



HAL
open science

La surveillance diffuse : entre Droit et Norme

Clemence Codron

► **To cite this version:**

Clemence Codron. La surveillance diffuse : entre Droit et Norme. Droit. Université de Lille, 2018. Français. NNT : 2018LILUD002 . tel-01905217

HAL Id: tel-01905217

<https://theses.hal.science/tel-01905217>

Submitted on 25 Oct 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Communauté
d'Universités et d'Établissements
Lille Nord de France



ComUE Lille Nord de France

Thèse délivrée par

L'Université de Lille, Droit et Santé

N° attribué par la bibliothèque

||_|_|_|_|_|_|_|_|

THÈSE

Pour obtenir le grade de Docteur en Droit Public

Présentée et soutenue publiquement par

Clémence CODRON

Le 15 juin 2018

La surveillance diffuse: entre Droit et Norme

JURY

Directeur de thèse :

Monsieur Jean-Jacques Lavenue - Professeur émérite Université de Lille

Membres du jury:

Madame Maria Belen Andreu Martinez (Rapporteur) - Professeur à l'Université de Murcie

Monsieur William Gilles (Rapporteur) - Maître de conférences (HDR) à l'Université Paris 1

Monsieur Yves Poirmeur (Président) - Professeur à l'Université Versailles Saint Quentin

Monsieur Michel Hastings (Suffragant) - Professeur à l'IEP de Lille

Monsieur Stéphane Bracq (Suffragant) - Maître de conférences (HDR) à l'IEP de Lille

Remerciements

La disponibilité et les conseils de mon directeur de thèse, Monsieur le Professeur Jean-Jacques Lavenue, ont été des plus précieux pour la réalisation de ce travail. Nos échanges, nos accords et nos désaccords, votre attention et votre bienveillance m'ont permis de mener une réflexion originale. J'espère que vous trouverez dans ces quelques lignes l'expression de la gratitude et du respect que je vous porte.

Ma reconnaissance va également à l'endroit des membres du jury qui ont bien voulu accorder de leur temps à l'appréciation de ce travail.

Aux rencontres stimulantes que les années de doctorat m'ont permises de faire. Je pense notamment à Maud Michaloux, Sébastien Brangoulo, Arnaud Galimberti, Stéphane Ménoret, Nicolas Museux, Nicolas Scuto, Simona Maggio, Christian Bouhier, Clémence Scottez, ainsi que Gaylord Hamerel, Sophie Ranchy et Françoise Menu.

A M. Stéphane Bracq, pour son regard empreint de saine curiosité quant à ce sujet de recherche, et pour sa bienveillance.

A mes amis; Fabienne, Luc et Julie, Adrien, Diederick, César; je réitère mon affection et ma gratitude.

A mon conjoint, pour son goût pour ce sujet et son aide au quotidien. Sa patience, son écoute, sa compréhension et sa tendresse ont rendu possible la conclusion de ce travail.

A mon frère et sa compagne pour leur écoute, leur réconfort, leur patience. Merci à vous deux, je vous dois beaucoup. A ma filleule.

A mes parents, pour leur soutien indéfectible, leur écoute, leur confiance, leur bienveillance. Votre présence au quotidien, votre compréhension, votre énergie et vos encouragements ont permis l'aboutissement de ce travail.

Sommaire

Introduction générale	21
Partie 1 : Une intégration de la surveillance diffuse modérée sous l'empire de la loi de 1978 et de la directive de 1995	61
Titre 1: L'institutionnalisation progressive de la surveillance diffuse: naissance et développement d'un phénomène de société	63
<i>Chapitre 1: La diffusion de la surveillance dans la société numérique</i>	<i>65</i>
<i>Chapitre 2: Des acteurs multiples au service de l'institutionnalisation de la surveillance diffuse: l'élaboration d'une culture de la surveillance</i>	<i>133</i>
Titre 2: Une intégration délicate de la surveillance diffuse dans la protection offerte au titre du droit des données personnelles sous l'empire de la loi de 1978 et de la directive de 1995.	191
<i>Chapitre 1: Un déficit de conscience des enjeux de la surveillance diffuse sous l'empire de la loi de 1978 et de la directive de 1995:</i>	<i>193</i>
<i>Chapitre 2: Un déficit d'effectivité globale des premières législations informatiques et libertés face à la surveillance diffuse</i>	<i>235</i>
Partie 2: L'intégration parfaite de la surveillance diffuse dans l'évolution des notions juridiques de vie privée et de données personnelles	287
Titre 1: La désinstitution du droit des données personnelles et de la vie privée sous l'empire des nouveaux instruments européens	291
<i>Chapitre 1: L'organisation d'une gouvernance des données personnelles au titre du règlement général sur la protection des données personnelles</i>	<i>293</i>
<i>Chapitre 2: L'organisation de la marchandisation de la vie privée par les nouveaux instruments européens: vers une désinstitution du droit au respect de la vie privée et de la protection des données personnelles au profit de la surveillance diffuse</i>	<i>333</i>
Titre 2: La désinstitution du Droit au profit de la nouvelle norme admise: la surveillance diffuse	377
<i>Chapitre 1: La surveillance diffuse: entre désinstitution de la fonction du droit et mutation du Droit par la nouvelle norme admise</i>	<i>379</i>
<i>Chapitre 2: La mutation du contrôle social par la surveillance diffuse et ses effets sur le Droit</i>	<i>423</i>
Index des principaux auteurs	545
Index des notions principales	551
Tables des matières	561

Glossaire

Accountability:

Globalement: obligation globale de rendre compte. Le principe d'accountability est clairement affirmé par le règlement général sur la protection des données dans le cadre de ses considérants et de ses articles. Le chapitre 4 du règlement énonce ainsi dès son premier article que « *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 oeuvre 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* ». Appliqué aux données personnelles, le principe d'accountability dans le cadre du règlement, vise à « *la mise en oeuvre de politiques appropriées en matière de protection des données par le responsable du traitement* », ou à la possibilité de faire application de codes de conduites et de mécanismes de certifications.

App-generation:

Expression fondée par les Professeurs Gardner et Davis (Université d'Harvard) afin de désigner la génération actuelle des adolescents, principalement caractérisée par son usage technologique, plutôt que par des événements politiques ou économiques majeurs. Cette métaphore permet de comprendre cette génération comme étant à la recherche permanente de l'application, numérique ou non, qui lui permet d'accomplir une tâche le plus rapidement et le plus efficacement possible

Backdoor:

Programme informatique introduit généralement, mais pas uniquement, par un pirate informatique, pour pouvoir ouvrir un accès dérobé à un système informatique ou à un programme informatique, afin d'en prendre le contrôle.

« Big Brother »:

Personnage de fiction issu du roman de Georges Orwell, 1984. Pour Orwell, ce nom désigne un dictateur totalitaire, omniprésent et omnipotent. Cette expression est aujourd'hui utilisée de manière récurrente pour qualifier toutes les institutions ou pratiques portant atteintes aux libertés fondamentales, et spécialement à la vie privée des individus.

Courant Porteur en Ligne (CPL):

Mode d'accès à internet très haut débit par le réseau électrique d'une habitation ou d'un bureau. La prise électrique est ici utilisée pour effectuer une connexion au réseau.

Digital Natives (« natifs du numