aeternam*, mais pour la durée nécessaire au traitement consenti.

Outre l'obtention du consentement des personnes physiques pour collecter les données à caractère personnel, de nouvelles obligations incombent aux responsables de traitement, en particulier la sécurité du traitement a été précisée. « *Lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque* »[2341]. Cette analyse d'impact doit permettre de vérifier le respect du règlement par ledit traitement, aucun article correspondant n'existe dans la directive 95/46/CE. Le Règlement général sur la protection des données décrit le contenu de cette analyse d'impact. En France, la Commission de l'informatique et des libertés a élaboré et publié, au cours de l'été 2015, sa propre méthode pour mener l'étude d'impact sur la vie privée, sous forme de deux guides consacrés respectivement à la démarche méthodologique et à l'outillage[2342]. Ces deux documents complètent un troisième document relatif aux bonnes pratiques édité en 2012[2343].

L'incorporation dans le règlement général sur la protection des données d'une démarche méthodique va permettre au responsable de traitement de se poser les bonnes questions sur les traitements de données personnelles. Le fait de limiter l'étude aux traitements les plus à risques, malgré la difficulté à établir une liste précise, obligera les organismes à se confronter aux problématiques de la sécurité de gestion de ces traitements et les responsabilisera quant au respect du droit des personnes. Il restera aux organismes de contrôles, comme la commission

---

[2340] Règlement général sur la protection des données , art.7.

[2341] Règlement général sur la protection des données, considérant n° 84 et art. 35.

[2342] Commission nationale de l'informatique et des libertés, « *PIA, LA MÉTHODE — Étude d'impact sur la vie privée (EIVP) – Privacy Impact Assessment (PIA), Comment mener une EIVP, un PIA* », juin 2015, en ligne à http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-1-Methode.pdf, consulté le 16 septembre 2017 et « *PIA, L'OUTILLAGE - Étude d'impact sur la vie privée (EIVP) – Privacy Impact Assessment (PIA), Modèles et bases de connaissances* », juin 2015, en ligne à http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-2-Outillage.pdf, consulté le 16 septembre 2017.

[2343] Commission nationale de l'informatique et des libertés, « *Guide – Mesures pour traiter les risques sur les libertés et la vie privée* », 2012, en ligne à https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-BonnesPratiques.pdf, consulté le 16 septembre 2017.

de l'informatique et des libertés, à vérifier la sincérité de ces analyses et leur pertinence, d'autant plus que cette analyse n'est pas liée à un traitement particulier, mais à un ensemble de traitements. Il s'agit d'une avancée pour les libertés individuelles, mais cette démarche va poser des difficultés aux organismes devant l'appliquer. La réalisation d'une analyse de risques demande des compétences en sécurité pour se montrer efficace sous peine d'être superficielle ou au contraire trop lourde si elle entre dans les détails techniques.

De plus, la violation des données à caractère personnel pouvant « *causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tel 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. En conséquence, dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il le notifie à l'autorité de contrôle dans les meilleurs délais* »[2344]. Ces dispositions existaient dans le cadre de la directive 95/46/CE sans que la précision de l'obligation pour le responsable du traitement soit aussi clairement définie. Le responsable de traitement ou son sous-traitant doivent garantir la mise en œuvre de méthodes et moyens garantissant un niveau de sécurité des données approprié, cette garantie peut être fournie par une certification reconnue délivrée par un organisme[2345] ou un code de conduite approprié[2346].

Le règlement général sur la protection des données donne les grandes lignes quant à la sécurisation des traitements et des données, ces grandes lignes devront être utilisées par les autorités de contrôle pour vérifier la bonne prise en compte du règlement par les responsables de traitement et leurs sous-traitants. Ces grandes lignes étant décrites dans un règlement européen, elles seront à minima identiques et pertinentes dans tous les États membres, induisant un niveau de contrôle harmonisé. De plus, le groupe de travail de l'article 29 ou G29 édite des lignes directrices qui clarifient et illustrent d'exemples concrets le nouveau cadre juridique issu du règlement européen sur la protection des données applicable en mai 2018 dans toute

[2344] Ibid. Considérant n° 85.
[2345] Ibid. art. 43.
[2346] Ibid. art. 32-34.

l'Europe : autorité du chef de file[2347] ; portabilité[2348] ; délégué à la protection des données[2349] ; analyse d'impact[2350].

Au travers d'un Règlement général sur la protection des données et de lignes directrices, l'Union européenne se dote d'un droit souple uniformisé pour la protection des données à caractère personnel. Ce règlement prévoit qu'il pourra s'appliquer lors de l'apparition de nouvelles techniques. Les autorités de contrôle devront être vigilantes à l'émergence de ces techniques et à leurs conséquences en termes de protection de la vie privée. À court terme, la prolifération des objets connectés sera un champ d'expérimentation de ces nouvelles contraintes, sachant par ailleurs que le Règlement général sur la protection des données demande à ce que les règles d'entreprises prévoient dès la conception du traitement la protection des données (*privacy by design*), le respect de la durée de conservation, ainsi que les mesures visant à garantir la sécurité de ces données.

L'article 23 du Règlement sur la protection des données prévoit que les États peuvent par voie législative atténuer les obligations de protection des données dans certains cas si l'essence des libertés et des droits fondamentaux est respectée et que cette limitation est nécessaire et proportionnée à l'objectif recherché[2351]. Le Règlement laisse donc aux juridictions étatiques le

---

[2347] Article 29 Data Protection Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority,* 5 avril 2017, en ligne à l'URL : https://www.cnil.fr/sites/default/files/atoms/files/lead_authorityen.pdf .

[2348] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, 5 avril 2017, en ligne à l'URL : https://www.cnil.fr/sites/default/files/atoms/files/ld_portabilite_eng.pdf .

[2349] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs'),* 5 avril 2017, en ligne à l'URL : https://www.cnil.fr/sites/default/files/atoms/files/guidelines_on_dpos_5_april_2017.pdf .

[2350] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 avril 2017, en ligne à l'URL : https://www.cnil.fr/sites/default/files/atoms/files/ld_dpia_eng.pdf.

[2351] Règlement (UE) 2016/679 art. 23 Limitations : « 1. *Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, 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 :*
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 réglementées, ainsi que les enquêtes et les poursuites en la matière ;

rôle de contrôler les atténuations de la protection en utilisant les règles de proportionnalité utilisées par la Cour européenne des droits de l'homme en matière des droits fondamentaux, ou par le Conseil constitutionnel en matière de respect par les lois de la Constitution.
Ce sera donc à la Cour européenne des droits de l'homme de protéger les données à caractère personnel des personnes physiques des traitements administratifs intrusifs au nom de l'article 8 de la Convention européenne des droits de l'homme, à la Cour de justice de l'Union européenne au titre des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, ou au Conseil constitutionnel à l'interprétation de la Déclaration des droits de l'homme et du citoyen.

§ 2 - Un contrôle des dérogations étatiques par une autorité indépendante

L'État français, depuis la mise à jour de la loi n°78-17 par la loi de transposition de 2004[2352], a prévu les mécanismes lui permettant d'atténuer la protection des libertés pour la sécurité.
Avec la lutte contre le terrorisme, le gouvernement peut, en France, décider de moyens de surveillance secrets d'une personne. Dès 1991, la Commission nationale des interceptions de sécurité ou CNCIS a été instituée[2353] en tant qu'autorité administrative indépendante. Elle était chargée de veiller au respect des dispositions relatives aux interceptions de sécurité, c'est-à-dire aux écoutes téléphoniques administratives, décidées par le Premier ministre et non placées sous le contrôle d'un juge d'instruction, donc hors de toute procédure judiciaire. La loi définit le nombre d'interceptions simultanées autorisées, ainsi que la procédure d'autorisation de ces interceptions.
En 2014, Jean-Jacques Urvoas se posait la question du contrôle des politiques de renseignement par le Parlement ainsi que du contrôle de légalité et de proportionnalité des interceptions soit

h) une mission de contrôle, d'inspection ou de réglementation 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 ».
[2352] 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,* publiée au JORF n°182 du 7 août 2004 p. 14063.
[2353] Loi nº 91-646 du 10 juillet *1991 relative au secret des correspondances émises par la voie des communications électroniques* publiée au JORF nº162 du 13 juillet 1991 p. 9167.

par le juge comme en Espagne, soit par une autorité administrative indépendante[2354]. La mission confiée à la CNCIS par le législateur est une mission de contrôle de la légalité sur les demandes d'interceptions dont elle est saisie[2355]. Ce contrôle intervient en amont de l'autorisation d'interception, sous la forme d'un avis transmis au Groupement interministériel de contrôle des demandes des services habilités, la décision d'autorisation relevant du pouvoir exclusif du Premier ministre ou de ses délégués. Le contrôle de la commission s'exerce durant toute l'exploitation de l'interception. Les chiffres fournis par la Commission dans son rapport[2356] font état en 2013 de 6 182 interceptions de sécurité sollicitées, 4 213 interceptions initiales et 1 969 renouvellements, avec 812 des 4 213 demandes initiales présentées selon la procédure d'urgence absolue. Parmi les 6 182 demandes sollicitées, seules, 80 ont donné lieu à un avis défavorable, avis suivi par le Premier ministre.

En 2015, la loi relative au renseignement[2357] a remplacé la CNCIS par une nouvelle commission : la Commission nationale de contrôle des techniques de renseignement ou CNCTR dont le nombre de ses membres passe de trois à neuf. Dans son avis sur le projet de loi relatif au renseignement, le Conseil d'État avait écrit, concernant la CNCTR : « *Dès lors que cette commission constitue l'une des garanties essentielles entourant la mise en œuvre des techniques de renseignement énumérées dans le projet de loi, sa composition, ses missions et ses règles déontologiques doivent être définies de manière à garantir l'effectivité de son contrôle. Aussi le Conseil d'État a-t-il jugé préférable de retenir un texte prévoyant une composition resserrée de cinq personnalités indépendantes et disponibles et une présidence à temps plein et permettant une présence suffisante, parmi les membres de la commission comme au sein de ses services, de personnes possédant des qualifications idoines en matière de réseaux de communications et de protection des données personnelles* »[2358]. Cet avis n'a pas été suivi d'effet, la loi prévoyant neuf membres dans la commission : deux députés et deux sénateurs, deux membres du Conseil d'État, deux magistrats de la Cour de cassation et une personnalité qualifiée « pour sa connaissance en matière de communications électroniques », mais les députés et les sénateurs ne siègent qu'en formation plénière. Ainsi, cette commission peut siéger

[2354] Jean-Jacques Urvoas, député, membre de la CNCIS, lors du colloque « Numérique, renseignement et vie privée : de nouveaux défis pour le droit » tenu le 22 mai 2014 au Sénat.
[2355] Commission nationale de contrôle des interceptions de sécurité, *22e rapport d'activité* 2013-2014, p. 71.
[2356] Ibid, p. 84.
[2357] Loi nº 2015-912 du 24 juillet 2015 *relative au renseignement*, publiée au JORF nº0171 du 26 juillet 2015 p. 12735.
[2358] Avis consultatif nº 389 754 du 12 mars 2015, rendu public et disponible à l'URL : http://www.conseil-etat.fr/Actualites/Communiques/Renseignement consulté le 12 janvier 2017.

à cinq membres et émettre ses avis hors du contrôle des parlementaires, membres de cette commission. En effet, les demandes sont transmises au président ou à défaut à l'un des membres issus du Conseil d'État ou de la Cour de cassation pour rendre un avis dans un délai de vingt-quatre heures, ou soixante-douze heures après en avoir informé le Premier ministre, si la demande est examinée en commission restreinte ou en commission plénière, seule instance ou siègent les représentants des parlementaires. Par ailleurs, en cas de non-respect des délais, un avis est considéré comme rendu favorable. De plus, en cas de nécessité absolue, le Premier ministre peut décider de l'interception sans solliciter l'avis préalable de la Commission, marquant ainsi un recul par rapport aux avis de la CNCIS.

Pour respecter la jurisprudence récente de la Cour de justice de l'Union européenne[2359] et de la Cour européenne des droits de l'homme, il semble que l'institution d'un véritable contrôle d'une autorité administrative indépendante soit à rétablir. Pour la Cour, « *l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* » et « *il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiée, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* ».

De plus, certaines dispositions prévues par l'état d'urgence se retrouvent dans la législation générale permettant au gouvernement de sortir de l'état d'urgence tout en en conservant des possibilités, dérogatoires aux droits de l'homme, de surveillance[2360]. Ces dispositions ont été votées par le Parlement[2361] et n'ont pas été soumises au Conseil constitutionnel. La nécessité

[2359] Cour de justice de l'Union européenne (grande chambre), *Affaires jointes C-203/15 et C-698/15 Tele2 Sverige AB c/ Post- och telestyrelsen et Secretary of State for the Home Department c/ Messieurs X, Y, et Z*, Arrêt du 21 décembre 2016.

[2360] Vincent Grégoire, « L'état d'urgence n'est pas l'état normal de l'État de droit », *Sens-Dessous*, 2017/1 (n° 19), pp. 63-74. URL : https://www.cairn.info/revue-sens-dessous-2017-1-page-63.htm consulté le 5 février 2018.

[2361] Loi n° 2017-1510 du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme* publiée au JORF n°0255 du 31 octobre 2017.

d'une autorité réellement indépendante, ayant le pouvoir de s'autosaisir des textes restreignant la protection des libertés, semble nécessaire pour une protection effective des citoyens. La surveillance électronique d'une personne physique est difficilement décelable et permet de remonter dans certaines activités sur Internet ou téléphoniques sur plusieurs mois en cas de détection d'un acte suspect.

De plus, la dérive actuelle liée à la lutte contre le terrorisme modifie la responsabilité de la défense des libertés personnelles, la transférant du juge judiciaire au juge administratif, en contradiction avec la Constitution et son article 66[2362]. Le juge administratif donne au gouvernement un avis sur les projets de loi, dans le cas de la lutte contre le terrorisme ou la criminalité, cet avis peut porter sur des moyens prévus sur la compétence donnée à ce juge. La séparation des pouvoirs[2363], chère à Montesquieu, peut sembler ne plus être garantie puisque, dans ce cadre, le Conseil d'État est à la fois juge, en donnant son avis, et partie, en tant que compétent pour juger les recours liés à l'application de la loi. Toutefois, le Conseil constitutionnel reste seul juge de la constitutionnalité des lois[2364], dès qu'il en est saisi.

[2362] Cf. Partie 1. Titre 2. Chapitre 1. Section 1. Sous-section 2. § 1 - Les restrictions administratives à la protection de la vie privée.

[2363] En droit français, la séparation des pouvoirs n'est pas évoquée dans le texte ni le préambule de la Constitution de 1958. Seul l'article 16 de la Déclaration des droits de l'homme et du citoyen en fait état : « *toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution* ».

[2364] Agnès Roblot-Troizier, « Un concept moderne : séparation des pouvoirs et contrôle de la loi », *Pouvoirs*, 2012/4 (n° 143), pp. 89-103. URL : https://www.cairn.info/revue-pouvoirs-2012-4-page-89.htm consulté le 5 février 2018.

Conclusion

Dans une société mondialisée et numérique, la défense des libertés demeure une lutte permanente. Le numérique est neutre, tout comme le réseau Internet[2365]. Cette neutralité est importante pour la diffusion des connaissances[2366]. Les opérateurs ont le pouvoir de surveiller, de choisir, de prioriser les contenus qui sont diffusés ou reçus par les citoyens-internautes. Ils ont le pouvoir de faire disparaître une plateforme des réseaux. Ils ont aussi un pouvoir absolu sur les données qui circulent sur leurs réseaux, et peuvent même les détruire, les empêcher de circuler. La neutralité signifie que chacun dispose des mêmes droits et ressources pour naviguer sur le réseau, bande passante, droits d'accès aux sites ou d'exister. Toutefois, l'accès aux sites peut être contrôlé soit par une décision administrative rendant certains sites inaccessibles sur le territoire français pour des raisons de sécurité et d'intérêt général, soit par la volonté des propriétaires du site qui souhaitent limiter l'accès aux seuls abonnés. La tentation peut être forte pour un fournisseur d'accès à Internet de limiter la bande passante pour des raisons mercantiles, en favorisant l'accès aux sites payants et dégradant l'accès aux autres sites, et ce d'autant plus que certains sites sont très consommateurs de bande passante[2367]. Le principe d'égalité d'accès aux différents sites est rompu aux États-Unis d'Amérique avec l'abandon du principe de neutralité des réseaux par la FCC[2368], par une simple décision administrative restaurant officiellement la « liberté d'Internet ». Corolaire de cette décision, la liberté d'accès aux sites n'est plus assurée, l'égalité entre les sites est rompue. La liberté d'information, d'expression se trouve aliénée par des contraintes commerciales et monétaires, alors qu'elle est protégée par le premier amendement. Au sein de l'Union européenne, ce principe de neutralité du réseau est inscrit dans la réglementation[2369]. En France, il est garanti par la loi pour une République

[2365] Benjamin Bayart, Agnès de Cornulier, « La neutralité du net », *Pouvoirs*, 2018/1 (N° 164), pp. 127-136. URL : https://www.cairn.info/revue-pouvoirs-2018-1-page-127.htm consulté le 5 février 2018.
[2366] Francesca Musiani, Hervé Le Crosnier, « La neutralité de l'Internet, un enjeu pour la documentation à l'ère du numérique », *I2D – Information, données & documents*, 2017/1 (Volume 54), pp. 7-9. URL : https://www.cairn.info/revue-i2d-information-donnees-et-documents-2017-1-page-7.htm consulté le 5 février 2018.
[2367] Aux États-Unis d'Amérique, NETFLIX représente plus d'un tiers (35 %) du trafic Internet (source Sandvine).
[2368] Federal Communications Commission, *Restoring Internet Freedom*, DA/FCC-17-166, January 4, 2018.
[2369] 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.*

numérique[2370]. Cet exemple montre que le contrôle et la gouvernance du réseau Internet demeurent un outil de domination[2371]. Il fait l'objet d'une importante bibliographie[2372].

Mais la société, avec le développement rapide et universel des techniques numériques, connaît actuellement une révolution dont les conséquences sont de nature à modifier les paradigmes actuels[2373] issus de la révolution industrielle[2374]. La société va se transformer comme elle s'est transformée au XIXe siècle, lors de la révolution industrielle. Cette révolution qui est en cours va modifier notre vision des libertés publiques et des libertés privées. La législation mise en place depuis la Révolution française pour définir et protéger nos libertés doit évoluer face à l'apport et l'emprise des nouvelles techniques et leurs conséquences sur ces libertés.

Les libertés d'expression et de communication deviennent universelles, tout individu connecté à Internet peut diffuser des informations, fausses ou non vérifiées, pouvant mettre en cause une personne physique, une personne morale ou un État. Les lois sur la presse encadrent ces libertés et elles ont été adaptées aux nouvelles techniques, mais l'incidence sur l'image d'une personne peut être importante et avoir des conséquences très rapidement, avant même que la personne visée n'en soit informée. Ces techniques peuvent être utilisées pour diffuser des messages de haine et inciter aux actes terroristes. Si la loi sur la presse permet de lutter contre de tels abus sur les sites traditionnels, de tels messages peuvent être diffusés sur les réseaux sociaux, Twitter en particulier, sans que leurs auteurs anonymes ne puissent être poursuivis[2375].

La liberté de pensée et de religion interdit de limiter ces échanges, mais considérant les risques pour les personnes ou pour la sécurité publique, les sites permettant ou diffusant des incitations au terrorisme peuvent être neutralisés et rendus inaccessibles à partir du territoire français. Mais selon que ces sites attentent à l'intégrité d'une personne physique ou à la sécurité publique, ce

---

[2370] Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique*, art. 40-41.

[2371] Francesca Musiani, Valérie Schafer, Hervé Le Crosnier, « Net Neutrality as an Internet Governance Issue: The Globalization of an American-Born Debate », *Revue française d'études américaines*, 2012/4 (n° 134), pp. 47-63. URL : https://www.cairn.info/revue-francaise-d-etudes-americaines-2012-4-page-47.htm consulté le 5 février 2018.

[2372] « The Internet and its Governance: *A General Bibliography* », *Revue française d'études américaines*, 2012/4 (n° 134), pp. 20-24. URL : https://www.cairn.info/revue-francaise-d-etudes-americaines-2012-4-page-20.htm consultée le 5 février 2018.

[2373] Christine Marsan, « Chapitre 2. Le changement de paradigme », dans *Réussir le changement. Comment sortir des blocages individuels et collectifs ?*Louvain-la-Neuve, De Boeck Supérieur, « Manager RH », 2008, pp. 43-74. URL : https://www.cairn.info/reussir-le-changement--9782804156282-page-43.htm consulté le 5 février 2018.

[2374] Rémy Rieffel, *Révolution numérique, révolution culturelle ?* Gallimard, 2014, pp.13-14.

[2375] Marie-Andrée Weiss, « Liberté d'expression sur les réseaux sociaux. Regards croisés États-Unis/Europe », *Documentaliste-Sciences de l'Information*, 2014/3 (Vol. 51), pp. 20-22. URL : https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2014-3-page-20.htm consulté le 5 février 2018.

sera soit la loi contre les sectes ou loi About-Picard, soit les lois de lutte contre le terrorisme qui seront actionnées pour sanctionner ces faits.

La numérisation de la société peut attenter aux libertés de création, d'entreprendre au travers de sites particuliers mettant en relation rapide un demandeur et un offreur de services. Ces sites créent de fait une concurrence asymétrique et inégalitaire avec les professions traditionnelles. En effet, si les sites marchands en ligne modifient les habitudes d'achat des consommateurs et créent une pression concurrentielle[2376], les échanges de services gratuits ou payants échappent en partie aux contraintes, normes et taxes auxquelles les entreprises sont soumises. Le développement de ces sites, créant une véritable économie parallèle, pose problème, car ils utilisent des possibilités offertes marginalement aux particuliers souhaitant offrir ces prestations[2377]. Ainsi, de marginale, l'offre parallèle devient véritable concurrence.

Si les libertés publiques sont affectées par la numérisation de la société, les libertés individuelles le sont également. Les facteurs de risque pour la liberté individuelle des individus sont triples : risques liés aux intrusions des États sous prétexte de garantir la sécurité publique ou l'égalité devant l'impôt ; risques dus au détournement criminel ou mercantile des données à caractère personnel générées par les activités quotidiennes des individus ; risques dus au comportement des individus eux-mêmes qui dévoilent des informations qui auraient dû rester secrètes ou dont la diffusion aurait dû rester limitée à une sphère intime. La prolifération des données induit une surveillance permanente des individus[2378].

Ce dernier risque ne peut pas faire l'objet d'une loi de protection, mais il doit être dénoncé[2379] et une information ou une sensibilisation des individus doit être réalisée dès l'école primaire avec l'apprentissage de l'écriture et de la lecture. La Commission nationale de l'informatique

---

[2376] Autorité de la concurrence, Avis 12-A-20 du 18 septembre 2012 relatif au fonctionnement concurrentiel du commerce électronique, URL : http://www.autoritedelaconcurrence.fr/pdf/avis/12a20.pdf consulté le 5 février 2018.
Mercanti-Guérin Maria, Flores Laurent, « Analyse de l'univers concurrentiel des sites de vente en ligne : une approche par le *Web Analytics* », *Vie & sciences de l'entreprise*, 2012/2 (N° 191 - 192), pp. 96-117. URL : https://www.cairn.info/revue-vie-et-sciences-de-l-entreprise-2012-2-page-96.htm consulté le 5 février 2016.

[2377] Alexis Gendry, « Uber, Airbnb, Netflix… : quelle réglementation ? », 18 mai 2007, *Contrepoints,* URL : https://www.contrepoints.org/2017/05/18/289685-uber-airbnb-netflix-reglementation consulté le 5 février 2018.

[2378] François-Bernard Huyghe, « Téléphonie mobile : capter la vie numérique des autres », *Hermès, La Revue*, 2009/1 (n° 53), pp. 79-84. URL : https://www.cairn.info/revue-hermes-la-revue-2009-1-page-79.htm consulté le 7 février 2018.
Tristan Nitot, *surveillance:// Les libertés au défi du numérique ; comprendre et agir,* septembre 2016, C&F éditions.

[2379] Fabrice Rochelandet, « IV. Les comportements en matière de vie privée sont-ils rationnels ? », dans *Économie des données personnelles et de la vie privée.* Paris, La Découverte, « Repères », 2010, pp. 67-87. URL : https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-67.htm consulté le 5 février 2018.

et des libertés émet des guides et des fiches pratiques[2380] vers les individus, mais ces guides ne connaissent pas une diffusion généralisée et ne font jamais l'objet de messages dans les médias, alors que de nombreux messages mettent en garde les individus sur les risques de contagion d'une épidémie saisonnière de grippe, durant la période de la campagne de vaccination annuelle, plusieurs fois par jour. Bien que certains individus puissent aller jusqu'au suicide face à une révélation sur Internet de certains faits, ou qu'une révélation puisse avoir de graves répercussions sur le devenir d'une personne, la protection de la vie privée n'a pas atteint le niveau de sensibilisation d'une mortalité importante liée à une épidémie de grippe. Une information des jeunes dès l'école primaire semble nécessaire, pour être efficace et utile, cette sensibilisation nécessite une formation des éducateurs.

Le risque lié à l'exploitation des données à caractère personnel par des entreprises à but mercantile reste lié à la valeur économique de ces données[2381]. Internet est entré dans une ère de collecte de données personnelles avec l'avènement des réseaux sociaux numériques et l'offre de services en ligne dont la valeur d'usage dépend de la production de données par les individus eux-mêmes. Une prolifération des données divulguées de manière volontaire par les individus est liée à la contrepartie des services et des contenus qu'ils utilisent[2382]. Leur protection est actuellement prise en compte par la loi et les règlements de l'Union européenne. Le Règlement général sur la protection des données modifie profondément la responsabilité des entreprises, mais il nécessite des moyens de contrôle harmonisés et opérationnels[2383]. La vigilance reste d'actualité ; les principales sociétés œuvrant sur Internet sont en majorité des sociétés extérieures à l'espace européen, et tentent soit de se protéger au travers de législations moins protectrices pour les individus au travers de conditions particulières d'utilisation contenant des clauses jugées abusives, donc nulles et non avenues en droit, soit d'influencer les Parlements par un lobbying efficace afin d'atténuer les conséquences de la loi. Les organes de contrôle

[2380] Accessibles à l'URL : https://www.cnil.fr/fr/mediatheque, ou https://www.cnil.fr/fr/maitriser-mes-donnees .

[2381] Fabrice Rochelandet, « III. Exploitation des données personnelles, vie privée et externalités », dans *Économie des données personnelles et de la vie privée.* Paris, La Découverte, « Repères », 2010, pp. 38-66. URL : https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-38.htm consulté le 5 février 2018.

[2382] Grazia Cecere, Fabrice Le Guel, Fabrice Rochelandet, « Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique », Réseaux, 2015/1 (n° 189), pp. 77-101. URL : https://www.cairn.info/revue-reseaux-2015-1-page-77.htm consulté le 5 février 2018.

[2383] Compte-tenu de la responsabilité donnée aux entreprises au travers de l'autocontrôle, des audits de certification ou des enquêtes devront être mises en place, comme il en existe pour les certifications industrielles ou commerciales.

comme la CNIL doivent rester vigilants et obtenir les moyens de leur action[2384]. Au travers de règles strictes, même si elles sont souples, elles ont à s'assurer que la réglementation européenne est respectée. Le nouveau règlement général sur la protection des données à caractère personnel leur donne plus de moyens de sanction, ce pouvoir de sanction, incluant la possibilité d'astreintes, doit être utilisé. Les organes comme la Commission nationale pour l'informatique et les libertés doivent pouvoir disposer de pouvoir d'investigation pour rechercher les fraudes sans nécessiter le dépôt formel d'une plainte. La protection des données à caractère personnel doit faire l'objet d'une législation stricte et respectée, et elle devrait être déclarée d'ordre public et considérée comme loi de police[2385].

Enfin, le dernier risque et non le moindre provient des États. Au nom de la lutte contre le terrorisme, ces derniers cherchent à surveiller une majorité d'individus afin de les contrôler et de préserver la sécurité publique[2386]. Cette surveillance, nourrie du risque réel de terrorisme, doit être contrôlée au niveau local par la loi et des organismes indépendants de contrôle. Mais les gouvernements ayant le contrôle de l'édification des lois et de leur promulgation peuvent atténuer, de par la loi ou la publication de décrets, directives et circulaires, les contraintes associées aux intrusions administratives dans la vie privée des personnes physiques. Le contrôle des lois et leur respect par les États sont réalisés par l'intermédiaire des juridictions nationales[2387] ou européennes[2388]. La Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme deviennent ainsi les garants des libertés et droits fondamentaux dans la société numérique et depuis quelques années leurs arrêts, décisions et avis concernent cette protection des droits fondamentaux dans une société de plus en plus numérique.

[2384] Comme le souligne la Commission nationale de l'informatique et des libertés, le Règlement général sur la protection des données « dote le régulateur de pouvoirs nécessaires à l'exercice de ses missions », mais que les moyens d'assumer ces pouvoirs ne semblent pas être accordés (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))

[2385] Conseil d'État, *Étude annuelle 2014 du Conseil d'État - Le numérique et les droits fondamentaux*, p. 24.

[2386] Mariel Garrigos-Kerjan, « La tendance sécuritaire de la lutte contre le terrorisme », *Archives de politique criminelle*, 2006/1 (n° 28), pp. 187-213. URL : https://www.cairn.info/revue-archives-de-politique-criminelle-2006-1-page-187.htm consulté le 5 février 2018.

[2387] Didier Ribes, « Atteintes publiques et atteintes privées au droit au respect de la vie privée dans la jurisprudence du Conseil constitutionnel », *Les Nouveaux Cahiers du Conseil constitutionnel*, 2015/3 (N° 48), pp. 35-46. URL : https://www.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2015-3-page-35.htm consulté le 5 février 2018.

[2388] Christophe Bigot, « La protection de la vie privée par la Cour européenne des droits de l'homme », *LEGICOM*, 2009/2 (N° 43), pp. 43-49. URL : https://www.cairn.info/revue-legicom-2009-2-page-43.htm consulté le 7 février 2018.

Comme le disait en 1998[2389], le Conseil d'État, Internet n'est pas une zone de non-droit, le droit doit s'y appliquer. La difficulté provient de la progression rapide des techniques et de la mondialisation des acteurs. Si nous voulons préserver et protéger nos libertés, il nous faudra rester vigilants, refuser de bénéficier des nouveaux services proposés, services qui deviennent rapidement addictifs, car apparemment gratuits. L'industrie du tabac a ainsi longtemps caché les aspects addictifs et dangereux du tabagisme. Aujourd'hui, ces aspects sont reconnus et la lutte contre le tabagisme est ouverte dans plusieurs États, malgré le lobbying puissant des industriels du secteur. Il faut que la population et les autorités prennent conscience des risques pour nos libertés liés à l'universalité du numérique afin de lutter efficacement contre les abus du numérique. Les outils de droit existent, il faut les utiliser et les harmoniser entre les États afin de réellement les rendre plus efficaces et éviter l'évitement par l'intermédiaire d'îlots moins protecteurs des libertés et la création de zones territoriales de « dumping du droit ». L'« optimisation numérique » doit être combattue en évitant des disparités dans la protection des données à caractère personnel, le Règlement général sur la protection des données, en unifiant les législations des États membres, est une première étape vers une protection universelle dans l'espace de l'Union européenne.

Dans un État démocratique, les techniques numériques peuvent permettre de contrôler la liberté d'expression en rendant inaccessibles certains sites appelant au terrorisme ou facilitant certains crimes, mais ces mêmes techniques peuvent être utilisées par un État moins démocratique pour limiter la liberté d'expression, en fermant systématiquement l'accès aux sites d'opposition au régime en place. Ces techniques permettent d'intercepter les communications, de surveiller les déplacements des personnes physiques. Ces techniques peuvent être utilisées légalement pour lutter contre le terrorisme, mais elles peuvent aussi être utilisées par un État pour une surveillance de masse non ciblée comme l'a révélé Edward Snowden. Les lois mises en place pour lutter contre le terrorisme limitent les libertés fondamentales des individus au nom de l'intérêt général et du bien public. Contrôlées dans leur application, elles peuvent cohabiter avec un régime démocratique. Ces lois, votées démocratiquement, pourraient lors d'un changement de régime exécutif autoritaire, être utilisées pour museler toute opposition, tout en bénéficiant de cette « onction démocratique ». Hitler est arrivé au pouvoir démocratiquement, il n'a imposé son régime dictatorial et génocidaire qu'après son arrivée au pouvoir, même si son programme

[2389] Jean-François Théry, Isabelle Falque Pierrotin, *Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998*, Conseil d'État. Section du rapport et des études, publiée à la documentation française, décembre 1998.

figurait dans *Mein Kampf*[2390]. Que n'aurait-il pu faire avec les techniques numériques actuelles et les lois « démocratiques » ?[2391] Dans nos sociétés démocratiques, les garde-fous des dérives numériques restent les organes de contrôle dont la suprématie internationale est reconnue par les États, la remise en cause de ces organes ouvrirait la « boîte de Pandore »[2392]. Nul ne peut imaginer ce que nos sociétés numériques deviendraient si elles étaient soumises à des dictatures.
Dans la société numérique, tout individu est objet de surveillance. Cette surveillance peut être présentée comme une aide à la décision : choisir un bon restaurant de proximité ; inciter à un achat ciblé, déduit des centres d'intérêt détectés par les actes enregistrés ou la navigation sur le réseau ; etc. Cette surveillance peut être utilisée pour définir le tarif d'une assurance en fonction des risques détectés : santé ; activité physique ; antécédents de toute sorte ; etc. Elle peut aussi être utilisée pour établir le profil complet d'une personne, profil réalisé en corrélant l'ensemble des informations disponibles en ligne, profil utilisé pour valider ou rejeter une embauche, ou justifier un licenciement.
Dans une société épiant chaque geste, chaque déplacement, chaque écrit d'un individu, que reste-t-il du libre arbitre et des libertés ? Se sachant surveillé, l'individu va tenter de se cacher ou va s'autocensurer dans ses actions. La liberté surveillée n'est plus la liberté.
Si la numérisation de la société a une forte valeur économique, elle peut être un vecteur de consolidation de certaines libertés publiques, mais elle peut réduire la protection de la liberté de l'individu, de sa vie privée et familiale[2393]. Le règlement général sur la protection des

[2390] Adolf Hitler, *Mein Kampf*, Eher-Verlag, 1925.
[2391] Jean Foyer, lors de la première séance de discussion à l'Assemblée nationale de la loi informatique et libertés, constatait : « *En cette heure, je pense avec effroi à ce qu'aurait été le sort de la Résistance si la police allemande et la Milice de Vichy avaient disposé de moyens informatiques modernes. Elles n'auraient pas attendu le printemps de 1944 pour démanteler les réseaux ! Et aucun texte ne les aurait retenues ».* (Assemblée nationale, 1re séance du 4 octobre 1977, Journal officiel p. 5784, URL : http://archives.assemblee-nationale.fr/5/cri/1977-1978-ordinaire1/002.pdf).
[2392] Dans la mythologie grecque, Prométhée vola le feu aux Dieux pour le donner aux hommes. Pour se venger, Zeus ordonna à Vulcain de créer une femme faite de terre et d'eau. Elle reçut des Dieux de nombreux dons : beauté, flatterie, amabilité, adresse, grâce, intelligence, mais aussi l'art de la tromperie et de la séduction. Ils lui donnèrent le nom de Pandore, qui en grec signifie « doté de tous les dons ». Elle fut ensuite envoyée chez Prométhée. Épiméthée, le frère de celui-ci, se laissa séduire et finit par l'épouser. Le jour de leur mariage, Pandore reçoit une jarre dans laquelle se trouvaient tous les maux de l'humanité, avec interdiction de l'ouvrir. Par curiosité, elle ne respecta pas la condition et tous les maux s'évadèrent pour se répandre sur la Terre. Seule l'espérance resta au fond du récipient, ne permettant donc même pas aux hommes de supporter les malheurs qui s'abattaient sur eux. C'est à partir de ce mythe qu'est née l'expression « boîte de Pandore », qui symbolise la cause d'une catastrophe. (source « Expressions », *L'Internaute*, URL : http://www.linternaute.com/expression/langue-francaise/80/la-boite-de-pandore/).
[2393] Dans l'étude d'impact du Projet de loi relatif à la protection des données personnelles du 12 décembre 2017, il est précisé dès l'introduction générale : « *La protection des données à caractère personnel revêt une dimension particulière depuis l'avènement de l'ère du numérique. Le partage et la collecte de telles données connaissent en effet un développement spectaculaire. C'est par ce biais que les nouvelles technologies transforment aujourd'hui profondément notre l'économie et les rapports sociaux. Dans le même temps, la protection des données à caractère*

données prend en compte l'évolution des techniques survenues au XXI[e] siècle. Cette protection généralisée dans l'Union européenne doit rester efficace face à l'intrusion grandissante des objets connectés. Pour suivre l'évolution rapide de la technique, des mécanismes de droit souple doivent être mis à disposition des organes de contrôle[2394].

Mais l'individu reste la personne centrale de cette protection. Il doit être conscient des risques embarqués dans les techniques numériques qui pour améliorer certains aspects de sa vie, vont obtenir des informations sur ses habitudes, sa santé, ses sentiments, ses désirs. Aucun texte, même le plus contraignant ne peut obliger un individu à divulguer ces informations. Pour être efficaces, les textes doivent être accompagnés d'action de sensibilisation[2395]. Des lanceurs d'alerte sont nécessaires pour mettre en garde les individus contre certaines pratiques industrielles et commerciales, voir politiques. Dans une émission de télévision[2396], les personnes physiques, interrogées sur la reconnaissance faciale mise en place par le gouvernement chinois pour toutes les caméras de vidéosurveillance, ne voyaient aucun problème concernant leur vie privée dans cette surveillance de masse.

Les techniques modernes ne sont pas utilisées que pour surveiller les individus. Elles permettent une meilleure diffusion de l'information et des connaissances, que ce soit avec l'open data et les données administratives, ou avec la masse d'information disponible sur Internet et accessible en quelques secondes en tout point du globe. Mais l'éducation est primordiale pour savoir utiliser cette source de connaissance. L'individu doit savoir que tout n'est pas vérité sur Internet et qu'il y circule autant de fausses que de vraies informations. Il devra apprendre à recouper les sources et les qualifier pour forger sa propre connaissance.

---

personnel constitue un motif de préoccupation croissante chez nos concitoyens ; étant entendu qu'une telle préoccupation est largement partagée en Europe. En 2017, 85% des Français se disent ainsi préoccupés par la protection de leurs données personnelles en général, soit une augmentation de quatre points par rapport à 2014. Une question qui suscite encore plus d'inquiétude dès lors qu'il s'agit de la protection des données sur Internet : 90% des personnes interrogées se disent préoccupés pour leurs données mises en ligne, ce qui représente cinq points de progression par rapport à en 2014 » (Introduction générale, alinéa 2.).

[2394] Dans l'étude d'impact du Projet de loi relatif à la protection des données personnelles précitée, parmi les missions de la Commission nationale de l'informatique et des libertés figue l'avis, l'approbation ou la création d'instruments de « droit souple ». « *Le droit souple est nécessaire en matière de protection des données à caractère personnel pour trois raisons : compte tenu des limites même de la norme générale dans un environnement en pleine mutation ; le traitement des données personnelles est de plus en plus déterritorialisé ; la protection des données personnelles est en train de changer de paradigme* » (« 1.2.2.1. Sur les mesures de droit souple », pp.20-21).

[2395] Cet aspect du rôle de la CNIL est également précisé dans l'étude d'impact précitée.

[2396] Reportage sur la prolifération des caméras de surveillance en Chine, avec reconnaissance faciale dans un journal télévisé de France 2 en début février 2018.

Si la société numérique peut restreindre les libertés publiques et individuelles, il appartient aux individus de réagir et aux gouvernements de les protéger. Protection double par des lois et règlements clairs, non ambigus et dont l'efficacité peut être contrôlée, et protection par l'éducation pour prévenir des habitudes néfastes sur Internet et pour trier les fausses informations enfermant l'individu, des informations contrôlées permettant un réel épanouissement de l'homme.

Des scandales comme celui de Facebook et Cambridge Analytica peuvent permettre de sensibiliser les individus aux risques collatéraux des réseaux sociaux, ou faire disparaître des géants. Dans un monde en perpétuelle évolution, les géants d'Internet grandissent et meurent. Qui se souvient du moteur de recherche Alta Vista qui existait avant Google, ou de la suite 123 supplantée par Office ?

La protection peut venir de la loi et des règlements, mais elle viendra aussi de l'éducation de tous, dès le plus jeune âge. Elle viendra d'abord de l'éducation, la loi ne sera alors qu'un garde-fou.

Bibliographie

Ouvrages

Ouvrages sur les libertés publiques

Boyer Georges, Couzinet Paul, Bréthe de la Gressaye Jean, Hauriou André, Maury Jacques, *Les garanties des libertés individuelles*, Librairie du recueil Sirey, 1933.

Cruet Jean, *Étude juridique de l'arbitraire gouvernemental et administratif – Des cas où l'autorité gouvernementale et administrative n'est pas tenue, sous des sanctions efficaces, de respecter les droits individuels et la légalité*, Librairie nouvelle de droit et de jurisprudence, Arthur Rousseau Éditeur, 1906.

Ducourteix Albert*, La liberté individuelle et le droit d'arrestation*, Imprimerie et librairie générale de jurisprudence, Marchal et Billard, Imprimeurs-Éditeurs, 1879.

Favoreu Louis, Gaïa Patrick, Ghevontian Richard et autres, *Droit des libertés fondamentales*, Précis Dalloz, 5e édition, 2009.

Lavenue Jean-Jacques, *E-révolutions et révolutions : Résistances et résiliences,* Septentrion, 2016.

Lepage Agathe, *Libertés et droits fondamentaux à l'épreuve de l'Internet*, Litec, Groupe Lexis Nexis, 2003.

Letteron Roseline, *Libertés publiques,* Précis Dalloz, 9e édition, 2012.

Mathieu Bertrand, Verpeaux Michel, *Contentieux constitutionnel des droits fondamentaux,* LGDJ, 2002.

Mourgeon Jacques, Théron Jean-Pierre, *Les libertés publiques*, Presses universitaires de France, 1985.

Pontier Jean-Marie, *Droits fondamentaux et libertés publiques*, Hachette, 5e édition, 2014.

Prélot Pierre-Henri, *Droit des libertés fondamentales*, Hachette, 2e édition, 2010.

Rivero Jean, Moutouh Hugues, *Libertés publiques*, tome 1, Presses universitaires de France, 9e édition, 2003.

Rivero Jean, Moutouh Hugues, *Libertés publiques, Tome II,* Presses Universitaires de France, 7e édition mise à jour, 2003.

Wachsmann Patrick, *Libertés Publiques*, Cours Dalloz, 8e édition 2017.

Ouvrages de droit (autres)

Ameller Michel, *L'Assemblée nationale*, Paris, PUF (Que sais-je ?), 1994.

Bensoussan Alain, *Code informatique, fichiers et libertés,* Larcier, 2014.

Féral-Schuhl Christiane, *Cyberdroit Le droit à l'épreuve du numérique*, Dalloz, 6e édition, 2010.

Gohin Olivier, *Droit constitutionnel*, LexisNexis, 3e édition 2016.

Laffaire Marie-Laure, *Protection des données à caractère personnel*, éd. d'organisations, 2005.

Loussouarn Yvon, Bourel Pierre, Vareilles-Sommières (de) Pascal, *Droit international privé*, Dalloz 9e édition, 2007.

Molfessis Nicolas, *Le Conseil constitutionnel et le droit privé*, LGDJ, 1997.

Rey Bénédicte**,** *La vie privée à l'ère du numérique*, Lavoisier, 2012.

Roques-Bonnet Marie-Charlotte, *Le droit peut-il ignorer la révolution numérique ?* Michalon éditions, 2010.

Weaver Russell L., *From Gutenberg to the Internet: Free speech, advancing technology, and the implications for democracy*, Carolina Academic Press, 2013.

Weaver Russell L., *Understanding the first amendment*, LexisNexis, 5th edition, 2014.

Autres ouvrages

Ariès Philippe, Duby Georges, *Histoire de la vie privée, Tome 2 De l'Europe féodale à la Renaissance*, Collection L'Univers historique, Éditions du Seuil, 1 988

Arpagian Nicolas, *La cybersécurité,* Presses universitaires de France, août 2010.

Arpagian Nicolas, *La cyberguerre, la guerre numérique a commencé*, Vuibert, mars 2009.

Babinet Gilles, *L'ère numérique, un nouvel âge de l'humanité. Cinq mutations qui vont bouleverser notre vie*. Le Passeur, 2014.

Bellanger Pierre**,** *La souveraineté numérique*, Stock, 2014.

Clarke Richard A. and Knake Robert K., *Cyberwar, the next threat to national security and what to do about it*, Harper Collins Publisher, 2010.

Colin Nicolas, Verdier Henri, *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2012

Compiègne Isabelle, *La société numérique en question(s)*, Éditions Sciences Humaines, 2011.

Diderot Denis, *Supplément au voyage de Bougainville, ou Dialogue entre A. et B. sur l'inconvénient d'attacher des idées morales à certaines actions physiques qui n'en comportent pas*, Correspondance littéraire, 1772.

Frayssinet Jean, *Informatique, fichiers et libertés*, éd., Litec, Paris, 1 992.

Frayssinet Jean, *L'Internet et la protection juridique des données personnelles. L'Internet et le droit* ? Victoires, 2001.

Hitler Adolf, *Mein Kampf,* Eher-Verlag, 18 juillet 1925.

Hobbes Thomas, *Leviathan or the matter, form and power of a common wealth ecclesiastical and civil,* Andrew Crooke, 1651

Kant Emmanuel, *Critique de la raison pure*, 1781, Nouvelle traduction française avec notes par A. Tremesaygues et B. Pacaud, Félix Alcan éditeur, 1905.

Kant Emmanuel, *Fondements de la métaphysique des mœurs*, 1785, Librairie philosophique de Ladrange, 1848.

Kant Emmanuel, « Qu'est-ce que s'orienter dans la pensée ? (VII) », *Mélanges de logique*, traduit par J. Tissot, Librairie Philosophique de Ladrange, 1862.

Klüver Heike, *Lobbying in the European Union : Interest Groups, Lobbying Coalitions, and Policy change*, Oxford, Oxford University Press, 2013.

Liang Qiao, Xiangsui Wang, *La guerre hors limites*, Rivages poche / Petite bibliothèque, 1999, traduit en français en 2003.

Locke John, *Questions concerning the law of nature*, 1664, Cornell University Press, 1990.

Locke John, *Lettre sur la tolérance,* 1689, Éditions ressources, 1980.

Locke John, *Two treatises of government*, 1 689, Black Swan, dated 1690.

Lucas André, Deveze Jean, Frayssinet Jean, *Droit de l'informatique et de l'Internet*, Presses universitaires de France, 2001.

Mayer Jean-François, *Internet et religion*, Religioscope, 2008.

Mayer-Schönberger Victor, Cukier Kenneh**,** *Big Data. La révolution des données est en marche*, Robert Laffont, 2014.

Montesquieu, *De l'esprit des lois,* 1748, Gallimard, 1995.

Mossé Claude, *Les institutions grecques à l'époque classique*, Armand Colin, 1967.

Nirot Tristan, *surveillance:// Les libertés au défi du numérique : comprendre et agir*, C&F éditions, 2016

Nissenbaum Helen, *Privacy in Context : Technology, Policy, and the Integrity of Social Life,* Stanford University Press, 2010.

Orwell George, *1984*, Editions Secker and Warburg, 1949, version française : Éditions Gallimard, 1950.

Paine Thomas, *Common sense addressed to the inhabitants of America*, R. Bell, 1776.

Rieffel Rémy, *Révolution numérique, révolution culturelle ?,* Gallimard, 2014.

Rousseau Jean-Jacques, *Du contrat social ou Principes du droit politique*, Marc-Michel Ray, 1762.

Rousseau Jean-Jacques, *Lettres écrites de la montagne*, Marc-Michel Ray, 1764.

Sillard Benoît**,** *Maîtres ou esclaves du numérique ?,* Éditions Eyrolles, 2011.

Sonnac Nathalie, Gabszewicz Jean, *L'Industrie des médias à l'ère numérique*, La Découverte, 3e éd., 2013.

Strowel Alain**,** *Quand Google défie le droit,* De Boeck-Larcier, 2011.

Tocqueville (de) Alexis, *De la démocratie en Amérique*, 1835-1840, Flammarion, 2008.

Türk Alex, *La vie privée en péril : des citoyens sous contrôle*, Paris O. Jacob, 2011.

Voltaire, *Traité sur la tolérance, A l'occasion de la mort de Jean Calas*, s.n. Genève*,* 1763.

Voltaire, *Dictionnaire philosophique portatif*, s.n. Londres, 1764.

Voltaire, *Collection des lettres sur les Miracles à Genève et à Neufchâtel*, s.n. Neufchâtel, 1767.

Thèses, mémoires

Thèses

Al Kaabi Juma. *La gestion de la menace terroriste. Le système français de prévention et de répression*, Université Jean Moulin (Lyon 3), 2017.

Barbosa Delgado Francisco, *Les limites de la marge nationale d'appréciation et la liberté d'expression : étude comparée de la jurisprudence de la Cour européenne et de la Cour interaméricaine des droits de l'homme*, Université de Nantes, 2010.

Beye Pape Moussa, *Libéralisme et exception : l'État de droit et le système onusien de sécurité collective à l'épreuve du jihadisme international*, Université Panthéon-Assas, 2016.

Cousson Anne, *Droits de l'homme au Royaume-Uni entre 1998 et 2010 : entre politique nationale et droit international*, Université Sorbonne Paris Cité, 2016.

Hadjipavlou Elena, Big Data, *Surveillance et Confiance : La question de la traçabilité dans le milieu aéroportuaire,* Université Côte d'Azur, 2016.

Jin Minjung, *Le journalisme amateur à l'ère d'Internet : illusion populaire ou nouvel espace de liberté d'expression ?* Université Panthéon-Assas, 2012.

Osman Ziad, *Les approches juridiques de la lutte antiterroriste : les nouvelles extensions du droit international, la coopération européenne et les règlementations du monde arabe*, Université Lille 2, 2011.

Roudier Karine, *Le contrôle de constitutionnalité de la législation antiterroriste. Étude comparée des expériences espagnole, française et italienne*, Université de Toulon, 2011.

Zwolinska Monika, *Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international*, Université Nice Sophia Antipolis, 2015.

Mémoires

Auger Delphine, *Biométrie : l'équilibre entre « liberté individuelle » et promesse sécuritaire serait-il impossible ?* Université Paris I – Panthéon Sorbonne, septembre 2005.

Aza Fabrice Emmanuel, *Le chiffrement : peut-il être élevé au statut de droit constitutionnellement protégé ?* Université Paris I – Panthéon Sorbonne, juin 2017.

Barreto Gwendoline, *Le transfert des données personnelles des passagers aériens d'Europe vers les États-Unis,* Université Paris I – Panthéon Sorbonne, 2006.

Capely Alix, *Objets connectés et protection des données personnelles*, Université Paris I – Panthéon Sorbonne, juin 2015.

Carsenti Serge, *La liberté d'expression sur Internet*, Université Paris I – Panthéon Sorbonne, juin 2003.

Garniel Rémi, *La double finalité du fichier STIC, quelles garanties pour les libertés individuelles ?* Université Paris I – Panthéon Sorbonne, septembre 2009.

Graindorge Thomas, *Le droit de la cryptologie et ses conséquences*, Université Paris I – Panthéon Sorbonne, juin 2015.

Koczorowski Eva, *L'atteinte à la réputation sur Internet : problématique juridique et stratégies de communication en ligne*, Université Paris I – Panthéon Sorbonne, 2009.

Kus Cindy, *Le gouvernement des algorithmes – Un encadrement juridique complexe bouleversant les concepts du droit*, Université Paris I – Panthéon Sorbonne, juin 2016.

Maksene Sarah, *Les enjeux de l'adoption d'une directive Passenger Name Record*, Université Paris I – Panthéon Sorbonne, juin 2015.

Moreau Delattre Ségolène, *Échange d'informations et protection des données à caractère personnel dans le cadre de la coopération policière en Europe*, Université Paris I – Panthéon Sorbonne, septembre 2015.

Parey Nathalie, *Constitution et droit du numérique*, Université Paris I – Panthéon Sorbonne, juin 2015.

Rouquet Léa, *L'adaptation de l'environnement juridique européen et national à la transformation numérique*, Université Paris I – Panthéon Sorbonne, juin 2016.

Rapports, Études

La France face au terrorisme, Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme, La Documentation française, 2006.

Étude d'impact - Projet de loi relatif au renseignement, Assemblée nationale, 18 mars 2015

Administrateur général des données, *Les données au service de la transformation de l'action publique*, *Rapport au Premier ministre sur la gouvernance de la donnée 2015*, décembre 2015.

Babinet Gilles, *Pour un « new Deal » numérique,* Étude février 2013, Institut Montaigne.

Batho Delphine, Bénisti Jacques Alain, *Rapport d'information sur les fichiers de police,* N° 1548, enregistré à la Présidence de l'Assemblée nationale le 24 mars 2009.

Batho Delphine, Bénisti Jacques Alain, *Rapport d'information déposé en application de l'article 145-8 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police*, N° 4513, enregistré à la Présidence de l'Assemblée nationale le 21 décembre 2011.

Bloche Patrick, Verchère Patrice, *Rapport d'information sur les droits de l'individu dans la révolution numérique*, N° 3560, enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011.

Braibant Guy, *Données personnelles et société de l'information*, Rapport au Premier ministre sur la transposition en droit français de la directive no 95/46, le 3 mars 1998.

Chenot Bernard, Aydalot Maurice, Tricot Bernard, Catala Pierre, *Rapport de la Commission informatique et liberté,* La documentation française, 1975.

Ciotti Éric, *Rapport 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 (n° 1697), d'orientation et de programmation pour la performance de la sécurité intérieure*, n° 2271 enregistré à la Présidence de l'Assemblée nationale le 27 janvier 2010.

Comité consultatif pour une révision de la Constitution, présidé par le doyen Georges Vedel, *Rapport au Président de la République, Propositions pour une révision de la Constitution*, La Documentation française, 15 février 1993.

Comité de réflexion sur le préambule de la Constitution, présidé par Mme Simone Veil, *Redécouvrir le Préambule de la Constitution, Rapport au Président de la République*, La Documentation française, Décembre 2008.

Commission nationale de contrôle des interceptions de sécurité, *22e rapport d'activité 2013-2014,* La documentation française, janvier 2015.

Commission nationale de l'informatique et des libertés, *Rapport annuel 2004*, La Documentation française, 2005.

Commission nationale de l'informatique et des libertés, *30e rapport d'activité 2010*, Direction de l'information légale et administrative, 2010.

Commission nationale de l'informatique et des libertés, *31ème rapport d'activité 2011*, Direction de l'information légale et administrative, 2011.

Commission nationale de l'informatique et des libertés, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur*, Rapport adopté par la CNIL réunie en séance plénière le 13 juin 2013.

Conseil d'État, *Étude annuelle 2013 - Le Droit souple*, Les rapports du Conseil d'État, La Documentation française, mai 2013.

Conseil d'État, *Étude annuelle 2014 - Le numérique et les droits fondamentaux*, Les rapports du Conseil d'État, La Documentation française, septembre 2014.

Détraigne Yves, Escoffier Anne-Marie, *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information,* Rapport d'information nº 441 (2008-2009) fait au nom de la commission des lois, déposé le 27 mai 2009, Sénat.

Détraigne Yves, Escoffier Anne-Marie, *Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique*, enregistrée à la Présidence du Sénat le 6 novembre 2009.

Diard Éric, Dray Julien, *Rapport d'information sur la mise en application de la loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers,* N° 683, enregistré le 5 février 2008 à la Présidence de l'Assemblée nationale.

Gorichon Jean-Claude, Varenne Dominique, Sportiche Maurice, *Internet et le respect de la vie privée, Rapport nº IV-1,9- 2008* – Ministère de l'économie, de l'industrie et de l'emploi*,* Mars 2009.

Groupe de travail « article 29 » sur la protection des données, *Avis 5/2009 sur les réseaux sociaux,* adopté le 12 juin 2009.

Groupe de travail présidé par Alain Bauer, *Fichiers de police et de gendarmerie - Comment améliorer leur contrôle et leur gestion ?* La documentation française, décembre 2006.

Groupe de travail présidé par Alain Bauer, *Mieux contrôler les fichiers de police pour protéger les libertés*, La documentation française, décembre 2008.

Gest Alain, Guyard Jacques, *Rapport fait au nom de la commission d'enquête sur les sectes,* Nº 2468, Enregistré à la Présidence de l'Assemblée nationale le 22 décembre 1995.

EC3, *First Year Report*, 2014.

Joulaud Marc, *Avis enregistré à la Présidence de l'Assemblée nationale le 22 juillet 2009 et présenté au nom de la commission de la défense nationale et des forces armées sur le projet de loi (nº 1697) d'orientation et de programmation pour la performance de la sécurité intérieure*, Nº 1861 22 juillet 2009.

Le Forum des droits sur Internet, *Rapport d'activité année 2009*, La documentation française, 2010.

Mazeaud Pierre, *La lutte contre le terrorisme dans la jurisprudence du Conseil constitutionnel*, Visite à la cour suprême du Canada, 24 au 26 avril 2006.

Mission interministérielle de vigilance et de lutte contre les dérives sectaires, *Internet : l'amplification du risque de dérives sectaires, Rapport au Premier ministre*, La documentation française, *2008*.

Mission interministérielle de vigilance et de lutte contre les dérives sectaires, *« Le risque sectaire et Internet », Rapport au Premier ministre, 2013-2014*, La Documentation française, avril 2015.

National Intelligence Council, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution,* ICA 2017-01D, January 6, 2017.

Nora Simon, Minc Alain, *L'informatisation de la société - Rapport à M. le Président de la République*, janvier 1978, La Documentation française.

Observatoire national de la délinquance et des réponses pénales*, La criminalité en France*, *Rapport de l'Observatoire national de la délinquance et des réponses pénales 2011*, CNRS éditions, Novembre 2011.

Organisation du Traité de l'Atlantique Nord (OTAN), *Rapport annuel 2012 du secrétaire général*, 1er février 2013.

Parlement européen, *Rapport sur les implications juridiques et institutionnelles du recours aux instruments juridiques non contraignants (soft law)* (2007/2028 (INI)) A6-0259/2007 du 28 juin 2007.

Pillet François, Soilihi Thani Mohamed, *L'équilibre de la loi du 29 juillet 1881 sur la liberté de la presse à l'épreuve d'Internet,* Rapport d'information N° 767 (2015-2016) enregistré à la Présidence du Sénat le 6 juillet 2016.

Pietrasanta Sébastien, *Rapport 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 (nº 2110), renforçant les dispositions relatives à la lutte contre le terrorisme,* N° 2173, enregistré à la Présidence de l'Assemblée nationale le 22 juillet 2014.

Vivien Alain, *Les sectes en France, expression de la liberté morale ou facteurs de manipulations ?* Rapport au Premier ministre, La Documentation française, Février 1983.

Secrétariat des Nations unis*, « Dans une liberté plus grande », Rapport du secrétaire général des Nations unies,* mars 2005.

Théry Jean-François, Falque Pierrotin Isabelle, *Internet et les réseaux numériques : étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998,* Conseil d'État. Section du rapport et des études, la Documentation française, décembre 1998.

Urvoas Jean-Jacques, *Rapport fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la république, après engagement de la procédure accélérée, sur le projet de loi (nº 2669) relatif au renseignement*, nº 2697, enregistré à la Présidence de l'Assemblée nationale le 2 avril 2015.

Viennois Maurice, Boucher Julien, *Propriété littéraire et artistique et libertés individuelles dans l'environnement numérique*, Commission sur la propriété littéraire et artistique et les libertés individuelles, 2 mars 2004.

Articles

Revues à comité de lecture

« La consécration par la CJUE d'un droit de déréférencement par les moteurs de recherche : principe, exceptions et mise en œuvre », *LEGICOM* 2015/1 (nº 54), pp. 89-105.

« Loppsi II : un patchwork répressif », *Plein droit* 2011/1 (n° 88), pp. 1-2.

Ader Basile, « La protection de la vie privée en droit positif français », *LEGICOM* 1999/4 (nº 20), pp. 5-8.

Ader Basile, « La loi de 1881, réceptacle naturel de toutes les infractions de « publication », depuis la presse et l'imprimerie jusqu'à Internet », *LEGICOM* 2016/2 (nº 57), pp. 19-21.

Aglietta Michel, Scialom Laurence, « Les risques de la monnaie électronique », *L'Économie politique* 2002/2 (nº 14), pp. 82-95.

Agostinelli Xavier, « Diffamation, injure et provocation à la discrimination raciale », *LEGICOM* 2002/3 (nº 28), pp. 47-60.

Algan Yann *et al.*, « Administration numérique », *Notes du conseil d'analyse économique* 2016/7 (nº 34), pp. 1-12.

Alix Julie, « Fascicule 20 : Terrorisme », *Jurisclasseur,* 15 mars 2011, mis à jour 30 juin 2014.

Allaert François-André *et al.*, « Les enjeux de la sécurité des objets connectés et applications de santé », *Journal de gestion et d'économie médicales* 2016/5 (Vol. 34), pp. 311-319.

Allard Laurence, « Dans quel monde voulons-nous être connectés ? Transhumanisme vs companionism », *Nectart* 2016/2 (nº 3), pp. 125-132.

Amsellem David, Limonier Kevin, « L'utilisation des outils cartographiques dans la sûreté des déplacements d'affaires », *Sécurité et stratégie* 2014/4 (19), pp. 5-12.

Anciaux Arnaud, Farchy Joëlle et Méadel Cécile, « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle* [En ligne], 158 | 2e trimestre 2017, mis en ligne le 15 juin 2019. URL : http://journals.openedition.org/rei/6540.

Antin (d') Olivier, Brossollet Luc, « Le domaine de la vie privée et sa délimitation jurisprudentielle », *LEGICOM* 1999/4 (nº 20), pp. 9-19.

Armand Gilles, « Que reste-t-il de la protection constitutionnelle de la liberté individuelle ? », *Revue française de droit constitutionnel* 2006/1 (nº 65), pp. 37-72.

Astier Stéphane, « Vers une régulation éthique de l'Internet : les défis d'une gouvernance mondiale », *Revue Internationale des Sciences Administratives* 2005/1 (Vol. 71), pp. 143-161.

Auvret Patrick, « L'équilibre entre la liberté et le respect de la vie privée selon la Cour européenne des droits de l'homme », *Gazette du Palais nº 102*, 12 avril 2005, p. 2.

Auvret Patrick, « Le Conseil de l'Europe et la protection de la vie privée en matière de presse », *LEGICOM* 1999/4 (nº 20), pp. 97-114.

Barbe Lionel *et al.*, « Un enjeu de société », *Documentaliste-Sciences de l'Information* 2010/1 (Vol. 47), pp. 56-67.

Barbry Éric, « Le droit des marques à l'épreuve de l'Internet », *LEGICOM* 1997/3 (nº 15), pp. 91-109.

Barbry Éric, « Cohérences et incohérences des législations », *Hermès, La Revue* 2009/1 (nº 53), pp. 145-151.

Barendt Éric, « La protection de la vie privée en Angleterre », *LEGICOM* 1999/4 (nº 20), pp. 115-120.

Barreau Catherine, « Le marché unique numérique et la régulation des données personnelles », *Annales des Mines - Réalités industrielles* 2016/3 (Août 2016), pp. 37-41.

Battisti Michèle, « La réutilisation des données publiques : un enjeu majeur pour la société européenne de l'information », *Documentaliste-Sciences de l'Information* 2004/6 (Vol. 41), pp. 349-355.

Bauman Zygmunt, Bigo Didier, Esteves Paulo, Guild Elspeth, Jabri Vivienne, Lyon David et Walker R. B. J. (Rob), « Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance », *Cultures & Conflits* [En ligne], 98 | été 2015, mis en ligne le 15 octobre 2016, consulté le 03 décembre 2015. URL : http://conflits.revues.org/19033 .

Bayart Benjamin, Cornulier (de) Agnès « La neutralité du net », *Pouvoirs* 2018/1 (N°164), pp. 127-136.

Beignier Bernard, « Vie privée et vie publique », *Légipresse, septembre 1995*, pp. 67-74.

Ben Henda Mokhtar, « Internet dans la révolution tunisienne », *Hermès, La Revue*, 2011/1 (n° 59), pp. 159-160.

Ben Henda Mokhtar, Hudrisier Henri, « Penser, classer, apprendre et communiquer. Normalisation et nouveaux modes de classification du savoir », *Hermès, La Revue*, 2013/2 (n° 66), pp. 160-166.

Benhamou Bernard, « L'Internet des objets. Défis technologiques, économiques et politiques », *Esprit* 2009/3 (Mars/avril), pp. 137-150.

Bensamoun Alexandra, Zolynski Célia, « *Cloud computing* et *big data*. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux* 2015/1 (nº 189), pp. 103-121.

Bensoussan Alain, « Vie privée – vie personnelle », *Gazette du Palais* nº 22, 22 janvier 2011, p. 3.

Bellanger Pierre, « Les données personnelles : une question de souveraineté », *Le Débat* 2015/1 (n° 183), pp. 14-25.

Berguig Matthieu, Coupez François, « Faut-il réellement craindre l'Open data pour la protection **de nos données personnelles ? », *LEGICOM* 2016/1 (nº 56), pp. 15-24.**

Bernier Claire, « Le RGPD en 4 leçons pour les retardataires », *Sécurité et stratégie* 2017/4 (28), pp. 85-90.

Berthoud Gérald, « L'horizon d'une surveillance omniprésente ? », *Revue européenne des sciences sociales*, 2002/2 (XL), p. 11.

Biétry Franck, » Les syndicats à l'heure des réseaux », *Revue française de gestion*, 4/2005 (nº 157), pp. 79-102.

Bigo Didier *et al.*, « Introduction. Les libertés sacrifiées au nom de la sécurité ? », *in* Didier Bigo *et al.*, *Au nom du 11 septembre...* , La Découverte « Cahiers libres », 2008, pp. 5-10.

Bigot Christophe, « Exposé introductif : les spécificités de la loi de 1881 concernant tant le régime de responsabilité en cascade que celui des règles dérogatoires de procédure et de prescription », *LEGICOM* 2006/1 (nº 35), pp. 21-23.

Bigot Christophe, « La protection de la vie privée par la Cour européenne des droits de l'homme », *LEGICOM* 2009/2 (nº 43), pp. 43-49.

Blanchetier Philippe, « Point de départ du délai de prescription des délits de presse sur Internet : l'occasion manquée », *Semaine juridique (J.C.P.)*, 2004 (29), pp. 1335-1336.

Blay-Grabarczyk Katarzyna, « Conventionnalité de la condamnation d'un exploitant de portail d'actualités sur Internet en raison de commentaires injurieux », *La Semaine Juridique Edition Générale* nº 27, 6 Juillet 2015, 798.

Blondiaux Loïc, « Démocratie locale et participation citoyenne : la promesse et le piège », *Mouvements* 2001/5 (nº 18), pp. 44-51.

Blöss Thierry, « L'individualisme dans la vie privée mythe ou réalité ? », *Revue Projet* 2002/3 (nº 271), pp. 71-80.

Bonnet Julien, Roblot-Troizier Agnès, « Droits fondamentaux et libertés publiques », *Les Nouveaux Cahiers du Conseil constitutionnel* 2016/3 (nº 52), pp. 71-91.

Boudou Guillaume, « Autopsie de la décision du Conseil constitutionnel du 16 juillet 1971 sur la liberté d'association », *Revue française de droit constitutionnel* 2014/1 (nº 97), pp. 5-120.

Bouhadana Irène, « Constitution et droit à l'oubli numérique : état des lieux et perspectives », Bouhadana Irène, Gilles William (sous la direction.), *Vie privée, vie publique à l'ère du numérique, Revue de l'institut du monde et du développement*, Les éditions IMODEV, mai 2011, pp.13-20.

Bouhadana Irène, "The right of access to public information: an analysis of international conventions", Bouhadana Irène, Gilles William (sous la direction.), *International Journal of Open Government,* Vol. (2015), pp. 1-10, URL: http://ojs.imodev.org/index.php/RIGO/article/view/1/31.

Bouhadana Irène, Gilles William, « Le brouillage des frontières entre vie privée et vie publique à l'ère du numérique », Bouhadana Irène, Gilles William (sous la direction.), *Vie privée, vie publique à l'ère du numérique*, *Revue de l'institut du monde et du développement*, Les éditions IMODEV, mai 2011, pp.5-6.

Boure Robert, Bousquet Franck, « Enjeux, jeux et usages d'une pétition politique en ligne. "La pétition Vauzelle" », *Réseaux* 2010/6 (n° 164), p. 127-159.

Boussois Sébastien, « Lutte contre le terrorisme : la Belgique, maillon faible ? », *Politique étrangère* 2017/4 (Hiver), pp. 173-185.

Boustany Joumana, « Accès et réutilisation des données publiques. État des lieux en France », *Les Cahiers du numérique* 2013/1 (Vol. 9), pp. 21-37.

Broussolle Damien, « Le commerce des services, un commerce en trompe-l'œil ? Une analyse fondée sur le point de vue de Hill », *Revue économique* 2012/6 (Vol. 63), pp. 1145-1177.

Bruna Yann, « La déconnexion aux technologies de géolocalisation. Une épreuve qui n'est pas à la portée de tous », *Réseaux* 2014/4 (n° 186), pp. 141-161.

Cadoux Louise, Tabatoni Pierre, « Internet et protection de la vie privée », *Commentaire* 2000/1 (Numéro 89), pp. 57-66.

Cailleba Patrice, « Lanceur d'alerte et silence organisationnel », *Revue internationale de psychosociologie et de gestion des comportements organisationnels* 2017/56 (Vol. XXIII), pp. 309-334.

Camus Colombe, « La lutte contre le terrorisme dans les démocraties occidentales : État de droit et exceptionnalisme », *Revue internationale et stratégique* 2007/2 (nº 66), pp. 9-24.

Canas Sophie, « L'influence de la fondamentalisation du droit au respect de la vie privée sur la mise en œuvre de l'article 9 du code civil », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015/3 (nº 48), pp. 47-58.

Carcassonne Guy, « Les interdits et la liberté d'expression », *Les Nouveaux Cahiers du Conseil constitutionnel* 2012/3 (nº 36), pp. 55-65.

Cardon Dominique, « Réseaux sociaux de l'Internet », *Communications* 2011/1 (nº 88).

Cassuto Thomas, « Vie privée, vie publique et cybercriminalité », *Sécurité globale* 2008/4 (nº 6), pp. 45-66.

Cauvin Emmanuel, « Courrier électronique », *Médium* 2009/1 (nº18), pp. 50-59.

Cazals (de) Marie, « La saisine du Conseil économique, social et environnemental par voie de pétition citoyenne : gage d'une Ve République "plus démocratique" ? », *Revue française de droit constitutionnel* 2010/2 (n° 82), p. 289-312.

Cecere Grazia *et al.*, « Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique », *Réseaux* 2015/1 (nº 189), pp. 77-101.

Chappey Jean-Luc, « Philippe Grateau, Les Cahiers de doléances, une relecture culturelle, Rennes, Presses Universitaires de Rennes, 2001, 383 p., 22 € », *Revue d'histoire moderne et contemporaine* 2005/2 (nº 52-2), pp. 213-213.

Chardel Pierre-Antoine et al., « Un USA Patriot Act à la française ? Ou les inquiétantes résonances d'une loi », *Lignes 2015/3* (nº 48), pp. 105-124.

Chilstein David, « Le droit de la communication à l'épreuve du droit pénal international », *LEGICOM* 2014/1 (nº 52), pp. 51-58.

Chobeaux François, « La légalité n'excuse pas tout. Le projet de prévention de la délinquance », *VST - Vie sociale et traitements* 2004/4 (nº 84), pp. 35-37.

Cohen Dany, « Le juge, gardien des libertés ? », *Pouvoirs* 2009/3 (nº 130), pp. 113-125.

Coll Sami, « La vie privée comme outil de gouvernance. Surveiller et fidéliser le lien marchand », *Les Cahiers du numérique* 2014/ (Vol. 10), pp. 45-68.

Cornu Marie, « Le statut des archives publiques dans le discours d'ouverture des données : de la formalisation d'un droit d'accès à l'émergence d'un droit d'exploiter la donnée », *LEGICOM* 2016/1 (nº 56), pp. 41-49.

Débet Anne, « La protection des données personnelles, point de vue du droit privé », *Revue du droit public nº 1*, 1er janvier 2016, p. 17.

Derieux Emmanuel, « Vie privée et données personnelles — Droit à la protection et "droit à l'oubli" face à la liberté d'expression », *Les nouveaux Cahiers du Conseil constitutionnel* nº 48, 1er juin 2016, p. 21.

Dorsner-Dolivet Annick, « Loi sur les sectes », *Recueil Dalloz* 2002, p.1086.

Doucet Ghislaine, « Terrorisme : définition, juridiction pénale internationale et victimes », *Revue internationale de droit pénal* 2005/3 (Vol. 76), pp. 251-273.

Dusollier Séverine, « Les mesures techniques dans la directive sur le droit d'auteur dans la société de l'information : un délicat compromis », *LEGICOM* 2001/2 (nº 25), pp. 75-86.

Drexl Josef, « Le commerce éléctronique et la protection des consommateurs », *Revue internationale de droit économique* 2002/2 (t. XVI), pp. 405-444.

Dubois Jean-Pierre, « Nos droits face aux « *big data* » : quels enjeux, quels risques, quelles garanties ? », *Après-demain* 2016/1 (nº 37, NF), pp. 6-9.

Duplessis Isabelle, « Le vertige et la *Soft Law* : réactions doctrinales en droit international », *Revue québécoise de droit international (Hors-série),* 2009, pp.245-268.

Ertzscheid Olivier, « L'homme, un document comme les autres », *Hermès, La Revue* 2009/1 (nº 53), pp. 33-40.

Falque-Pierrotin Isabelle, « La Constitution et l'Internet », *Les Nouveaux Cahiers du Conseil constitutionnel* 2012/3 (nº 36), pp. 31-44.

Favro Karine, « Introduction », *LEGICOM* 2016/1 (N° 56), pp. 3-12.

Ferragu Gilles, La France et ses « siècles de plomb », *Confluences Méditerranée* 2017/3 (N° 102), pp. 13-28.

Fondeur Yannick, « Internet, recrutement et recherche d'emploi : une introduction », *Revue de l'IRES* Nº 52 - 2006/3.

Fortier Charles, « Vers un régime juridique de la diffamation propre aux universitaires », 6 novembre 2017, *AJDA* 2017, p.2097.

Frayssinet Jean, « La régulation de la protection des données personnelles », *LEGICOM* 2009/1 (nº 42), pp. 5-9.

Fried Charles, « Liberté d'expression, liberté de pensée, libertés hors du droit ? Deux décisions controversées de la Cour suprême des États-Unis », *Les Nouveaux Cahiers du Conseil constitutionnel* 2012/3 (nº 36), pp. 157-164.

Fulli-Lemaire Samuel, « Affaire PIP : quelques réflexions sur les aspects de droit international privé », *Revue internationale de droit économique* 2015/1 (t. XXIX), pp. 99-122.

Gamba Fiorenza, « Rituels postmodernes d'immortalité : les cimetières virtuels comme technologie de la mémoire vivante », *Sociétés* 2007/3 (nº 97), pp. 109-123.

Gautron Virginie, Monniaux David, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », *Archives de politique criminelle* 2016/1 (nº 38), p. 123-135.

Gilles William, "From the right to transparency to the right to open government in digital era. A French approach", Bouhadana Irène, Gilles William (sous la direction.), *International Journal of Open Government,* Vol. 2 (2015), pp. 11-26, URL: http://ojs.imodev.org/index.php/RIGO/article/view/4/34.

Gitton Antoine, « La copie privée numérique : vers une licence d'édition privée », *LEGICOM* 2001/2 (nº 25), pp. 61-74.

Goëta Samuel, Mabi Clément, « L'open data peut-il (encore) servir les citoyens ? », *Mouvements*, 2014/3 (n° 79), pp. 81-91.

Gomez Mejia Gustavo, « De quoi le "nuage" est-il le nom ? Le statut des supports face aux régimes du *cloud computing* », *Communication & langages* 2014/4 (nº 182), pp. 77-93.

Gonzalez-Quijano Yves, « Internet, le "Printemps arabe" et la dévaluation du cyberactivisme arabe », *Égypte/Monde arabe* [En ligne], Troisième série, Évolution des systèmes médiatiques après les révoltes arabes, mis en ligne le 25 mars 2015, consulté le 26 avril 2017. URL : http://ema.revues.org/3400 .

Granjon Fabien, « De quelques pathologies sociales de l'individualité numérique. Exposition de soi et autoréification sur les sites de réseaux sociaux », *Réseaux* 2011/3 (nº 167), pp. 75-103.

Granjon Fabien, « Du (dé) contrôle de l'exposition de soi sur les sites de réseaux sociaux », *Les Cahiers du numérique* 2014/ (Vol. 10), pp. 19-44.

Grégoire Stéphane, « Le statut de l'adresse IP : Conséquences sur les mécanismes de constat, d'avertissement et de sanction du peer to peer envisagés par les accords de l'Élysée et le projet de loi « Création et Internet » », *LEGICOM* 2009/2 (nº 43), pp. 103-107.

Grégoire Vincent, « L'état d'urgence n'est pas l'état normal de l'État de droit », *Sens-Dessous* 2017/1 (nº 19), pp. 63-74.

Gridel Jean-Pierre, « Protection de la vie privée, rupture ou continuité ? », *Gazette du Palais* nº 139, 19 mai 2007, p. 4.

Guiraudon Virginie, « La coopération transatlantique après le 11 septembre : », *Critique internationale* 2005/3 (nº 28), pp. 21-35.

Halpérin Jean-Louis, « Diffamation, vie publique et vie privée en France de 1 789 à 1 944 », *Droit et Cultures*, 2013/1, 65, p. 149.

Halpérin Jean-Louis, « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015/3 (nº 48), pp. 59-68.

Harchoux Antoine, « Le droit au respect de la vie privée a Royaume-Uni », *Gazette du Palais* nº 264, p.11, 21 septembre 2006.

Heymann-Doat Arlette, « L'état d'urgence, un régime juridique d'exception pour lutter contre le terrorisme ? », *Archives de politique criminelle* 2016/1 (nº 38), pp. 59-74.

Huet Jérôme, Leclercq Pierre, « La CNIL a-t-elle accompli les missions dévolues par le législateur ? », *LEGICOM* 2009/1 (nº 42), pp. 13-21.

Huyghe François-Bernard, « Téléphonie mobile : capter la vie numérique des autres », *Hermès, La Revue* 2009/1 (nº 53), pp. 79-84.

Jean-Paul Jean, « Aspects contemporains et comparés de l'oubli en Europe », *Histoire de la justice* 2018/1 (nº 28), pp. 123-134.

Jouanneau Bernard, « Répression du négationnisme : la voix dissonante », *LEGICOM 2015/1* (nº 54), pp. 59-67.

Kaan Pierre, « Stalinisme ou hitlérisme dans une Europe organisée », *Commentaire* 1998/2 (Numéro 82), pp. 379-382.

Kempf Olivier, « La cyberstratégie de l'Union Européenne », *Sécurité globale* 2013/2 (nº 24), pp. 25-40.

Laldji Mounir, « Les menaces des entités criminelles transnationales sur la sécurité intérieure des États », *Sécurité globale* 2016/2 (nº 6), pp. 43-62.

Lancelot Miltgen Caroline, « Vie privée et marketing. Étude de la décision de fournir des données personnelles dans un cadre commercial », *Réseaux* 2011/3 (nº 167), pp. 131-166.

Lancelot Miltgen Caroline, « Dévoilement de données personnelles et contreparties attendues en e-commerce : une approche typologique et interculturelle », *Systèmes d'information & management* 2010/4 (Volume 15), pp. 45-91.

Lavenue Jean-Jacques, « Internalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberespace confronté à la notion d'ordre public », *Les Electronica,* vol 11, n° 2 (Automne / Fall 2006).

Le Voguer Gildas, « Le "complexe industriel" du renseignement américain et la préservation des libertés », *Politique américaine* 2014/2 (nº 24), pp. 29-44.

Lebreton Gilles, « Critique de la Déclaration universelle des Droits de l'homme », *CRDF,* n° 7, 2009, pp.17-22.

Lebrun Pierre-Brice, « La vie privée », *Empan* 2015/4 (nº 100), pp. 168-172.

Lentzen Evelyne, « Fichiers nominatifs et vie privée », *Courrier hebdomadaire du CRISP* 1982/3 (nº 948-949), pp. 1-59.

Léo Magali, « Patient connecté et données de santé : les vrais risques », *I2D – Information, données & documents* 2016/3 (Volume 53), pp. 65-66.

Lepri Charlotte, « Obama et la lutte contre le terrorisme : comment gérer l'héritage Bush ? », *Revue internationale et stratégique* 2009/4 (nº 76), pp. 163-168.

Levallois-Barth Claire, « La géolocalisation : un nouvel impératif », *Hermès, La Revue* 2009/1 (nº 53), pp. 99-104.

Linhardt Dominique, « La "question informationnelle" éléments pour une sociologie politique des fichiers de police et de population en Allemagne et en France (années 1970 et 1980) », *Déviance et Société* 2005/3 (Vol. 29), pp. 259-272.

Livingstone Sonia et al., « Utilisation des réseaux socionumériques par les jeunes européens. Nouveaux résultats sur la vie privée, l'identité et les connexions sociales », *Hermès, La Revue 2011/1* (nº 59), pp. 89-97.

Loiseau Grégoire, « L'évolution de la jurisprudence française sur la vie privée des personnalités politiques », *LEGICOM* 2015/1 (nº 54), pp. 119-123.

Luca Nathalie, « Quelles politiques face aux sectes ? La singularité française », *Critique internationale* 2002/4 (nº 17), pp. 105-125.

Mallet-Poujol Nathalie, « La notion de publication sur l'Internet et son incidence concernant la prescription des délits en ligne », *LEGICOM* 2006/1 (nº 35), pp. 53-69.

Maisl Hubert, « Le droit à l'oubli numérique : état des lieux et perspectives », Bouhadana Irène, Gilles William (sous la direction.), *Vie privée, vie publique à l'ère du numérique*, *Revue de l'institut du monde et du développement,* mai 2011, pp.9-11.

Maffesoli Michel. « Vie publique - Vie privée. », *Réseaux, volume 1, nº 3, 1983. La communication au quotidien*. pp. 37-48.

Malleray (de) Pierre-Alain, « Le marketing dans l'assurance : le tournant du digital », *Revue d'économie financière* 2017/2 (nº 126), pp. 145-168.

Marshall Terence, « Épistémologie, ontologie, philosophie politique », *Droits* 2007/2 (nº 46), pp. 213-276.

Marzouki Meryem, « Nouvelles modalités de la censure : le cas d'Internet en France », *Le Temps des médias* 2003/1 (nº 1), pp. 148-161.

Mattatia Fabrice, « L'efficacité de la protection des données personnelles contre les usages abusifs : état des lieux et pistes d'amélioration », Bouhadana Irène, Gilles William (sous la direction.), *Vie privée, vie publique à l'ère du numérique*, *Revue de l'institut du monde et du développement,* Les éditions IMODEV, mai 2011, pp.45-52.

Maxwell Winston J., « La jurisprudence américaine en matière de liberté d'expression sur Internet », *Étude 2014 du Conseil d'État,* « *Le numérique et les droits fondamentaux* », septembre 2014, pp. 393-406.

Mazeaud Vincent, « La constitutionalisation du droit u respect de la vie privée », *Les nouveaux cahiers du Conseil constitutionnel* nº 48, 1er juin 2015, p. 7.

Mélandri Pierre, « Le terrorisme, voilà l'ennemi ». Les attentats et la politique étrangère des États-Unis, *Vingtième Siècle. Revue d'histoire* 2002/4 (no 76), pp. 45-63.

Mellet Kevin, « L'Internet et le marché du travail. Cadrage des interactions et pluralité des formats d'information », *Réseaux* 2004/3 (nº 125), pp. 113-142.

Mercanti-Guérin Maria, Flores Laurent, « Analyse de l'univers concurrentiel des sites de vente en ligne : une approche par le *Web Analytics* », *Vie & sciences de l'entreprise* 2012/2 (N° 191-192), pp. 96-117.

Merzeau Louise, « De la surveillance à la veille », *Cités* 2009/3 (nº 39), pp. 67-80.

Michels Ank, « Les innovations dans la gouvernance démocratique – En quoi la participation citoyenne contribue-t-elle à l'amélioration de la démocratie ? », *Revue Internationale des Sciences Administratives* 2011/2 (Vol. 77), pp. 275-296.

Mitsilegas Valsamis, « 8. Coopération antiterroriste États-Unis/Union européenne : l'entente cordiale », *in* Didier Bigo *et al.*, *Au nom du 11 septembre...* , La Découverte « Cahiers libres », 2008, pp. 118-130.

Mollier Jean-Yves, « La censure et l'histoire », *Ethnologie française* 2006/1 (Vol. 36), pp. 125-128.

Mondoux André, « Identité numérique et surveillance », *Les Cahiers du numérique* 2011/1 (Vol. 7), pp. 49-59.

Monfort Jean-Yves, « Le racisme, le sexisme et l'homophobie ne sont pas des "opinions" », *LEGICOM* 2015/1 (nº 54), pp. 77-81.

Monod Jean-Claude, « Vers un droit international d'exception ? », *Esprit* 2006/8 (Août/septembre), pp. 173-193.

Moret-Bailly Joël, « Esquisse d'une théorie pragmatiste du droit », *Droits* 2012/1 (nº 55), pp. 177-212.

Musiani Francesca *et al.*, « Net Neutrality as an Internet Governance Issue: The Globalization of an American-Born Debate », *Revue française d'études américaines* 2012/4 (nº 134), pp. 47-63.

Musiani Francesca, Le Crosnier Hervé, « La neutralité de l'Internet, un enjeu pour la documentation à l'ère du numérique », *I2D – Information, données & documents* 2017/1 (Volume 54), pp. 7-9.

Naudin Odile, « Internet : former les parents autant que leurs enfants », *Après̀demain* 2009/1 (nº 9, NF), pp. 39-44.

Nerbonne Sophie, « La publicité ciblée : collecte, conservation et exploitation commerciale des données personnelles (usage, réglementation et régulation) », *LEGICOM* 2009/2 (nº 43), pp. 89-92.

Neveu Erik, « Médias, mouvements sociaux, espaces publics » *Réseaux*, 1999, volume 17 nº 98. pp. 17-85.

Nioche Jean-Pierre, « Les trois paradigmes de l'évaluation des politiques publiques face à l'obligation de rendre des comptes et de rendre compte », *Revue française d'administration publique* 2016/4 (N° 160), pp. 1227-1240.

Ollivier Daniel, « Le succès du télétravail. Les effets de la nouvelle loi Travail », *Études* 2017/12 (Décembre), pp. 33-46.

Onida Valério, « La liberté d'expression en Italie : un regard d'ensemble », *CRDF nº8*, 2010, pp. 27-32.

Orgerit Xavier, « Le développement du "e-syndicalisme" et la liberté syndicale à l'ère de la communication numérique » in *Lettre « Actualités Droits-Libertés » du CREDOF*, 2 octobre 2013.

Padis Marc-Olivier, « Sécurité et terrorisme : un défi pour la démocratie », *Esprit* 2006/8 (Août/septembre), pp. 67-69.

Patterson Lyman Ray, "Copyright And `The Exclusive Right' Of Authors"*, Journal of Intellectual Property*, Vol. 1, No.1 Fall 1993.

Paye Jean-Claude, « Lutte antiterroriste et contrôle de la vie privée », *Multitudes* 2003/1 (nº 11), pp. 91-105.

Paye Jean-Claude, « L'état d'exception : forme de gouvernement de l'Empire ? », *Multitudes* 2004/2 (nº 16), pp. 179-190.

Pech Laurent, « Fasc. 1 250 : Liberté d'expression : aperçus de droit comparé », *JurisClasseur*, 10 juillet 2010.

Pechillon Éric, « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique* 2015/8 (Volume 91), pp. 645-649.

Pellé Eleonore, « Heike Klüver, *Lobbying in the European Union : Interest Groups, Lobbying Coalitions, and Policy change*, Oxford, Oxford University Press, 2013, 278 pages. », *Politique européenne* 2016/3 (nº 53), pp. 132-135.

Pereira Brigitte, « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », *Revue internationale de droit économique* 2016/3 (t. XXX), pp. 387-409.

Perez Pascal, « Liberté et vie privée à l'aube des nouveaux médias », *Après-demain* 2013/3 (nº 27-28, NF), pp. 49-52.

Perez Pascal, « Tous connectés, tous observés, tous surveillés ? », *Après-demain* 2011/2 (nº 18, NF), pp. 28-32.

Perriault Jacques, « Traces numériques personnelles, incertitude et lien social », *Hermès, La Revue* 2009/1 (nº 53), pp. 13-20.

Peyrat Didier, « Société, liberté, sécurité », *Le Débat* 2003/5 (nº 127), pp. 94-103.

Pigeat Henri, « Liberté de la presse. Nuances transatlantiques », *Commentaire* 2003/1 (Numéro 101), pp. 103-110.

Pigneur Yves, « Satisfaction des utilisateurs, protection de la vie privée, connaissances et innovation sous la loupe des chercheurs », *Systèmes d'information & management* 2010/4 (Volume 15), pp. 3-6.

Poullet Yves, « La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ? », *LEGICOM* 2009/1 (nº 42), pp. 47-69.

Pradel Jean, « Investigations téléphoniques au cours de l'enquête », *Recueil Dalloz* 2006, p. 2836.

Preuss-Laussinotte Sylvia, « Bases de données personnelles et politiques de sécurité : une protection illusoire ? », *Cultures & Conflits* [En ligne], 64 | hiver 2006, mis en ligne le 06 mars 2007. URL : http://conflits.revues.org/2133.

Preuvot Perrine, « Le droit de pétition : mutations d'un instrument démocratique », *Jurisdoctoria* nº 4, 2010.

Quéméner Myriam, « La directive NIS, un texte majeur en matière de cybersécurité », *Sécurité et stratégie* 2016/3 (23), pp. 50-56.

Quéméner Myriam, « La géolocalisation : un outil de protection ou de surveillance ? », *Sécurité et stratégie* 2013/4 (15), pp. 11-17.

Raflik Jenny, « La France face au terrorisme d'hier à aujourd'hui », *Outre-Terre* 2017/2 (nº 51), pp. 202-214.

Rallet Alain et al., « De la *Privacy by Design* à la *Privacy by Using*. Regards croisés droit/économie », *Réseaux* 2015/1 (nº 189), pp. 15-46.

Raynal Florence *et al.*, « De nouvelles dispositions pour protéger les données personnelles », *Documentaliste-Sciences de l'Information* 2014/3 (Vol. 51), pp. 23-25.

Renoux Thierry S., « Juger le terrorisme ? » in *Dossier : La justice dans la constitution*, *Cahiers du Conseil constitutionnel* nº 14, mai 2003.

Rey Bénédicte, « Les intelligences numériques des informations personnelles. Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique* 2014 (Vol. 10), pp. 9-18.

Ribes Didier, « Atteintes publiques et atteintes privées au droit au respect de la vie privée dans la jurisprudence du Conseil constitutionnel », *Les nouveaux Cahiers du Conseil constitutionnel* nº 48, 1er juin 2015, pp.35.

Rioche Julian, « L'enjeu de la sécurité des objets connectés », *I2D – Information, données & documents* 2017/3 (Volume 54), pp. 64-65.

Roblot-Troizier Agnès, « Un concept moderne : séparation des pouvoirs et contrôle de la loi », *Pouvoirs* 2012/4 (nº 143), pp. 89-103.

Roblot-Troizier Agnès, « Droits fondamentaux et libertés publiques », *Les Nouveaux Cahiers du Conseil constitutionnel* 2015/3 (nº 48), pp. 161-176.

Roudier Karine, « Prix de thèse du Conseil constitutionnel : Le contrôle de constitutionnalité de la législation antiterroriste. Étude comparée des expériences espagnole, française et italienne », *Nouveaux cahiers du Conseil constitutionnel* nº 37, octobre 2012, pp. 147-154.

Sabbagh Daniel, « Sécurité et libertés aux États-Unis dans l'après-11 septembre : un état des lieux », *Critique internationale* 2003/2 (nº 19), pp. 17-23.

Sajus Bertrand *et al.*, « Web 2.0, et après ? Critique et prospective », *Documentaliste-Sciences de l'Information* 2009/1 (Vol. 46), pp. 54-66.

Salas Denis, « L'état d'urgence : poison ou remède au terrorisme ? », *Archives de politique criminelle* 2016/1 (nº 38), pp. 75-87.

Schaffhauser Lise-Marie, « Constitution de réseaux et protection de la vie privée. Cadre juridique dans le domaine du travail social et avec les familles », *Informations sociales* 2008/3 (nº 147), pp. 82-89.

Schweitzer Laëtitia, « Surveillance électronique », *Communications 2011/1* (nº 88), pp. 169-176.

Serfaty Viviane, « Le refus d'interdire : éléments pour une analyse de la liberté d'expression sur Internet aux États-Unis », *Raisons politiques* 2012/3 (nº 47), pp. 189-202.

Severo Marta, « L'information quotidienne face au Web 2.0. La stratégie multiplateforme de six quotidiens nationaux français », *Études de communication* [En ligne], 41 | 2013, mis en ligne le 01 décembre 2013, consulté le 15 mars 2017. URL : http://edc.revues.org/5399.

Soriano Sébastien, « Quelle régulation pour les plateformes ? », *Annales des Mines - Réalités industrielles* 2016/3 (Août 2016), pp. 47-50.

Sudre Frédéric, Gonzalez Gérard, Blay-Grabarczyk Katarzina, Milano Laure, Surrel Hélène, *«* Chronique de la jurisprudence de la Cour européenne des droits de l'homme (2015) *»* in *Revue du Droit public*, nº 3, 1er mai 2016, p. 1013.

Stefanick Lorna, « L'externalisation et la circulation transfrontalière des données : Défi de la protection des renseignements personnels dans le cadre du USA Patriot Act », *Revue Internationale des Sciences Administratives* 2007/4 (Vol .73), pp. 583-603.

Stitou Rajaa, « Faut-il renoncer à la liberté pour être heureux ? Roland Gori, Éditions Les Liens qui Libèrent, 2014 », *Cahiers de psychologie clinique* 2015/1 (nº 44),

Sudre Frédéric, Gonzalez Gérard, Blay-Graberczyk Katarzina, Milano Laure, Surrel Hélène, « Chronique de jurisprudence de la Cour européenne des droits de l'homme (2015) », *Revue de droit public* nº 3*,* 1er mai 2016, p.1013.

Tanghe Hélène, Gibert Paul-Olivier, « L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales* 2017/4, pp. 79-93.

Tchuente Dieudonné *et al.*, « Accès à l'information dans les réseaux socionumériques », *Hermès, La Revue* 2011/1 (nº 59), pp. 59-64.

Terrier Christophe, « La valeur des données géographiques », *L'Espace géographique* 2011/2 (Tome 40), pp. 103-108.

Tijardovic Stéphane, « La protection juridique des données personnelles. Vers une nécessaire adaptation de la norme juridique aux évolutions du monde numérique », *Les Cahiers du numérique* 2003/3 (Vol. 4), pp. 185-203.

Tisseron Serge, « Intimité et extimité », *Communications* 2011/1 (nº 88), pp. 83-91.

Trudel Pierre, « La protection de la vie privée et de l'image aux États-Unis », dans *Institut de formation continue du Barreau de Paris, Liberté de presse, respect de la vie privée et de l'image en droit comparé*, *Supplément de la Gazette du Palais*, 1992, pp. 14-24.

Türk Alex, Piazza Pierre, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011, consulté le 30 septembre 2016. URL : http://conflits.revues.org/17806.

Tabaka Benoit, « PriceMinister, acteur de la lutte contre la cyberdélinquance », Bouhadana Irène, Gilles William (sous la direction.), *Cybercriminalité cybermenaces & cyberfraudes*, Les éditions IMODEV, Mars 2012, pp. 206-209.

Vadillo Floran, « Du terrorisme en démocratie », *Sécurité et stratégie* 2015/1 (20), pp. 5-13.

Valjavec Emmanuel, « Internet, un nouvel espace de liberté sous surveillance », *Études* 2013/3 (Tome 418), pp. 317-327.

Vallet Caroline, « Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs », *Droit et société* 2012/1 (nº 80), pp. 163-188.

Varnerot Valérie, « La fictionnalisation de la vie privée », *Revue interdisciplinaire d'études juridiques* 2010/1 (Volume 64), pp. 183-244.

Verly Nicolas, « Le point sur la diffamation et l'injure pour les blogueurs, la responsabilité des éditeurs de sites en cas de contributions extérieures (commentaires, forums de discussion...) », *LEGICOM* 2016/2 (nº 57), pp. 35-43.

Verpeaux Michel, « La liberté d'expression dans les jurisprudences constitutionnelles », *Les Nouveaux Cahiers du Conseil constitutionnel* 2012/3 (nº 36), pp. 135-155.

Vidal Geneviève, « Prendre la mesure du renoncement négocié », *Multitudes* 2017/3 (n° 68), pp. 54-59.

Vidal Geneviève, « Présentation. Instabilité et permanence des usages numériques », *Les Cahiers du numérique* 2013/2 (Vol. 9), pp. 9-46.

Vitran Jean-Claude, « Vous êtes étiquetés ? », *Revue Projet* 2010/6 (n° 319), pp. 55-61.

Weaver Russell L., « Transparency, Privacy, and Democracy in a Digital Era », Bouhadana Irène, Gilles William (sous la direction.), *International Journal of Open Government* [2017 – Vol. 4], pp. 49-63, à http://ojs.imodev.org/index.php/RIGO.

Weiss Marie-Andrée, « De la sphère au bouclier : qu'est-ce que le Privacy Shield ? », *I2D – Information, données & documents* 2016/3 (Volume 53), pp. 20-22.

Chapitres parus dans des ouvrages collectifs

Allard France, « Les droits de la personnalité », in Barreau du Québec, *Personnes, famille et successions*, Collection de droit 1997-1998, volume 3, Cowansville, Éditions Yvon Blais, pp. 55-75.

Bouhadana Irène, Gilles William, Harivel Jean, "Freedom of expression and the values of the French Republic. Article dedicated to the memory of the victims of the terrorist attacks of 2015 in France", in Weaver Russell L., Friedland Steven I. (Edited by), *Comparative Perspectives*

on Freedom of Expression, Global Papers Series, Vol. II, Carolina Academic Press, 2017, pp. 141-158.

Duval Elisabeth, « La cybercriminalité subie et combattue par un opérateur tel SFR », in Bouhadana Irène, Gilles William (sous la direction.), *Cybercriminalité cybermenaces & cyberfraudes*, Les éditions IMODEV, Mars 2012, pp. 196-205.

Hamon Bruno, « Les cyberattaques et le cyberespionnage », in Bouhadana Irène, Gilles William (sous la direction.), *Cybercriminalité cybermenaces & cyberfraudes*, Les éditions IMODEV, Mars 2012, pp.70-75.

Joxe Pierre, « La cybercriminalité, résurgence du furtum noctu à l'ère du numérique », in I. Bouhadana Irène, Gilles William (sous la direction de), Bouhadana Irène, Gilles William (sous la direction.), *Cybercriminalité, cybermenaces et cyberfraudes*, Les éditions Imodev, 2012.

Lavenue Jean-Jacques, « L'interconnexion des fichiers de police : les ambiguïtés du rapport dialectique entre nécessité de la sécurité publique et protection des libertés » in Institut Maurice Hauriou, *Les fichiers de police,* Université de Toulouse, 15 septembre 2017.

Lavenue Jean-Jacques, « Internet : efficacité des poursuites et ordre public international », in Bouhadana Irène, Gilles William (sous la direction.), *Cybercriminalité cybermenaces et cyberfraudes*, Les éditions Imodev, mars 2012 pp. 84-91.

Leclerc Gérard, « De la censure à la liberté de penser », in Leclerc Gérard (dir.) *Histoire de l'autorité. L'assignation des énoncés culturels et la généalogie de la croyance*, Paris, Presses Universitaires de France, « Sociologie d'aujourd'hui », 1996, pp. 219-246.

Leclerc Olivier, « Lanceur d'alerte », in Emmanuel Henry *et al.*, *Dictionnaire critique de l'expertise*, Presses de Sciences Po (P.F.N.S.P.) « Références », 2015, pp. 194-202.

Laurent Sébastien, « Faire l'histoire de la surveillance » in Aghroum Christian, et al. *Identification et surveillance des individus : Quels enjeux pour nos démocraties ?* Nouvelle édition [en ligne]. Paris : Éditions de la Bibliothèque publique d'information, 2010, p. 26. URL : http://books.openedition.org/bibpompidou/1192.

Lyon David, « 6. Le 11 septembre, la "guerre au terrorisme" et la surveillance généralisée », in Didier Bigo *et al.*, *Au nom du 11 septembre...*, La Découverte « Cahiers libres », 2008, pp. 90-103.

Mattatia Fabrice, « L'usurpation d'identité en ligne », in Bouhadana Irène, Gilles William (sous la direction.), *Cybercriminalité cybermenaces & cyberfraudes*, Les éditions IMODEV, Mars 2012, pp.135-139.

Poullet Yves, Henrotte Jean-François, « La protection des données (à caractère personnel) à l'heure de l'Internet », in *Protection du consommateur, pratiques commerciales et T.I.C.*, collection Commission Université-Palais, volume 109, pp. 197-245.

Schoen Gérard, « Les douanes face à la cybercriminalité », in Bouhadana Irène, Gilles William (sous la direction.), *Cybercriminalité cybermenaces & cyberfraudes*, Les éditions IMODEV, Mars 2012, pp.169-172.

Turki Slim, Foulonneau Muriel, « Valorisation des données ouvertes : acteurs, enjeux et modèles d'affaires », in Broudoux Évelyne et al., *Big Data - Open Data : Quelles valeurs ? Quels enjeux ?*, De Boeck Supérieur « Information et stratégie », 2015, pp. 113-125.

Voisset Michèle, « Droit au respect de la vie privée et société de l'information », in Tabatoni Pierre (dir.), *La protection de la vie privée dans la société d'information*, 2002, Presses Universitaires de France, Tome 3, pp. 249-254.

Autres revues

« Les données personnelles, ingrédient de base des recettes à succès sur smartphone » in *La lettre innovation et prospective de la CNIL, nº8*, novembre 2014.

Agnieszka Moniak-Azzopardi, « Les religions et l'État en Russie », *Le Courrier des pays de l'Est 5/2004* (nº 1045), pp. 28-38.

Blum Léon alias « un juriste », « Comment ont été faites les lois scélérates », *La Revue Blanche*, 1er juillet 1898.

Bouhadana Irène, Gilles William, Harivel Jean, « Darknet, le côté obscur du net », *Panthéon Sorbonne magazine, nº 6*, janvier-février 2014, pp. 12-15.

Debré Michel, « Allocution devant le Conseil d'État », in *Travaux préparatoires des institutions de la Vᵉ République, volume III*, La Documentation française, 1991, pp. 268-269.

Freyssinet Éric, « L'Europe en lutte contre la cybercriminalité » in *La criminalité en France, Rapport de l'Observatoire national de la délinquance et des réponses pénales 2011*, Novembre 2011, CNRS éditions, p. 887.

Jospin Lionel, *Déclaration sur la mise en œuvre et les orientations de développement du Programme d'action gouvernementale pour la société de l'information (PAGSI) depuis son lancement en 1997 et la préparation du passage électronique à l'an 2000*, Hourtin le 26 août 1999.

Mazeaud Pierre, *La lutte contre le terrorisme dans la jurisprudence du Conseil constitutionnel*, Visite à la cour suprême du Canada, 24 au 26 avril 2006.

Milanović Andro, Srbljić Siniša, Ražnjević Ivo, Sladden Darryl, Matošević Ivan, and Skrobo Daniel, *Methods for Lawful Interception in IP Telephony Networks Based on H.323*, EUROCON 2003 Ljubljana, Slovenia.

Narayanan Arvind and Shmatikov Vitaly, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset,* The University of Texas at Austin, February 5, 2008.

Thibaud Vincent, « Législation antiterroriste, lutte contre la criminalité organisée : le Conseil constitutionnel face aux politiques pénales actuelles », *Atelier n°5 « justice et Constitution »*, VIIe Congrès français de droit constitutionnel, 25, 26 et 27 septembre 2008.

Trudel Pierre, *La protection de la vie privée*, cours, Chaire L. R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, Faculté de droit, Université de Montréal.

Tabatoni Pierre, « Vie privée : une notion et des pratiques complexes » in *La protection de la vie privée dans la société d'information*, Presses Universitaires de France (Cahiers des Sciences morales et politiques).

Articles de presse

Berger François, « Le transhumanisme est un charlatanisme dangereux », *Sciences et Avenir*, Août 2016.

Boucher Philippe, « Safari ou la chasse aux français », *Le Monde*, 21 mars 1974.

Sender Elena, « Californie : la police connaît déjà l'heure du crime », *Sciences et Avenir n°782*, avril 2012, pp. 68-73.

Webographie

"Court throws out Yahoo case over French WEB restrictions", Juanary 18, 2006 at https://www.rcfp.org/browse-media-law-resources/news/court-throws-out-yahoo-case-over-french-web-restrictions, consulté le 16 février 2017.

"Project no. AST3-CT-2004 502858_OpTag, Op Tag Improving Airport Efficiency, Security and Passenger Flow by Enhanced Passenger Monitoring Executive Summary", à http://cordis.europa.eu/docs/publications/1239/123991301-6_en.pdf, consulté le 2 août 2017.

« À qui appartiennent les instituts de sondages ? », 20 mars 2008, à https://www.legrandsoir.info/SONDO-MENSONGES-a-qui-appartiennent-les-instituts-de-sondages.html, consulté le 9 août 2017).

« La lutte contre le téléchargement illégal ailleurs dans le monde », *Le Monde.fr*, 9 mars 2009, à http://www.lemonde.fr/technologies/article/2009/03/09/la-lutte-contre-le-telechargement-illegal-ailleurs-dans-le-monde_1162567_651865.html, consulté le 3 mars 2017.

« La CNIL met en garde contre le service de géolocalisation de Facebook », *Le Monde.fr*, 20 octobre 2010, à http://www.lemonde.fr/technologies/article/2010/10/20/la-cnil-met-en-garde-contre-le-service-de-geolocalisation-de-facebook_1428569_651865.html, consulté le 5 mai 2012

« Le ministère de l'Economie et des Finances, victime d'une attaque informatique », *Libération. fr*, 7 mars 2011, à http://www.liberation.fr/economie/01012324121-le-ministere-de-l-economie-et-des-finances-victime-d-une-attaque-informatique, consulté le 5 mai 2012.

« Bercy : la cyberattaque visait le G20. Plus de 150 ordinateurs ont été piratés depuis décembre, selon Paris-Match. Baroin confirme. », *Europe 1*, 7 mars 2011, à http://www.europe1.fr/france/bercy-la-cyber-attaque-visait-le-g20-442555, consulté le 17 juin 2017.

« STIC : Histoires vécues », à http://www.cnil.fr/la-cnil/actu-cnil/article/article/stic-histoires-vecues/ consulté le 13 mai 2012.

« La révolution égyptienne ou le rôle des médias sociaux dans les soulèvements » à http://egypterevolution.wordpress.com/, 11 avril 2011, consulté le 5 mai 2012.

« Les Brésiliens se mobilisent contre la corruption », *LeMonde.fr*, 20 septembre 2011 à http://www.lemonde.fr/ameriques/article/2011/09/20/les-bresiliens-se-mobilisent-contre-la-corruption_1574614_3222.html, consulté le 5 mai 2012.

« Israël interdit l'accès de son territoire à des centaines de militants pro-Palestiniens », 15 avril 2012 à http://www.france24.com/fr/20120415-israel-militants-pro-palestiniens-interdits-entree-cisjordanie-ben-gourion-bienvenue-palestine-tel-aviv, consulté le 8 juin 2012.

« Près de 50 000 personnes s'invitent à un anniversaire via Facebook », *France Info*, 26 avril 2012 à http://www.franceinfo.fr/high-tech/pres-de-50-000-personnes-s%E2%80%99invitent-a-un-anniversaire-via-facebook-597821-2012-04-26, consulté le 10 mai 2012.

« Anniversaire géant et tapage nocturne "monstre" à Vertou cette nuit », *Presse Océan*, 6 mai 2012 à http://www.presseocean.fr/actu/actu_detail_-Anniversaire-geant-et-tapage-nocturne-monstre-a-Vertou-cette-nuit_9182, 40 310,403 11, 12 028,120 27, 12 024,129 81, 9180-2073953_actu. Htm, consulté le 10 mai 2012.

« Voyage au cœur des smartphones et des applications mobiles avec la CNIL et Inria », 9 avril 2013, à http://www.inria.fr/actualite/mediacenter/cnil-et-inria, consulté le 7 janvier 2016.

« Le FBI aurait accès aux serveurs de Google, Facebook, Microsoft, Yahoo! et d'autres géants d'Internet », *Le Monde*, 7 juin 2013, à http://www.lemonde.fr/ameriques/article/2013/06/07/le-fbi-a-acces-aux-serveurs-des-geants-d-Internet_3425810_3222.html#OEF9XUIrZqgC8Yqk.99, consulté le 16 décembre 2015.

« Surveillance d'Internet : un ancien employé de la CIA à l'origine des fuites », *Le Monde*, 9 juin 2013, à http://www.lemonde.fr/ameriques/article/2013/06/09/un-ancien-employe-de-la-nsa-derriere-les-revelations-sur-les-ecoutes-numeriques_3426888_3222.html#b77c0qYFGAKhIYKC.99, consulté le 16 décembre 2015.

« Gmail : l'analyse des e-mails par Google devant la justice américaine », *ZDNet*, 27 septembre 2013, à http://www.zdnet.fr/actualites/gmail-l-analyse-des-emails-par-google-devant-la-justice-americaine-39794372.htm consulté le 12 juillet 2017.

"Operator of Silk Road 2.0 WEBsite Charged in Manhattan Federal Court", 6 novembre 2014, à https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court, consulté le 2 août 2017.

« Comment le Darknet peut-il améliorer la vie des gens ? », 18 janvier 2015 à https://lucieetval.wordpress.com/tag/edward-snowden/, consulté le 1er mars 2017.

« Fausse mort de Martin Bouygues : Les médias sont-ils pour toujours condamnés à l'emballement ? », *le Blog du communicant*, 1er mars 2015, à http://www.leblogducommunicant2-0.com/2015/03/01/fausse-mort-de-martin-bouygues-les-medias-sont-ils-pour-toujours-condamnes-a-lemballement/, consulté le 23 janvier 2017.

« Californie : recours autorisé pour des chauffeurs Uber réclamant un statut de salarié », 2 septembre 2015, à http://lexpansion.lexpress.fr/high-tech/californie-recours-autorise-pour-des-des-chauffeurs-uber-reclamant-un-statut-de-salarie_1711685.html, consulté le 5 octobre 2015.

« Apple : le cryptage de données interdit au Royaume-Uni ? », *iPhonote*, 3 novembre 2015, à https://www.iphonote.com/actu/89908/apple-le-cryptage-de-donnees-interdit-au-royaume-uni, consulté le 7août 2017.

« Anti-terrorisme : l'interdiction du cryptage des smartphones, une mesure peu efficace contre les djihadistes, mais ravageuse pour l'économie et les libertés », *Atlantico*, 11 décembre 2015, à http://www.atlantico.fr/decryptage/lutte-anti-terrorisme-interdiction-cryptage-smartphones-mesure-peu-efficace-contre-djihadistes-mais-ravageuse-pour-economie-et-2487813.html#1VER0m8RHlfEFQvI.99, consulté le 3 août 2017.

« Piratages durant l'élection présidentielle : Barack Obama annonce des représailles contre la Russie », *le Huffington Post*, 16 décembre 2016, à http://www.huffingtonpost.fr/2016/12/16/piratages-election-presidentielle-americaine-etats-unis-barack-obama-represailles-russie-vladimir-poutine/, consulté le 16 janvier 2017.

« Uber et UberPop : c'est quoi la différence ? », *Le figaro.fr*, 3 juillet 2015, à http://www.lefigaro.fr/secteur/high-tech/2015/07/03/32001-20150703ARTFIG00177-uber-et-uberpop-c-est-quoi-la-difference.php, consulté le 2 mars 2017.

« Microsoft rachète LinkedIn qui décolle en Bourse », *Challenges,* 13 juin 2016, à http://www.challenges.fr/Internet/20160613.CHA0490/microsoft-racheterait-linkedin.html, consulté le 2 juillet 2016.

« Global Cyber Attack Synchronized, Ransonware-Driven », *TeachThought News*, à http://www.teachthought.com/current-events/global-cyber-attack-appeared-synchronized-ransonware-driven/, consulté le 17 juin 2017.

« Cyberattaque WannaCry : Microsoft met en cause la NSA et veut une "convention de Genève numérique" », *HUFFPOST*, 15 mai 2017, à http://www.huffingtonpost.fr/2017/05/15/cyberattaque-microsoft-met-en-cause-la-nsa-et-veut-une-convent_a_22086836/, consulté le 17 juin 2017.

« La clause des CGU de Facebook imposant un tribunal californien est abusive », *Légalis*, 23 février 2016, à https://www.legalis.net/actualite/la-clause-des-cgu-de-facebook-imposant-un-tribunal-californien-est-abusive/, consulté le 13 juillet 2017.

« Gmail : Google renonce à scanner les courriels pour cibler les pubs », *ZDNet,* 26 juin 2017, en ligne à http://www.zdnet.fr/actualites/gmail-google-renonce-a-scanner-les-courriels-pour-cibler-les-pubs-39854144.htm, consulté le 7 août 2017.

Ambassade des États-Unis d'Amérique, « La liberté d'expression aux États-Unis », publié en 2003, à http://photos.state.gov/libraries/amgov/133183/french/1304_Freedom_of_Expression_UnitedStates_French_Digital.pdf, consulté le 6 février 2017.

ANSSI, « La SSI en France », à http://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/, consulté le 7 décembre 2015.

Astier Stéphane, « Le droit au respect de la vie privée, droit constitutionnellement reconnu », *JurilexBlog*, 21 janvier 2010, à http://www.jurilexblog.com/droit-respect-vie-privee-droit-constitutionnellement-reconnu-260783, consulté le 18 août 2017.

Audenard Jean-François, « Interceptions légales : Retour aux bases », *Les blogs Orange Business*, à http://blogs.orange-business.com/securite/2010/11/interceptions-legales-retour-aux-bases.html consulté le 30 avril 2012.

Aufray Christophe, « Géolocalisation : la Cnil inflige 100 000 euros d'amende à Google », *ZDNet.fr*, 21 mars 2011, à http://www.zdnet.fr/actualites/geolocalisation-la-cnil-inflige-100-000-euros-d-amende-a-google-39759236.htm, consulté le 5 mai 2012.

Baer Sébastien, « Que devient TV5 Monde après la cyberattaque ? », 25 juillet 2015, à http://www.franceinfo.fr/emission/ils-ont-fait-l-actu/2015-ete/que-devient-tv5-monde-apres-la-cyberattaque-23-07-2015-07-25, consulté le 7 décembre 2015.

Baumont Didier, « Liberté d'expression et irresponsabilité des députés », https://www.unicaen.fr/puc/images/crdf0202baumont.pdf, consulté le 4 février 2017.

Belfiore Guillaume, « Vie privée : l'Allemagne relance son offensive contre Google », 1er octobre 2014, à http://www.clubic.com/pro/entreprises/google/actualite-730451-vie-privee-allemagne-relance-offensive-google.html, consulté le 7 octobre 2016.

Bellanova Rocco, De Hert Paul, « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », *Cultures & Conflits*, 03 mai 2011, consulté le 01 janvier 2013, à http://conflits.revues.org/17805 .

Benayoun Arik, « Le Royaume-Uni valide son Hadopi », *DegroupNews*, 7 mars 2012, à https://www.degroupnews.com/Internet/royaume_uni-hadopi-telechargement-riposte_graduee-piratage, consulté le 3 mars 2017.

Bensoussan Alain, « Faut-il réguler la marchandisation des données personnelles sur Internet ? », 30 janvier 2013, à http://blog.lefigaro.fr/bensoussan/2013/01/le-profilage-commercial-est-inherent.html, consulté le 13 novembre 2015.

Berthet Charly, Tribune « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible », *Le Monde.fr*, 22 août 2016, disponible à https://cnnumerique.fr/tribune-chiffrement/, consulté le 3 août 2017.

Biem Anthony, « Facebook : illicéité de la clause attributive compétence du tribunal californien de ses CGU », 28 juin 2016, à http://www.legavox.fr/blog/maitre-anthony-bem/facebook-illiceite-clause-attributive-competence-21407.htm, consulté le 6 janvier 2017.

Blanchard Cécile, « Localisation des passagers par RFID ou bluetooth testée à l'aéroport de Copenhague », 4 juin 2008, in *ReseauxTelecom.net* à http://www.reseaux-telecoms.net/actualites/lire-localisation-des-passagers-par-rfid-ou-bluetooth-testee-a-l-aeroport-de-copenhague-18282.html consulté le 5 mai 2012.

Commission européenne, Communiqué de Presse du 9 janvier 2013 : « Le Centre européen de lutte contre la cybercriminalité (EC3) sera inauguré le 11 janvier », 9 janvier 2013, disponible à http://europa.eu/rapid/press-release_IP-13-13_fr.htm, consulté le 17 juin 2017.

Commission Nationale de l'informatique et des Libertés, « Testing de la CNIL auprès de la RATP : l'exercice du droit des usagers à se déplacer anonymement n'est pas garanti », 6 janvier 2009, à http://www.cnil.fr/la-cnil/actu-cnil/article/article/testing-de-la-cnil-aupres-de-la-ratp-lexercice-du-droit-des-usagers-a-se-deplacer-anonymement/, consulté le 5 mai 2012.

Commission Nationale de l'informatique et des Libertés, « Contrôle du STIC : Les propositions de la CNIL pour une utilisation du fichier plus respectueuse du droit des personnes », 20 janvier 2009, à http://www.cnil.fr/la-cnil/actu-cnil/article/article/controle-du-stic-les-propositions-de-la-cnil-pour-une-utilisation-du-fichier-plus-respectueuse-du/, consulté le 13 mai 2012.

Commission Nationale de l'informatique et des Libertés, « Les dispositifs de géolocalisation GSM/GPS » à http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/les-dispositifs-de-geolocalisation-gsmgps/, consulté le 5 mai 2012.

Commission nationale de l'informatique et des libertés , « Vidéosurveillance / vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », 21 juin 2012, à https://www.cnil.fr/fr/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de-la-vie, consulté le 7 juillet 2017.

Commission Nationale de l'informatique et des Libertés, « Contrôle des fichiers d'antécédents : conclusions et propositions de la CNIL », 13 juin 2013, à http://www.cnil.fr/linstitution/actualite/article/article/controle-des-fichiers-dantecedents-conclusions-et-propositions-de-la-cnil/ consulté le 7 décembre 2015.

Commission nationale de l'informatique et des libertés, « Comment réaliser une évaluation d'impact sur la vie privée (EIVP) pour les dispositifs RFID ? », septembre 2013, à https://www.cnil.fr/sites/default/files/typo/document/Methodologie-etude_impact_RFID.pdf, consulté le 31 juillet 2017.

Commission Nationale de l'informatique et des Libertés, « Affaire PRISM : ce que fait la CNIL », 24 octobre 2013, à http://www.cnil.fr/nc/linstitution/actualite/article/article/affaire-prism-ce-que-fait-la-cnil/, consulté le 16 décembre 2015.

Commission nationale de l'informatique et des libertés , « Les conseils de la CNIL pour mieux maîtriser la publication de photos », 13 octobre 2014, à https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mieux-maitriser-la-publication-de-photos-0, consulté le 7 juillet 2016.

Commission nationale de l'informatique et des libertés , « Article Mobilitics, saison 2 : nouvelle plongée dans l'univers des smartphones et de leurs applications », 15 décembre 2014, à http://www.cnil.fr/linstitution/actualite/article/article/mobilitics-saison-2-nouvelle-plongee-dans-lunivers-des-smartphones-et-de-leurs-applications/?tx_ttnews%5BbackPid%5D=91&cHash=497ed7bf0a1b668cf702e2cfb41dbf99, consulté le 7 janvier 2016.

Conseil pontifical pour les communications sociales, « L'église et Internet », à http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_church-Internet_fr.html, consulté le 22 février 2017.

Cosnard Denis, « "Secret des affaires" : le gouvernement retire son projet », *Le Monde.fr*, 30 janvier 2015, à http://www.lemonde.fr/economie/article/2015/01/30/secret-des-affaires-le-gouvernement-retire-son-projet_4566657_3234.html, consulté le 23 janvier 2017.

Coulibaly Ibrahim, « Le puissant droit d'accès aux données à caractère personnel », 18 août 2014, *Village de la Justice*, à http://www.village-justice.com/articles/puissant-droit-acces-aux-donnees,17541.html consulté le 24 mai 2016.

Cour de cassation, « Discours de l'audience solennelle de rentrée », 14 janvier 2016, à https://www.courdecassation.fr/venements_23/audiences_solennelles_59/debut_annee_60/annees_2010_3342/janvier_2016_33391.html, consulté le 14 juin 2017.

Davan-Soula Melinda, « Facebook a encore dû présenter ses excuses après avoir censuré une vidéo diffusée dans le cadre de la campagne de prévention du cancer du sein », 21 octobre 2016, at http://www.lci.fr/high-tech/couvrez-ce-sein-que-je-ne-saurais-voir-facebook-le-censure-2008822.html, consulté le 16 février 2017.

Demoment Alexis, Maccarinelli Elliot, « Les citoyens contre la vidéo-surveillance », *Le Journal international*, 11 février 2015, à http://www.lejournalinternational.fr/Les-citoyens-contre-la-video-surveillance_a2286.html, consulté le 4 janvier 2016.

Duportail Judith, « Comprendre la censure sur Facebook » in http://www.lexpress.fr/actualite/high-tech/comprendre-la-censure-sur-facebook_980973.html du 9 avril 2011, consulté le 5 mai 2012.

Dutheil Guy, « Airbnb : Paris veut éviter le syndrome de "Barceloneta" », *Le Monde,* 1er octobre 2015 à http://www.lemonde.fr/economie/article/2015/10/01/pour-airbnb-paris-vaut-bien-une-taxe_4779202_3234.html, consulté le 5 octobre 2015.

Foegle Jean-Philippe, « Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme [En ligne*], Actualités Droits-Libertés, 30 mars 2016, à http://revdh.revues.org/2074, consulté le 30 septembre 2016.

France diplomatie, « Liberté de religion ou de conviction. La France est la liberté de religion et de conviction », décembre 2015, à http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/droits-de-l-homme/liberte-de-religion-ou-de-conviction/, consulté le 18 février 2017.

Gelles Viviane, « Adresse IP : donnée à caractère personnel ? », *Jurisexpert,* 28 août 2014, à http://www.jurisexpert.net/adresse-ip-donnee-caractere-personnel/ consulté le 24 mars 2016.

Godefridi Drieu, « Sectarisme parlementaire », *LaLibre.be*, 28 octobre 2005, at http://www.lalibre.be/debats/opinions/sectarisme-parlementaire-51b88c0fe4b0de6db9ace680, consulté le 30 août 2017.

Grassi Robin, « Loi pour une République numérique : coup de com ou démocratie ? », 4 janvier 2016, à http://radio-londres.fr/2016/01/loi-numerique-com-democratie/, consulté le 11 août 2017.

Greenwald Glenn, MacAskill Ewen, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, 7 juin 2013, à http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, consulté le 16 décembre 2015.

Guerrier Philippe, « Publicité ciblée : Google arrête le scan des contenus sur Gmail, mais change de levier », *ITexpresso*, 26 juin 2017, à http://www.itespresso.fr/publicite-ciblee-google-arrete-scan-contenus-gmail-163336.html?inf_by=596643b1671db84e358b4855, consulté le 12 juillet 2017.

Johannès Franck, « La Cour européenne des droits de l'homme rendra une décision sur la loi renseignement – Le dossier en droit », *Le Monde*, 16 mai 2017, à http://libertes.blog.lemonde.fr/2017/05/16/la-cour-europeenne-des-droits-de-lhomme-rendra-une-decision-sur-la-loi-renseignement-le-dossier-en-droit/, consulté le 21 juin 2017.

Jost Clémence, Texier Bruno, « Comment mieux protéger vos données personnelles ? », *archimag*, 19 janvier 2017, URL : http://www.archimag.com/univers-data/2017/01/19/10-conseils-outils-indispensables-proteger-donnees-personnelles, consulté le 25 novembre 2017.Le Bailly David, « Gigantesque affaire d'espionnage à Bercy », *Paris Match*, 7 mars 2011, à http://www.parismatch.com/Actu/Societe/Affaire-d-espionnage-au-ministere-par-de-l-Economie-et-des-Finances-Paris-Match-146419 consulté le 17 juin 2017.

Le forum des étudiants de Sciences Po, « La jurisprudence de la Cour européenne des droits de l'homme », *Les cours d'économie du forum des étudiants de Sciences Po*, à http://www.forum-scpo.com/union-europeenne/jurisprudence-convention-europeenne-des-droits-de-l-homme-cedh.htm, consulté le 13 juillet 2017.

Le Monde.fr avec AFP, « La CNIL veut inscrire dans la Constitution la protection des données personnelles », *Le Monde.fr* 13 mai 2009, à http://www.lemonde.fr/societe/article/2008/05/16/la-cnil-veut-inscrire-dans-la-constitution-la-protection-des-donnees-personnelles_1046127_3224.html, consulté le 6 juin 2016.

Letteron Roseline, « L'idéologie des Droits de l'Homme en France et aux États-Unis », *L'Universalité des Droits de l'Homme : apparences et réalités*, à http://www.diplomatie.gouv.fr/fr/IMG/pdf/FD001351.pdf, consulté le 4 janvier 2017.

Macron Emmanuel, « Discours de la politique de lutte contre le terrorisme », 10 avril 2017, Retranscription du discours d'Emmanuel Macron à Paris, disponible en ligne à https://en-marche.fr/article/meeting-macron-politique-lutte-contre-le-terrorisme, consulté le 1 juillet 2017.

Manenti Boris, « Données personnelles : la Cnil milite pour modifier la Constitution, L'autorité a plaidé auprès des parlementaires et du gouvernement pour inscrire une garantie de la protection des données personnelles dans la révision constitutionnelle », *Le cahier tendance de l'Obs*, 24 mai 2013, à http://o.nouvelobs.com/high-tech/20130524.OBS0534/donnees-personnelles-la-cnil-milite-pour-modifier-la-constitution.html, consulté le 6 juin 2016.

Ministère de l'intérieur, « Plan de Vidéo protection pour Paris : Bilan opérationnel de l'exploitation des caméras par la D.S.P.A.P. », 24 avril 2013, à http://www.interieur.gouv.fr/content/download/41759/322134/file/exploitation-videoprotection-dspap.pdf, consulté le 4 janvier 2016.

Monenti Bois, « Nicolas Sarkozy, Twitter et la censure », 21 février 2012, à http://tempsreel.nouvelobs.com/high-tech/20120221.OBS1927/nicolas-sarkozy-twitter-et-la-censure.html, consulté le 5 mai 2012.

O'Hagan Timothy, « Public et privé, hommes et femmes » in *Achives de Philosopie du droit, tome 41 (1997)*, pp. 43-51, à http://www.philosophie-droit.asso.fr/APDpourweb/173.pdf, consulté le 3 août 2017.

Peyrou Sylvie, « Surveillance de masse : un coup d'arrêt aux dérives de la lutte antiterroriste (CEDH, Szabo et Vissy c/ Hongrie, 12 janvier 2016) », 30 janvier 2016, à http://www.gdr-elsj.eu/2016/01/30/droits-fondamentaux/surveillance-de-masse-un-coup-darret-aux-derives-de-la-lutte-antiterroriste-cedh-szabo-et-vissy-c-hongrie-12-janvier-2016/, consulté le 12 janvier 2017.

Pigeon-Bormans Anne, « Vie privée et personnalités publiques à propos de deux arrêts de la CEDH », 1er septembre 2014 à http://pigeon-bormans.com/Vie-privee-et-personnalites.html, consulté le 2 août 2017.

Poullet Yves, Rouvroy Antoinette, « Une réévaluation de l'importance de la vie privée pour le démocratie », *actes de la conférence « Reinventing Data Protection ? »,* Bruxelles, octobre 2007, à http://www.crid.be/pdf/public/6050.pdf, consulté le 27 décembre 2016.

Rees Marc, « Loi Renseignement : l'actuel président de la CNCIS réitère ses doutes et critiques », *NextImpact*, 21 septembre 2015, à https://www.nextinpact.com/news/96585-loi-renseignement-actuel-president-cncis-reitere-ses-doutes-et-critiques.htm, consulté le 18 juillet 2017.

Rees Marc, « Injure, diffamation : au Sénat, les délais de prescription sur Internet explosent », *NextImpact,* 15 septembre 2016, à https://www.nextinpact.com/news/101368-injure-diffamation-au-senat-delais-prescription-sur-Internet-explosent.htm, consulté le 2 février 2017.

Rivière Philippe, « Cyber-attaque contre Téhéran », mars 2001, in http://www.monde-diplomatique.fr/2011/03/RIVIERE/20197 mars 2001, consulté le 5 mai 2012.

Rousselet Kathy, « La liberté de conscience en Russie : du transfert d'un concept au conflit de normes », in Sylvie Martin (dir.) *Circulation des concepts entre Occident et Russie*, [en ligne], Lyon, ENS LSH, mis en ligne le 10 décembre 2008. URL : http://institut-est-ouest.ens-lsh.fr/spip.php?article147, consulté le 20 août 2016.

Elena Scappaticci, « Droit de pétition : de quoi parle Emmanuel Macron ? », *le scan politique*, Le Figaro.fr, publié le 03 juillet 2017 à http://www.lefigaro.fr/politique/le-scan/2017/07/03/25001-20170703ARTFIG00278-droit-de-petition-de-quoi-parle-emmanuel-macron.php, consulté le 10 août 2017.

SYMANTEC, « Menace Flamer », à http://www.symantec.com/fr/fr/outbreak/?id=flamer&inid=fr_ghp_hero1_flamer, consulté le 6 juin 2012.

Türk Alex, Piazza Pierre, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Cultures & Conflits [En ligne],* 76 | hiver 2009 03 mai 2011, consulté le 06 janvier 2013, à http://conflits.revues.org/17806 .

Tréguer Félix, « Feu vert à la surveillance de masse », *Le Monde diplomatique*, juin 2015, pp. 1, 4-5, disponible en ligne à https://www.monde-diplomatique.fr/2015/06/TREGUER/53056, consulté le 13 juillet 2017.

Urvoas Jean-Jacques, « Contre le "fichier des honnêtes gens" », 6 mars 2012, à http://www.urvoas.bzh/2012/03/06/contre-le-fichier-des-honnetes-gens/, consulté le 27 juin 2017.

Voisset Michèle, « Droit au respect de la vie privée et société de l'information », in Tabatoni (dir.) *La protection de la vie privée dans la société d'information*, Presses Universitaires de France, pp. 249-254, à http://asmp.fr/travaux/gpw/Internetvieprivee/rapport3/chapitr16.pdf, consulté le 1er juillet 2016.

Principaux textes juridiques français

Constitution du 4 octobre 1958.

Déclaration des droits de l'Homme et du citoyen du 26 août 1789.

Textes législatifs

Loi du 30 juin 1881 *sur la liberté de réunion.*

Loi du 29 juillet 1881 *sur la liberté de la presse.*

Loi du 12 décembre 1893 *portant modification des articles 24, paragraphe 1er, 25 et 49 de la loi du 29 juillet 1881.*

Loi du 1er juillet 1901 *relative au contrat d'association.*

Loi du 9 décembre 1905 *concernant la séparation des Églises et de l'État.*

Loi du 28 mars 1907 *relative aux réunions publiques.*

Loi nº 50-10 du 6 janvier 1950 *portant modification et codification des textes relatifs aux pouvoirs publics.*

Loi nº 52-336 du 25 mars 1952 *modifiant certaines dispositions de la loi du 29 juillet 1881 sur la liberté de la presse.*

Loi nº 52-1352 du 19 décembre 1952 *modifiant les articles 25, 30, 35 de la loi du 29 juillet 1881 sur la liberté de la presse.*

Loi nº 53-184 du 12 mars 1953 *modifiant les articles 39 et 48 de la loi du 29 juillet 1881 sur la liberté de la presse.*

Loi nº 55-385 du 3 avril 1955 *instituant un état d'urgence et en déclarant l'application en Algérie.*

Loi nº 55-1552 du 28 novembre 1955 complétant la loi du 29 juillet 1881 sur la liberté de la presse.

Loi nº 58-92 du 4 février 1958 *complétant l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse.*

Loi nº70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens.*

Loi nº 72-546 du 1er juillet 1972 *relative à la lutte contre le racisme*.

Loi nº 77-808 du 19 juillet 1977 *relative à la publication et à la diffusion de certains sondages d'opinion.*

Loi nº 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés.*

Loi nº 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.*

Loi nº 86-1020 du 9 septembre 1986 *relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État.*

Loi nº 88-19 du 5 janvier 1988*, relative à la fraude informatique.*

Loi nº 90-615 du 13 juillet 1990 *tendant à réprimer tout acte raciste, antisémite ou xénophobe.*

Loi nº 90-1170 du 29 décembre 1990 *sur la réglementation des télécommunications.*

Loi nº 91-646 du 10 juillet 1991 *relative au secret des correspondances émises par la voie des télécommunications.*

Loi nº 92-1336 du 16 décembre 1992 *relative à l'entrée en vigueur du nouveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur.*

Loi nº 94-548 du 1er juillet 1994 *relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libert*és.

Loi nº95-73 du 21 janvier 1995 *d'orientation et de programmation relative à la sécurité.*

Loi nº 96-647 du 22 juillet 1996 *tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire.*

Loi nº 96-659 du 26 juillet 1996 *de réglementation des télécommunications*.

Loi nº 98-468 du 17 juin 1998 *relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.*

Loi nº 2000-230 du 13 mars 2000 *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.*

Loi nº 2000-516 du 15 juin 2000 *renforçant la protection de la présomption d'innocence et les droits des victimes.*

Loi nº 2001-504 du 12 juin 2001 *tendant à renforcer la prévention et la répression des mouvements sectaires portant atteinte aux droits de l'homme et aux libertés fondamentales.*

Loi nº 2001-1 062 du 15 novembre 2001 *relative à la sécurité quotidienne.*

Loi nº 2002-1 094 du 29 août 2002 *d'orientation et de programmation pour la sécurité intérieure (LOPSI).*

Loi nº 2002-1 138 du 9 septembre 2002 *d'orientation et de programmation pour la justice*.

Loi nº 2003-239 du 18 mars 2003 *pour la sécurité intérieure.*

Loi nº 2004-204 du 9 mars 2004 *portant adaptation de la justice aux évolutions de la criminalité.*

Loi nº 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique.*

Loi nº 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 nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

Loi nº 2004-1 343 du 9 décembre 2004 *de simplification du droit.*

Loi nº 2005-1 549 du 12 décembre 2005 *relative au traitement de la récidive des infractions pénales.*

Loi nº 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.*

Loi nº 2006-961 du 1er août 2006 *relative au droit d'auteur et aux droits voisins dans la société de l'information*.

Loi nº 2007-1 443 du 9 octobre 2007 *portant création d'une délégation parlementaire au renseignement.*

Loi nº 2007-1 544 du 29 octobre 2007 *de lutte contre la contrefaçon.*

Loi nº 2007-1 598 du 13 novembre 2007 *relative à la lutte contre la corruption.*

Loi nº2007-1787 du 20 décembre 2007 *relative à la simplification du droit.*

Loi nº 2008-1 245 du 1er décembre 2008 *visant à prolonger l'application des articles 3, 6 et 9 de la loi nº 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*

Loi nº 2009-526 du 12 mai 2009 *de simplification et de clarification du droit et d'allègement des procédures.*

Loi nº 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur Internet.*

Loi nº 2009-1 311 du 28 octobre 2009 *relative à la protection pénale de la propriété littéraire et artistique sur Internet.*

Loi nº 2010-1 du 4 janvier 2010 *relative à la protection du secret des sources des journalistes.*

Loi nº 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure* dite LOPPSI 2.

Loi nº 2011-302 du 22 mars 2011 *portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques.*

Loi nº 2011-2012 du 29 décembre 2011 *relative au renforcement de la sécurité du médicament et des produits de santé (loi Bertrand).*

Loi nº 2012-410 du 27 mars 2012 *relative à la protection de l'identité.*

Loi nº 2012-954 du 6 août 2012 *relative au harcèlement sexuel.*

Loi nº 2012-1 432 du 21 décembre 2012 *relative à la sécurité et à la lutte contre le terrorisme.*

Loi nº 2013-316 du 16 avril 2013 *relative à l'indépendance de l'expertise en matière de santé et d'environnement et à la protection des lanceurs d'alerte (loi Blandin).*

Loi nº 2013-711 du 5 août 2013 *portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne et des engagements internationaux de la France.*

Loi n º 2013-907 du 11 octobre 2013 *relative à la transparence de la vie publique.*

Loi du 6 décembre 2013 nº 2013-1 117 *relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière.*

Loi nº 2013-1 168 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.*

Loi nº 2014-56 du 27 janvier 2014 *visant à harmoniser les délais de prescription des infractions prévues par la loi sur la liberté de la presse du 29 juillet 1881, commises en raison du sexe, de l'orientation ou de l'identité sexuelle ou du handicap.*

Loi nº 2014-372 du 28 mars 2014 *relative à la géolocalisation.*

Loi nº 2014-1 353 du 13 novembre 2014 *renforçant les dispositions relatives à la lutte contre le terrorisme.*

Loi nº 2015-912 du 24 juillet 2015 *relative au renseignement.*

Loi nº 2015-1 501 du 20 novembre 2015 *prorogeant l'application de la loi nº 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions.*

Loi nº 2015-1 556 du 30 novembre 2015 *relative aux mesures de surveillance des communications électroniques internationales.*

Loi nº 2016-508 du 25 avril 2016 *de modernisation de diverses règles applicables aux élections.*

Loi nº 2016-731 du 3 juin 2016 *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.*

Loi nº 2016-987 du 21 juillet 2016 *prorogeant l'application de la loi nº 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.*

Loi nº 2016-1 321 du 7 octobre 2016 *pour une République numérique.*

Loi nº 2016-1 691 du 9 décembre 2016 *relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.*

Loi nº 2017-56 du 20 janvier 2017 *portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes.*
Loi nº 2017-86 du 27 janvier 2017 *relative à l'égalité et à la citoyenneté.*
Loi nº 2017-1 154 du 11 juillet 2017 *prorogeant l'application de la loi nº 55-385 du 3 avril 1955 relative à l'état d'urgence.*

Textes réglementaires

Ordonnance du 6 mai 1944 *relative à la répression des délits de presse.*
Ordonnance du 26 août 1944 *sur l'organisation de la presse française.*
Ordonnance nº 58-1100 du 17 novembre 1958 *relative au fonctionnement des assemblées parlementaires.*
Ordonnance nº 2001-741 du 23 août 2001 *portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation.*
Ordonnance nº 2010-379 du 14 avril 2010 *relative à la santé des sportifs et à la mise en conformité du code du sport avec les principes du code mondial antidopage.*
Ordonnance nº 2012-351 du 12 mars 2012 *relative à la partie législative du code de la sécurité intérieure.*
Ordonnance nº 2015-1 341 du 23 octobre 2015 *relative aux dispositions législatives du code des relations entre le public et l'administration*.
Ordonnance nº 2016-131 du 10 février 2016 *portant réforme du droit des contrats, du régime général et de la preuve des obligations*.
Décret-loi du 18 avril 1939 *fixant le régime des matériels de guerre, armes et munitions.*
Décret nº 73-364 du 12 mars 1973 *relatif à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions.*
Décret nº 86-250 du 18 février 1986, *portant modification du décret nº 73 — 364 du 12 mars 1973 relatif à l'application du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions.*
Décret nº 98-101 du 24 février 1998 *définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.*
Décret nº 98-102 du 24 février 1998 *définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications.*

Décret nº 98-206 du 23 mars 1998 *définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.*

Décret nº 98-207 du 23 mars 1998 *définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.*

Décret n º 99-1047 du 14 décembre 1999 *pris pour l'application de l'article 107 de la loi de finances pour 1999 (nº 98-1266 du 30 décembre 1998) relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par la direction générale des impôts, la direction générale de la comptabilité publique et la direction générale des douanes et droits indirects.*

Décret nº 99-200 du 17 mars 1999 *définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.*

Décret nº 2000-8 du 4 janvier 2000 *pris pour l'application de l'article L.288 du livre des procédures fiscales.*

Décret nº 2001-272 du 30 mars 2001 *pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.*

Décret nº2001-583 du 5 juillet 2001 *pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées.*

Décret nº 2002-36 du 8 janvier 2002 *relatif à certaines clauses types des cahiers des charges annexés aux autorisations délivrées en application de l'article L.33-1 du code des postes et télécommunications*.

Décret nº 2002-535 du 18 avril 2002 *relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.*

Décret nº 2003-752 du 1er août 2003 *relatif aux annuaires universels et aux services universels de renseignements et modifiant le code des postes et télécommunications.*

Décret nº 2003-755 du 1er août 2003 *modifiant le code des postes et télécommunications.*

Décret nº 2006-358 du 24 mars 2006 *relatif à la conservation des données des communications électroniques.*

Décret nº 2006-1 258 du 14 octobre 2006 *modifiant le décret nº 2001-583 du 5 juillet 2001 portant création du système de traitement des infractions constatées dénommé « STIC ».*

Décret nº2006-1411 du 20 novembre 2006 *portant création du système judiciaire de documentation et d'exploitation dénommé « JUDEX ».*

Décret nº 2007-663 du 2 mai 2007 *pris pour l'application des articles 30, 31 et 36 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie.*

Décret nº2009-1773 du 29 décembre 2009 *relatif à l'organisation de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet.*

Décret nº 2010-569 du 28 mai 2010 *relatif au fichier des personnes recherchées.*

Décret nº 2012-652 du 4 mai 2012 *relatif au traitement d'antécédents judiciaires.*

Décret nº 2012-687 du 7 mai 2012 *relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle.*

Décret nº 2012-689 du 7 mai 2012 *relatif aux conditions de mise en œuvre des fichiers d'analyse sérielle et des logiciels de rapprochement judiciaire.*

Décret nº 2014-1 050 du 16 septembre 2014 *instituant un administrateur général des données.*

Décret nº 2015-26 du 14 janvier 2015 *relatif à l'interdiction de sortie du territoire des ressortissants français projetant de participer à des activités terroristes à l'étrange*r.

Décret nº 2015-253 du 4 mars *2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique*.

Décret nº 2015-1 475 du 14 novembre 2015 *portant application de la loi nº 55-385 du 3 avril 1955.*

Décret nº 2016-1 460 du 28 octobre 2016 *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.*

Arrêté du 13 mars 1998 *définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie*.

Arrêté du 13 mars 1998 *définissant le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis à autorisation.*

Arrêté du 13 mars 1998 *fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes.*

Arrêté du 13 mars 1998 *fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes.*

Arrêté du 13 mars 1998 *fixant le tarif forfaitaire pour la mise en œuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi nº 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications*.

Arrêté du 30 mai 2006 *portant extension de l'accord national interprofessionnel relatif au télétravail.*

Arrêté du 1er septembre 2009 *portant création d'un traitement automatisé de données à caractère personnel dénommé « Système d'information décisionnel du système d'immatriculation des véhicules ».*

Circulaire du 26 mai 2011 *relative à la création du portail unique des informations publiques de l'État « data.gouv.fr » par la mission « Etalab » et l'application des dispositions régissant le droit de réutilisation des informations publiques.*

Circulaire du 14 septembre 2011 *relative au cadre juridique applicable à l'installation de caméras de vidéoprotection sur la voie publique et dans des lieux ou établissements ouverts au public, d'une part, et dans des lieux non ouverts au public, d'autre part*, NOR : PRMX1124533C.

Circulaire du 18 août 2014 *relative aux fichiers d'antécédents judiciaires,* NOR : JUSD1419980C.

Circulaire du 5 décembre 2014 *de présentation de la loi nº 2014-1 353 renforçant les dispositions relatives à la lutte contre le terrorisme — Renforcement de la coordination de la lutte antiterroriste* NOR : JUSD1429083C.

Codes

Code civil.

Code de procédure pénale.

Code de la consommation.

Code de la sécurité intérieure.

Code des postes et communications électroniques.

Code des relations entre le public et l'administration.

Code général des collectivités territoriales.

Code monétaire et financier.

Code pénal.

Principaux textes européens

Traité instituant la Communauté européenne ou Traité de Rome du 25 mars 1957, devenu le traité sur le fonctionnement de l'Union européenne selon le « traité modificatif » signé le 13 décembre 2007 à Lisbonne, dit traité de Lisbonne.

Conseil de l'Europe

Conseil de l'Europe, *Convention de sauvegarde des droits de l'homme et des libertés fondamentales,* Rome, 4 novembre 1950.

Conseil de l'Europe, traité nº 108, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 janvier 1981.

Conseil de l'Europe*, Convention sur la cybercriminalité, STCE nº 185* Budapest, 23 novembre 2001.

Conseil de l'Europe, Assemblée parlementaire, Commission des questions juridiques et des droits de l'homme, *La protection des mineurs contre les dérives sectaires*, Doc. 13 441, 17 mars 2014.

Règlements de l'Union européennes

Règlement (CE) nº 44/2001 du Conseil du 22 décembre 2000 *concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.*

Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.*

Règlement (CE) nº 2201/2003 du Conseil du 27 novembre 2003 relatif à la compétence, la reconnaissance et l'exécution des décisions en matière matrimoniale et en matière de responsabilité parentale abrogeant le règlement (CE) nº 1347/2000.

Règlement (CE) nº 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (« Rome II »). Règlement (CE) nº 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I)

Règlement (UE) nº 1259/2010 du Conseil du 20 décembre 2010 mettant en œuvre une coopération renforcée dans le domaine de la loi applicable au divorce et à la séparation de corps.

Règlement (UE) nº 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 (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).*

Directives de l'Union européenne

Directive 89/397/CEE du Conseil du 14 juin 1989 *relative au contrôle officiel des denrées alimentaires.*

Directive 93/13/CEE du Conseil du 5 avril 1993 *concernant les clauses abusives dans les contrats conclus avec les consommateurs.*

Directive 1999/2/CE du Parlement européen et du Conseil du 22 février 1999 *relative au rapprochement des législations des États membres sur les denrées et ingrédients alimentaires traités par ionisation.*

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.*

Directive 95/53/CE du Conseil du 25 octobre 1995 *fixant les principes relatifs à l'organisation des contrôles officiels dans le domaine de l'alimentation animale.*

Directive 96/71/CE du Parlement européen et du Conseil du 16 décembre 1996 *concernant le détachement de travailleurs effectué dans le cadre d'une prestation de services.*

Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 *concernant la protection des consommateurs en matière de contrats à distance.*

Directive 97/55/CE du Parlement européen et du Conseil du 6 octobre 1997 *modifiant la directive 84/450/CEE sur la publicité trompeuse afin d'y inclure la publicité comparative.*

Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.*

Directive 98/27/CE du Parlement européen et du Conseil du 19 mai 1998 *relative aux actions en cessation en matière de protection des intérêts des consommateurs.*

Directive 1999/20/CE du 22 mars 1999 du Conseil *modifiant les directives 70/524/CEE concernant les additifs dans l'alimentation des animaux, 82/471/CEE concernant certains produits utilisés dans l'alimentation des animaux, 95/53/CE fixant les principes relatifs à l'organisation des contrôles officiels dans le domaine de l'alimentation animale et 95/69/CE établissant les conditions et modalités applicables à l'agrément et à l'enregistrement de certains établissements et intermédiaires dans le secteur de l'alimentation animale.*

Directive 1999/44/CE du Parlement européen et du Conseil du 25 mai 1999 *sur certains aspects de la vente et des garanties des biens de consommation.*

Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999*, sur un cadre communautaire pour les signatures électroniques.*

Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »).*

Directive 2000/77/CE du 14 décembre 2000 du Parlement européen et du Conseil *modifiant la directive 95/53/CE du Conseil fixant les principes relatifs à l'organisation des contrôles officiels dans le domaine de l'alimentation animale.*

Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 *sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.*

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).*

Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 *concernant la réutilisation des informations du secteur public.*

Directive 2004/82/CE du Conseil du 29 avril 2004 *concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.*

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.*

Directive 2007/2/CE du Parlement européen et du Conseil *établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE).*

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.

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.*

Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.*

Directive (UE) 2016/1 148 du Parlement européen et du Conseil du 6 juillet 2016 *concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.*

Commission et Parlement européen

European Commission, COM (2016) 117 final, Communication from the Commission to the European Parliement and the Council Transatlantic, "*Data Flows : Restoring Trust through Strong Safeguards*", February 29, 2016.

Parlement européen, *Protection des personnes physiques à l'égard du traitement des données à caractère personnel,* P8_TA (2016) 0125, texte adopté le 14 avril 2016.

Parlement européen, *Traitement des données à caractère personnel à des fins de prévention des infractions pénales,* P8_TA (2016) 0126, texte adopté le 14 avril 2016.

Parlement européen, *Utilisation des données des passagers (UE-PNR)*, P8_TA (2016) 0127, texte adopté le 14 avril 2016.

Résolution du Parlement européen *sur la liberté d'expression sur Internet*, P6_TA/2006/0324 du 6 juillet 2006.

Traités européens et internationaux

Accord - cadre européen *sur le télétravail* signé le 16 juillet 2002 par les partenaires sociaux (CES, l'UNICE/UEAPME et le CEEP).

Charte des droits fondamentaux de l'Union européenne (2000/C 364/01), 18 décembre 2000.

Convention européenne des droits de l'homme, Rome, novembre 1950, amendée par les Protocoles n^{os} 11 et 14, complétée par le Protocole additionnel et les Protocoles nos 4, 6, 7, 12 et 13.

Convention européenne des droits de l'homme, 3 septembre 1953.

Convention américaine relative aux droits de l'homme, San José, Costa Rica, 22 novembre 1969.

Déclaration universelle des droits de l'homme, 10 décembre 1948.

Nations unies, *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 2 200 A (XXI) du 16 décembre 1966.

Nation unies, *Projet de déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux : les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation, Douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale Salvador (Brésil),* 12-19 avril 2010.

Traité instituant la Communauté européenne ou Traité de Rome du 25 mars 1957, devenu le traité sur le fonctionnement de l'Union européenne selon le « traité modificatif » signé le 13 décembre 2007 à Lisbonne, dit traité de Lisbonne.

Jurisprudence

Conseil constitutionnel

Conseil constitutionnel, Décision nº 71-44 DC du 16 juillet 1971 - Loi *complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association.*

Conseil constitutionnel, Décision nº 76-75 DC du 12 janvier 1977 - *Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales.*

Conseil constitutionnel, Décision nº 84-181 DC du 11 octobre 1984 - *Loi visant à limiter la concentration et à assurer la transparence financière et le pluralisme des entreprises de presse.*

Conseil constitutionnel, Décision nº 86-213 DC du 03 septembre 1986 - *Loi relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État.*

Conseil constitutionnel, Décision nº 89-257 DC du 25 juillet 1989 - *Loi modifiant le code du travail et relative à la prévention du licenciement économique et au droit à la conversion.*

Conseil constitutionnel, Décision nº 93-325 DC du 13 août 1993 - *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France.*

Conseil constitutionnel, Décision nº 94-352 DC du 18 janvier 1995 - *Loi d'orientation et de programmation relative à la sécurité.*

Conseil constitutionnel, Décision nº 96-377 DC du 16 juillet 1996 - *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire.*

Conseil constitutionnel, Décision nº 98-405 DC du 29 décembre 1998 - *Loi de finances pour 1999.*

Conseil constitutionnel, Décision nº 99-416 du 23 juillet 1999 - *Loi portant création d'une couverture maladie universelle.*

Conseil constitutionnel, Décision nº 2003-467 DC du 13 mars 2003 - *Loi pour la sécurité intérieure.*

Conseil constitutionnel, Décision nº 2004-492 DC du 02 mars 2004 - *Loi portant adaptation de la justice aux évolutions de la criminalité.*

Conseil constitutionnel, Décision nº 2004-496 DC du 10 juin 2004 - *Loi pour la confiance dans l'économie numérique.*

Conseil constitutionnel, Décision 2005-532 DC du 19 janvier 2006 - *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.*

Conseil constitutionnel, Décision nº 2006-540 DC du 27 juillet 2006 - *Loi relative au droit d'auteur et aux droits voisins dans la société de l'information.*

Conseil constitutionnel, décision nº 2009-580 DC du 10 juin 2009 - *Loi favorisant la diffusion et la protection de la création sur Internet.*

Conseil constitutionnel, Décision nº 2009-590 DC du 22 octobre 2009 - *Loi relative à la protection pénale de la propriété littéraire et artistique sur Internet.*

Conseil constitutionnel, Décision nº 2010-604 DC du 25 février 2010 - *Loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public.*

Conseil constitutionnel, Décision nº 2011-625 DC du 10 mars 2011 - *Loi d'orientation et de programmation pour la performance de la sécurité intérieure.*

Conseil constitutionnel, Décision nº 2012-652 DC du 22 mars 2012 - *Loi relative à la protection de l'identité.*

Conseil constitutionnel, Décision nº 2014-693 DC du 25 mars 2014 - *Loi relative à la géolocalisation.*

Conseil constitutionnel, Décision nº 2015-713 DC du 23 juillet 2015 - *Loi relative au renseignement.*

Conseil constitutionnel, Décision nº 2015-722 DC du 26 novembre 2015 - *Loi relative aux mesures de surveillance des communications électroniques internationales.*

Conseil constitutionnel, Décision nº 2010-25 QPC du 16 septembre 2010, *M. Jean-Victor C. [Fichier empreintes génétiques]*.

Conseil constitutionnel, Décision nº 2010-45 QPC du 06 octobre 2010, *M. Mathieu P. [Noms de domaine Internet]*.

Conseil constitutionnel, Décision nº 2011-131 QPC du 20 mai 2011, *Mme Térésa C. et autre [Exception de vérité des faits diffamatoires de plus de dix ans]*.

Conseil constitutionnel, Décision nº 2013-319 QPC du 7 juin 2013, *M. Philippe B. [Exception de vérité des faits diffamatoires constituant une infraction amnistiée ou prescrite, ou ayant donné lieu à une condamnation effacée par la réhabilitation ou la révision]*.

Conseil constitutionnel, Décision nº 2013-345 QPC du 27 septembre 2013, *Syndicat national Groupe Air France CFTC [Communication syndicale par voie électronique dans l'entreprise]*.

Conseil constitutionnel, Décision nº 2014-439 QPC du 23 janvier 2015, *M. Ahmed S. [Déchéance de nationalité]*.

Conseil constitutionnel, Décision nº 2015-463 QPC du 09 avril 2015, *M. Kamel B. et autre [Direction d'une entreprise exerçant des activités privées de sécurité - Condition de nationalité]*.

Conseil constitutionnel, Décision nº 2015-492 QPC du 16 octobre 2015, *Association Communauté rwandaise de France [Associations pouvant exercer les droits reconnus à la partie civile en ce qui concerne l'apologie des crimes de guerre et des crimes contre l'humanité]*.

Conseil constitutionnel, Décision nº 2015-527 QPC du 22 décembre 2015 *M. Cédric D. [Assignations à résidence dans le cadre de l'état d'urgence]*.

Conseil constitutionnel, Décision nº 2016-590 QPC du 21 octobre 2016, *La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne]*.

Conseil constitutionnel, Décision nº 2016-611 QPC du 10 février 2017, *M. David P. [Délit de consultation habituelle de sites Internet terroristes]*.

Cour européenne des droits de l'homme

Cour européenne des droits de l'homme (plénière), Arrêt du 7 décembre 1976, Requête nº 5493/*72 Handyside c/ Royaume-Uni.*

Cour européenne des droits de l'homme, Arrêt du 6 septembre 1978, Requête nº 529/71, *Klass et autres c/ Allemagne.*

Cour européenne des droits de l'homme, Arrêt du 6 novembre 1980, Requête nº 7367/76, *Affaire Guzzardi c/ Italie*.

Cour européenne de droits de l'homme (chambre plénière), Arrêt du 2 août 1984, Requête nº 8 691/79, *Affaire Malone v. the United Kingdom* .

Cour européenne des droits de l'homme, Arrêt du 24 avril 1990, Requête nº11105/84, *Affaire Kruslin c/ France*, Requête nº11801/85, *Affaire Huvig c/ France* .

Cour européenne des droits de l'homme, Arrêt du 26 avril 1991, Requête nº 11800/85, Affaire *Ezelin c/ France* .

Cour européenne des droits de l'homme, Arrêt du 26 novembre 1991, série A nº 216, *Observer et Guardian Newspapers Ltd c/ Royaume-Uni.*

Cour européenne des droits de l'homme, Arrêt du 27 mars 1996, Requête nº 17488/90, *Affaire Goodwin c/Royaume-Uni*.

Cour européenne des droits de l'homme, Arrêt du 25 juin 1996, Requête nº 19776/92, *Affaire Amuur c/ France*.

Cour européenne des droits de l'homme, Arrêt du 21 janvier 1999*,* Requête nº 29183/95, *Affaire Fressoz et Roire c/ France, plus communément appelé l'affaire du canard enchainé*.

Cour européenne des droits de l'homme, Arrêt du 20 mai 1999*,* Requête nº 21980/93, *Affaire Bladet Tromsø et Stensaas c/ Norvège.*

Cour européenne des droits de l'homme, Arrêt du 2 août 2001, Requête nº 44955/98, *Affaire Mancini c/ Italie.*

Cour européenne des droits de l'homme, Décision du 6 novembre 2001 *sur la recevabilité de la requête nº 53430/99 présentée par la Fédération Chrétienne des Témoins de Jéhovah de France contre la France*.

Cour européenne des droits de l'homme, Arrêt du 17 décembre 2002, Requête nº 35373/97, *Affaire A. c/ Royaume-Uni*.

Cour européenne des droits de l'homme, Arrêt du 30 janvier 2003, Requête nº 40877/98, *Affaire Cordova c/ Italie (nº 1)*.

Cour européenne des droits de l'homme, Arrêt du 4 décembre 2003, Requête nº 35071/97, *Affaire Gündüz c/ Turquie.*

Cour européenne des droits de l'homme, Arrêt du 16 juin 2005, Requête nº 61603/00, *Affaire Storck c/ Allemagne*.

Cour européenne des droits de l'homme, Arrêt du 31 mai 2005, Requête nº 59842/00, *Affaire Vetter c/ France*.

Cour européenne des droits de l'homme, Arrêt du 8 décembre 2008, Requêtes nº 30562/04 et 30 566/04, *Affaire S. et MARPER c/ Royaume-Uni*.

Cour européenne des droits de l'homme, 4e Section, Arrêt du 15 décembre 2009, Requête nº 821/03, *Affaire Financial Times LTD et autres c/ Royaume-Uni*.

Cour européenne des droits de l'homme, décision du 10 juin 2010, *Témoins de Jéhovah c/ Russie*.

Cour européenne des droits de l'homme, Arrêt du 2 septembre 2010, Requête nº 35623/05, *Affaire Uzun c/ Allemagne*.

Cour européenne des droits de l'homme, Arrêt du 30 juin 2011, Requête nº 8916/05, *Association Les Témoins de Jéhovah c/ France*.

Cour européenne des droits de l'homme, Arrêt du 18 mars 2013, Requête nº 3111/10, Affaire *Ahmet Yildirim c/ Turquie*.

Cour européenne des droits de l'homme, Arrêt du 18 septembre 2014, Requête nº 21010/10, Affaire *Brunet c/ France*.

Cour européenne des droits de l'homme, Arrêt du 2 octobre 2014, Requête nº 10609/10, Affaire *Matelly c/ France.*

Cour européenne des droits de l'homme, Grande chambre, Arrêt du 16 juin 2015, Requête nº 64569/09, *Affaire Delfi c/ Estonie*.

Cour européenne des droits de l'homme, Arrêt du 20 octobre 2015, Requête nº 5201/11, Affaire *Sher et autres c/ Royaume-Uni*.

Cour européenne des droits de l'homme (Grande chambre), Arrêt du 10 novembre 2015, *R*equête nº 40454/07, Affaire *Couderc et Hachette Filipacchi associés c/ France.*

Cour européenne des droits de l'homme, Arrêt du 4 décembre 2015, Requête nº 47143/06, Affaire *Roman Zakharov c/ Russie*.

Cour européenne des droits de l'homme, Arrêt du 12 janvier 2016, Requête nº 37138/14, *Affaire Szabo et Vissy c/ Hongrie*.

Cour européenne des droits de l'homme, Arrêt du 27 octobre 2016, Requêtes nos 4 696/11 et 4 703/11, Affaire *Les Authentiks et Supras Auteuil 91 c/ France*.

Cour européenne des droits de l'homme, Arrêt du 22 juin 2017, Requête nº 8806/12, Affaire *Aycaguer c/ France*.

Cour de justice de l'Union européenne

Cour de justice de la Communauté européenne, arrêt du 21 juin 1974, affaire 2/74, *Reyner contre État belge*.

Cour de justice de la Communauté européenne, arrêt du 3 décembre 1974, , Affaire 33/74, *Johannes Henricus Maria van Binsbergen contre Bestuur van de Bedrijfsvereniging voor de Metaalnijverheid.*

Cour de justice de l'Union européenne, grande chambre, Arrêt du 30 mai 2006, affaires jointes C-317/04 et C-318/04, *Parlement européen c/ Commission et c. Conseil*.

Cour de justice de l'Union européenne (Grande chambre), Arrêt du 29 janvier 2008, Affaire c-275/06, *Productores de Música de España (Promusicae) c/Telefónica de España SAU*.

Cour de justice de l'Union européenne, Arrêt du 25 octobre 2011, affaires jointes C-509/09 et C-161/10, *eDate Advertising GmbH e.a. c/ X et Société MGN Limited*.

Cour de justice de l'Union européenne, quatrième chambre, Arrêt du 3 octobre 2013, Demande de décision préjudicielle, introduite par la Cour de cassation (France), Affaire C-170/12, *Peter Pinckney contre KDG Mediatech AG*.

Cour de justice de l'Union européenne, Arrêt du 14 novembre 2013, Affaire C-478/12, *Armin Maletic et Marianne Maletic c/ lastminute.com Gmbh et TUI Österreich GmbH.*

Cour de justice de l'Union européenne, 8e chambre, Arrêt du14 novembre 2013, Affaire nºC-478/12, *M. et Mme Maletic c/lastminute.com GmbH et TUI Osterreich*.

Cour de justice de l'Union européenne, Arrêt du 8 avril 2014, Affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlande, et Kärntner Landesregierung*.

Cour de justice de l'Union européenne (grande chambre), Arrêt du 13 mai 2014, Affaire C-131/12, *Google Spain SL, Google Inc. c/Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

Cour de justice de l'Union européenne (assemblée plénière), Avis 2/13 du 18 décembre 2014, « *Avis rendu en vertu de l'article 218, paragraphe 11, TFUE – Projet d'accord international – Adhésion de l'Union européenne à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales – Compatibilité dudit projet avec les traités UE et FUE* ».

Cour de justice de l'Union européenne, troisième chambre, Arrêt du 1er octobre 2015, Affaire C-201/14, *Smaranda Bara e.a. c/ Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF).*

Cour de justice de l'Union européenne, Arrêt du 1er octobre 2015, Affaire C-230/14, *Weltimmo*.

Cour de justice de l'Union européenne (grande chambre), Arrêt du 6 octobre 2015, Affaire C-362/14, *Maximillian Schrems c/ Data Protection Commissioner*.

Cour de justice de l'Union européenne, Arrêt du 8 avril 2017, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger e.a.*

Tribunal de justice de l'Union européenne, Avis 1/15 de la Cour (grande chambre), 26 juillet 2017.

Conseil d'État

Conseil d'État, 10e et 9e sous-sections réunies, décision du 23/05/2007, nº288149.

Conseil d'État, Section de l'intérieur - Avis nº 385.125 - 24 mai 2011, *Champs d'application respectifs de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.*

Conseil d'État, Assemblée, 26 octobre 2011, n^{os} 317827 et autres, *Association pour la promotion de l'image et autres*.

Conseil d'État, Décision du 8 février 2012, n^{o} 353357, *M. Mélenchon*.

Conseil d'État, Décision du 16 octobre 2013, n° 351115, 351116, 351152, 351153, 351220, 354484, 354485, 354507, 354508, *Garde des Sceaux, ministre de la justice et des libertés c/ m. n... et autres*.

Conseil d'État, Ordonnance du 9 janvier 2014, n^{o} 374508, *ministre de l'intérieur c/Société Les Productions de la Plume et M. Dieudonné M'Bala M'Bala.*

Conseil d'État, Avis consultatif n^{o} 389754 du 12 mars 2015, *Projet de loi relatif au renseignement.*

Conseil d'État, Ordonnance du 23 décembre 2015, n^{o} 395229, *M. B...*

Conseil d'État, Section de l'intérieur, Avis n^{o} 390180 du 23 février 2016*, relatif à la possibilité de créer un fichier regroupant les données relatives aux cartes nationales d'identité et aux passeports.*

Cour de cassation

Cour de cassation, Chambre criminelle, arrêt du 8 juin 1993, pourvoi n^{o} 89-83 298.

Cour de cassation, Chambre criminelle, arrêt du 27 juin 1995, pourvoi n^{o} 93-82.552.

Cour de cassation, Première chambre civile, arrêt du 28 février 2006, pourvois N^{o} 05-15.824 et 05-16.002.

Cour de Cassation, Chambre criminelle, arrêt du 5 septembre 2007, pourvoi n^{o} 07-81.031.

Cour de cassation, Première chambre civile, arrêt du 19 juin 2008, pourvoi n^{o} 07-14.277.

Cour de cassation, 1ère chambre civile, arrêt du11 février 2010, pourvoi n^{o} 08-22.111.

Cour de cassation, Chambre criminelle, arrêt du 29 juin 2011, pourvoi n^{o} 10-85.479, *Affaire Schoering-Plough - DGCCRF.*

Cour de cassation, civile, chambre sociale, arrêt du 3 novembre 2011, pourvoi 10-18.036.

Cour de cassation, chambre criminelle, Audience publique du 16 octobre 2013, pourvois n° 03-83910, 05-82121, 12-81532, *I-M. Alain X., Mme Aline Y., épouse Z.*

Cour de cassation, Chambre criminelle, Audience publique du 22 octobre 2013, pourvoi n° 13-81.945, *M. Mohamed X.*

Cour de cassation, Chambre criminelle, Audience publique du 22 octobre 2013, pourvoi n° 13-81.949, *M. Yohan X.*

Cour de cassation, chambre civile 1, arrêt du 22 janvier 2014, pourvoi n°10-15.890, *M. Pinckney c/ KDG Mediatech*.

Cour de cassation, chambre civile 1, arrêt du 22 janvier 2014, pourvoi n° 11-24019, *Samuel X. C. BBC.*

Cour de cassation, chambre civile 1, arrêt du 22 janvier 2014, pourvoi n° 11-26822, *Korda c/ Onion/The Onion.*

Cour de cassation, Chambre sociale, arrêt du 26 janvier 2016, pourvoi n° 14-15.360.

Cour de cassation, Chambre criminelle, arrêt du 22 mars 2016, pourvoi n° 15-83.207, *M. Gilbert X.*

Cour de cassation, Chambre criminelle, arrêt du 12 juillet 2016, pourvoi n° 15-86645, *Mme Agness X.*

Cour de cassation, 1ère chambre civile, arrêt du 3 novembre 2016, *Cabinet Peterson / Groupe Logisneuf et autres.*

Juridictions judiciaires

Chambre de l'instruction de la cour d'appel de Paris, arrêt n° 5, 7 mai 2015.

Cour d'Appel de Paris, Chambre 04 A, jugement n°06/07506 du 4 avril 2007.

Cour d'Appel de Paris, 13e chambre, Section B, arrêt du 27 avril 2007, *Anthony G. c/SCPP*

Cour d'Appel de Paris, 13e chambre, Section A, arrêt du 15 mai 2007, *Henri S. c/HCPP.*

Cour d'appel de Paris, arrêt du 29 septembre 2016, *Orange / Sud PTT.*

Tribunal de Grande Instance de Paris, Ordonnance de référé du 22 mai 2000, *UEJF et Licra c/Yahoo! Inc. et Yahoo France.*

Tribunal de grande instance de Paris, 3e chambre, 2e section, jugement n°03/08500 du 30 avril 2004.

Tribunal de grande instance de Paris 3e chambre, 3e section, Jugement du 24 juin 2009, *Jean-Yves Lafesse et autres/Google et autres.*

Tribunal de grande instance de Paris, Ordonnance de référé du 17 juillet 2014, *Chantal M./Crédit Lyonnais.*

Tribunal de Grande Instance de Paris, 17e ch. correctionnelle, jugement du 4 novembre 2016, *Messieurs X. et Y., le Procureur de la République / Monsieur Z., Ligne WEB Services et Adista.*

Tribunal correctionnel de Paris, 17e chambre correctionnelle, jugement du 13 janvier 2017, *CHIMIREC c/ Laurent NEYRET.*

Commission nationale de l'informatique et des libertés et Groupe de travail « Article 29 »

Commission nationale de l'informatique et des libertés, Délibération n o 88-120 du 08 novembre 1988 *Délibération portant avis sur la mise en œuvre conjointe par le Ministère de l'Intérieur et le Ministère de la Défense du traitement automatisé d'informations nominatives relatif au fichier des personnes recherchées (F.P.R.).*

Commission nationale de l'informatique et des libertés, Délibération nº 92-056 du 09 juin 1992, *Délibération portant avis sur le projet d'arrêté relatif au fichier des personnes recherchées géré par le Ministère de l'Intérieur et le Ministère de la Défense.*

Commission nationale de l'informatique et des libertés, Délibération nº 95-051 du 25 avril 1995, *Délibération portant avis conforme sur le projet de décret portant application au fichier des personnes recherchées des dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

Commission nationale de l'informatique et des libertés, Délibération nº 03-034 du 19 juin 2003 *portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance.*

Commission nationale de l'informatique et des libertés, *Loi informatique et libertés du 6 janvier 1978 : introduction et grands principes*, 12 janvier 2004.

Groupe de travail « Article 29 », 01613/06/FR « *Avis 9/2006 sur la mise en œuvre de la directive. 2004/82/CE du Conseil concernant l'obligation pour les transporteurs de communiquer au préalable les données relatives aux passagers (PNR) »*, adopté le 28 septembre 2006.

Commission nationale de l'informatique et des libertés , Délibération n º 2006-292 du 21 décembre 2006 *portant avis sur le projet d'arrêté portant modification de l'arrêté du 15 mai 1996 modifié relatif au fichier des personnes recherchées (FPR).*

Commission nationale de l'informatique et des libertés , Délibération nº 2007-216 du 10 juillet 2007 *autorisant la mise en œuvre, par le ministère de l'économie, des finances et de l'industrie, d'un traitement automatisé de données à caractère personnel ayant pour objet l'identification des contribuables dénommé « PERS »* (demande d'avis nº 1168820).

Commission nationale de l'informatique et des libertés, Délibération n° 2007-368 du 11 décembre 2007 *portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.*

Commission nationale de l'informatique et des libertés, Délibération nº 2009-587 du 12 novembre 2009 *portant avis sur un projet de décret en Conseil d'État relatif au fichier des personnes recherchées (FPR).*

Commission nationale de l'informatique et des libertés, *Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi d'orientation et de programmation de la performance de la sécurité intérieure (LOPPSI),* adoptée en séance plénière le 6 mai 2010.

Commission nationale de l'informatique et des libertés, *Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité,* Examinée en séance plénière le 25 octobre 2011.

Groupe de travail « Article 29 », « *Avis 02/2013 sur les applications destinées aux dispositifs intelligents du G29 »,* adopté le 27 février 2013.

Commission nationale de l'informatique et des libertés, Délibération nº 2013-404 du 19 décembre 2013 *portant avis sur un projet de loi relatif à la géolocalisation.*

Commission nationale de l'informatique et des libertés, *Les conseils de la CNIL pour mieux maîtriser la publication de photos*, 13 octobre 2014.

Article 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12*, adopted on 26 November 2014.

Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, WP 238 adopted on 13 April 2016.

Commission nationale de l'informatique et des libertés, Délibération nº 2016-292 du 29 septembre 2016 *portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (saisine nº 1979541).*

Commission nationale de l'informatique et des libertés, *Travail & vie privée — La géolocalisation des véhicules*, octobre 2016.

Commission nationale de l'informatique et des libertés, 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).

Législation étrangère

Belgique

Duquesne Antoine et Willems Luc, *Enquête parlementaire visant à élaborer une politique en vue de lutter contre les pratiques illégales des sectes et le danger qu'elles représentent pour la société et pour les personnes, particulièrement les mineurs d'âge*, Chambre des Représentants de Belgique, 313/7 - 95/96.

Cour de cassation de Belgique, Arrêt nºC.05.0494.N *État Belge contre Église universelle du Royaume de Dieu, a.s.b.l., .O. J-C., B. K., D.B.B. A. N.*, 1er juin 2006.

Italie

Constitution du royaume de Sardaigne, puis du royaume d'Italie, Statut Albertin, 1 848.

Costituzione della Repubblica Italiana (Constitution de la République italienne), 27 décembre 1947.

République Fédérale d'Allemagne

Grundgesetz für die Bundesrepublik Deutschland, GG, 23 Mai 1949.

Cour constitutionnelle fédérale d'Allemagne, Affaire *Lüth/Harlan* (Rayonnement des droits fondamentaux en droit civil), Arrêt de la Première Chambre du 15 janvier 1958 (Recueil des décisions de la Cour constitutionnelle fédérale, BVerfGE, t. 7, pp. 198-230).

Royaume-Uni

Magna Carta Libertatum (Grande Charte), 15 juin 1215.

House of Lords, *Malone v Commissioner for the Metropolis Police (nº.2),* [1979] Chancery Division 344.

Licensing Act 1662 (13 & 14 Car. II. ch. 33), *An Act for preventing the frequent Abuses in printing seditious treasonable and unlicensed Bookes and Pamphlets and for regulating of Printing and Printing Presses.*

Libel Act 1792 Chapter 60 32 Geo 3, *An Act to remove Doubts respecting the Functions of Juries in Cases of Libel.*

États-Unis d'Amérique

Constitution américaine du 17 septembre 1787.

United States Bill of Rights.

United States Supreme Court, *Schenck v. United States,* nºs. 437, 438, March 3, 1919, 249 U.S. 47.

United States Supreme Court, *Near v. Minnesota,* nº. 91, June 1, 1931, 283 U.S. 697.

United States Supreme Court, *Griswold v. Connecticut,* nº 496, June 7, 1965, 381 U.S. 479.

United States Supreme Court, *Berger v. New York* (nº. 615), June 12, 1967, 388 U.S. 41.

United States Supreme Court, *Katz v. United States*, nº 35, December 18, 1967, 389 U.S. 347.

United States Supreme Court, *New York Times Co. v. United States*, nº 1873, June 30, 1971, 403 U.S. 713,1.

United States Supreme Court, *Roe v. Wade,* Nº 70-18, January 22, 1973, 410 U.S. 113.

Privacy Act of 1974, 5 U.S.C.

United States Supreme Court, *R.A.V. v. City of St. Paul,* Nº 90-7675, June 22, 1992*,* 505 U.S. 377 (1992).

United States Supreme Court, *Reno c/ACLU,* nº 96-511, June 26,1997*,* 521 U.S. 844.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, *Public law* 107-56-Oct. 26, 2001.

Annexes

Annexe 1 Fac-similé de l'adhésion de la France à la CESDH

DECLARATIONS ET RESERVES

L'instrument de ratification de la France comporte les déclarations et réserves suivantes :

« Articles 5 et 6.

Le Gouvernement de la République, conformément à l'article 64 de la Convention, émet une réserve concernant les articles 5 et 6 de cette Convention en ce sens que ces articles ne sauraient faire obstacle à l'application des dispositions de l'article 27 de la loi n° 72-662 du 13 juillet 1972 portant statut général des militaires, relatives au régime disciplinaire dans les armées, ainsi qu'à celles de l'article 375 du Code de justice militaire.

Article 10.

Le Gouvernement de la République déclare qu'il interprète les dispositions de l'article 10 comme étant compatibles avec le régime institué en France par la loi n° 72-553 du 10 juillet 1972 portant statut de la Radiodiffusion-télévision française.

Article 15 (paragraphe 1).

Le Gouvernement de la République, conformément à l'article 64 de la Convention, émet une réserve concernant le paragraphe 1 de l'article 15 en ce sens, d'une part, que les circonstances énumérées par l'article 16 de la Constitution pour sa mise en œuvre, par l'article 1er de la loi du 3 avril 1878 et par la loi du 9 août 1849 pour la déclaration de l'état de siège, par l'article 1er de la loi n° 55-385 du 3 avril 1955 pour la déclaration de l'état d'urgence, et qui permettent la mise en application des dispositions de ces textes, doivent être comprises comme correspondant à l'objet de l'article 15 de la Convention et, d'autre part, que pour l'interprétation et l'application de l'article 16 de la Constitution de la République, les termes « dans la stricte mesure où la situation l'exige » ne sauraient limiter le pouvoir du Président de la République de prendre « les mesures exigées par les circonstances ».

Le Gouvernement de la République déclare en outre que la présente Convention s'appliquera à l'ensemble du territoire de la République, compte tenu, en ce qui concerne les territoires d'Outre-Mer, des nécessités locales auxquelles l'article 63 fait référence.

Le Gouvernement de la République souligne enfin qu'il n'est pas partie au Protocole n° 2 en date du 6 mai 1963 attribuant à la Cour européenne des Droits de l'homme la compétence de donner des avis consultatifs et qu'en conséquence, pour autant que les articles 1 à 4 de ce Protocole seraient considérés comme intégrés à la Convention, il n'en accepte pas les dispositions. »

Fac-similé du Journal officiel du 4 mai 1974

Annexe 2 Exemples de géolocalisation

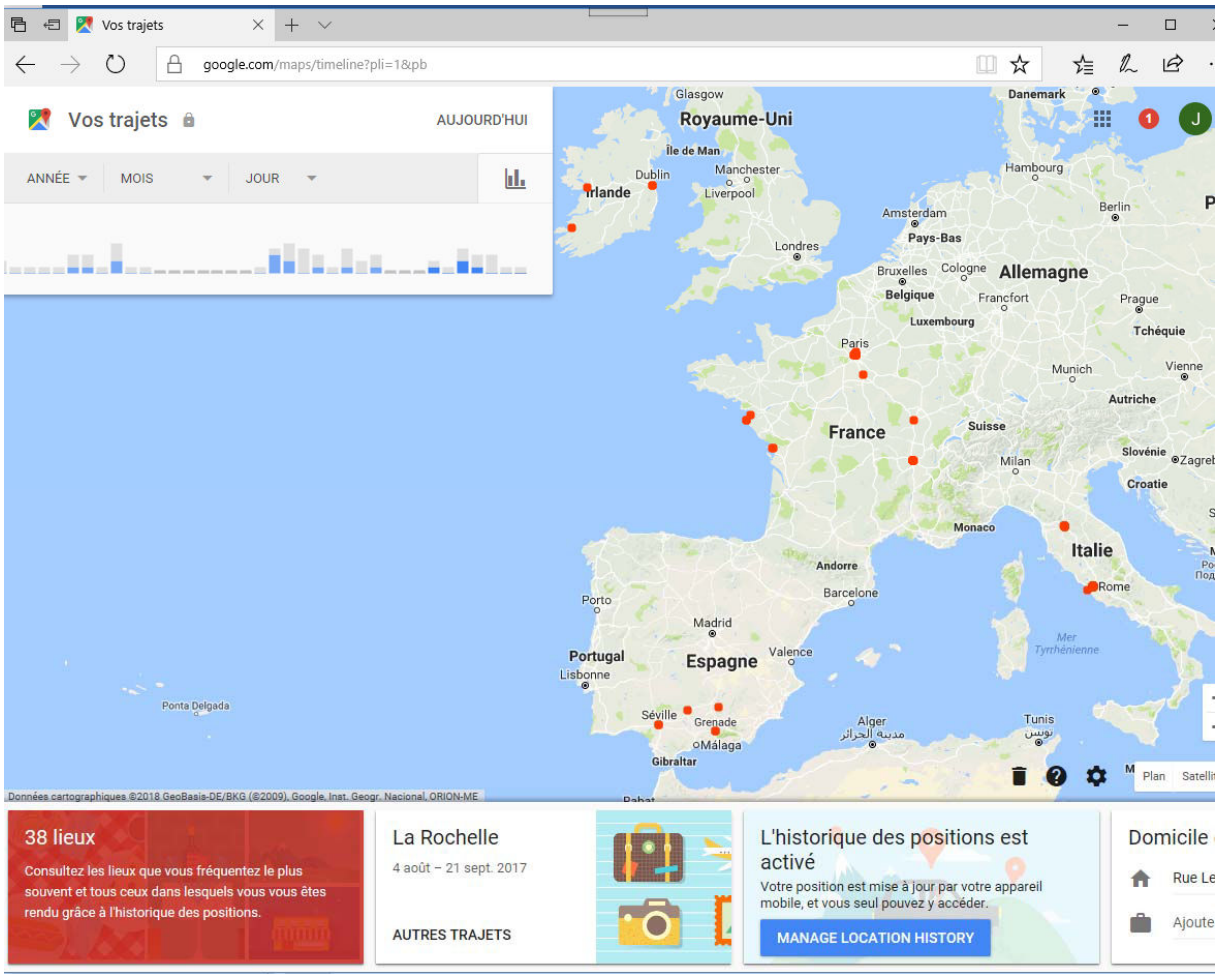


Figure 6 Capture d'écran montrant les déplacements de l'auteur

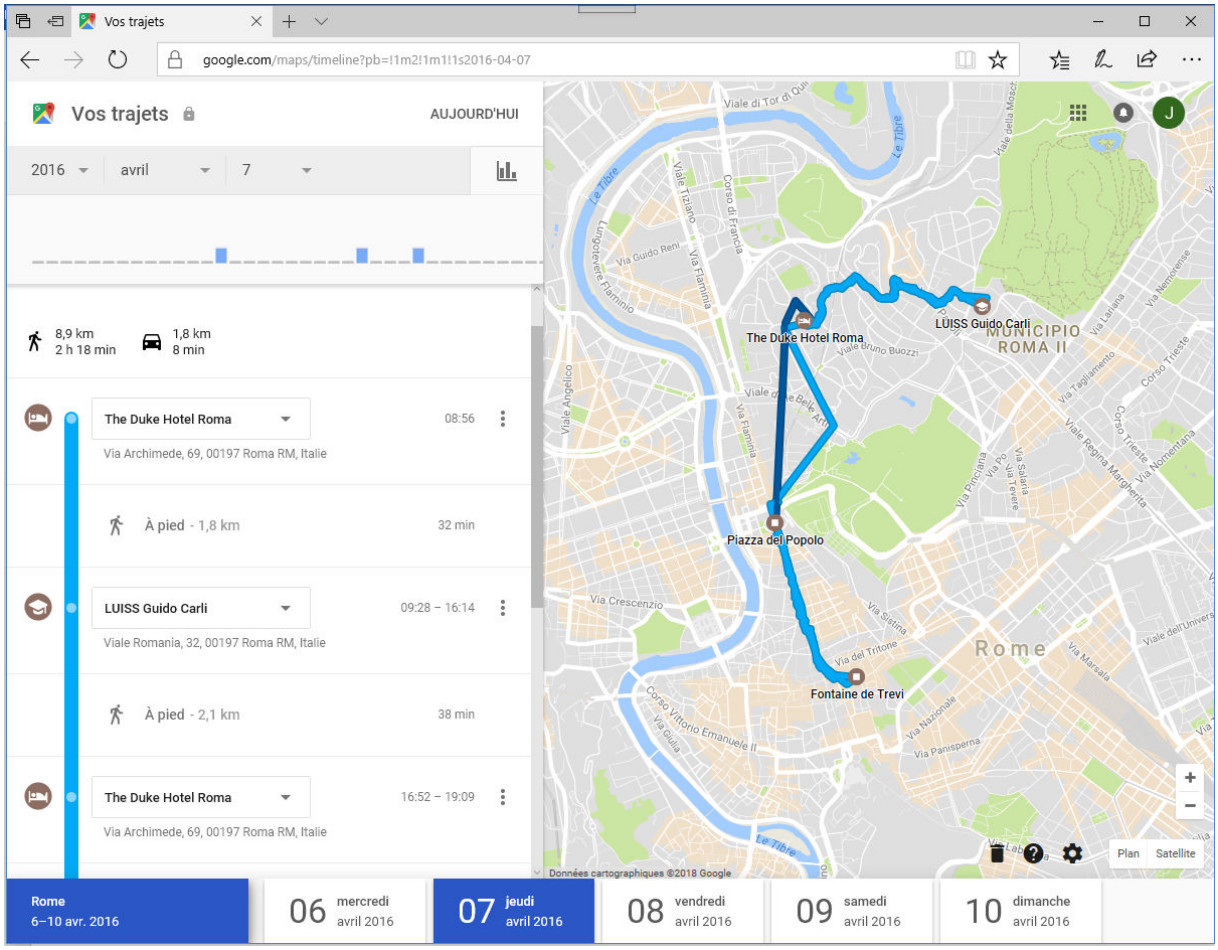
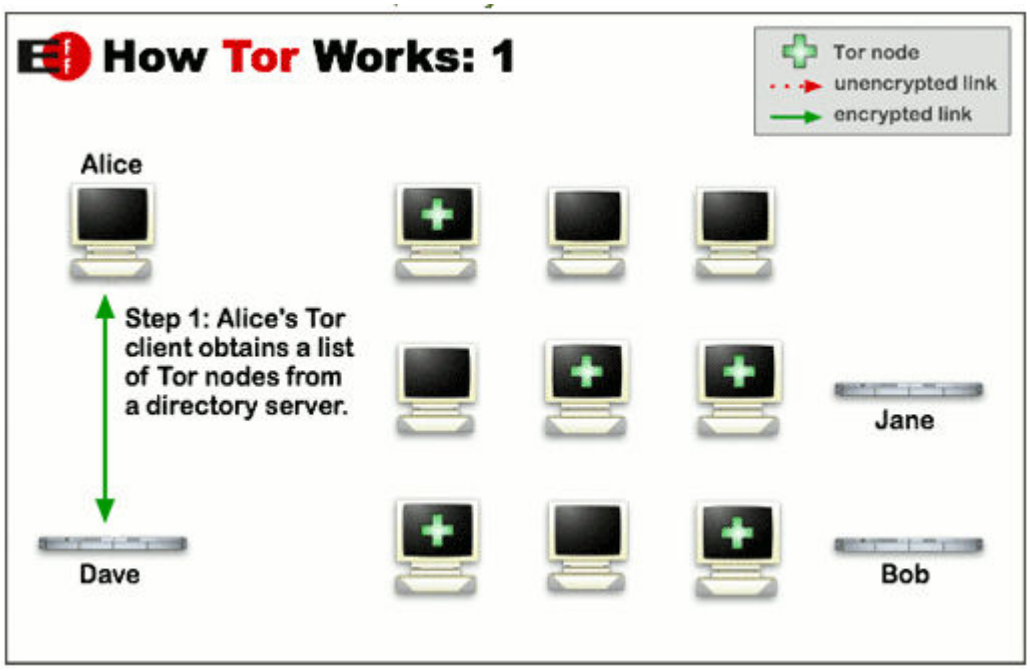
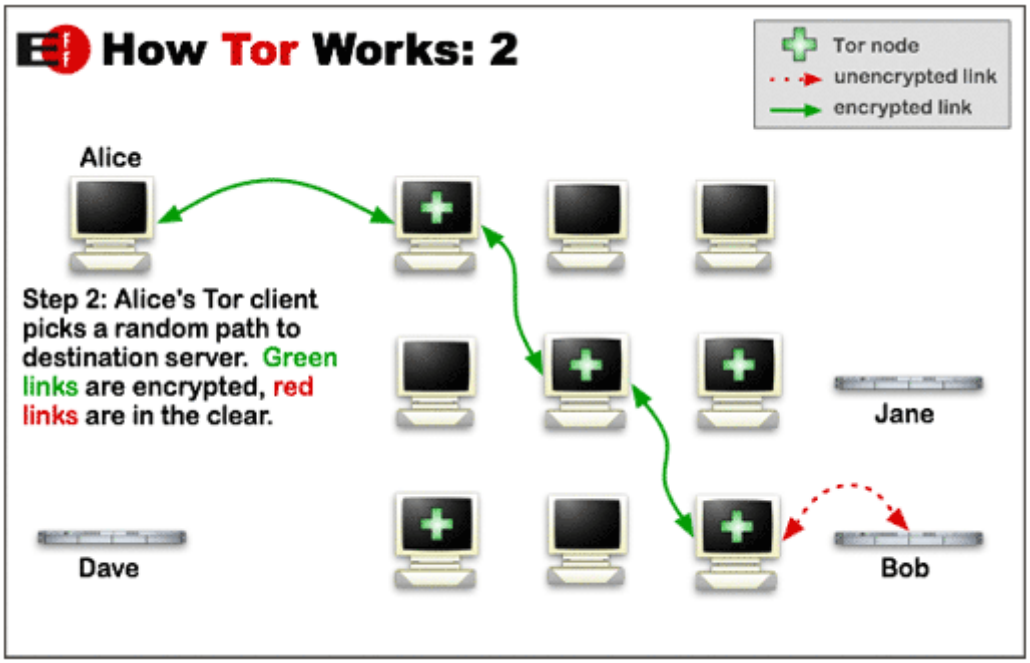
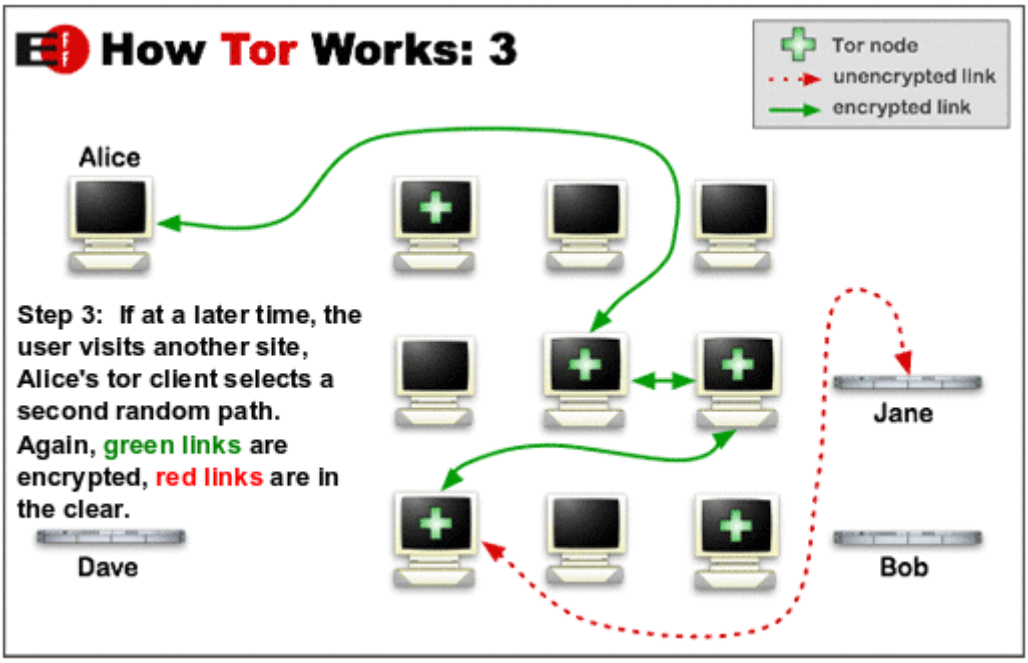


Figure 7 Détail d'un trajet particulier

Annexe 3 Principes de fonctionnement de TOR






How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Annexe 4 Liste des cartes de crédit par AMAZON

Index

Table des matières détaillée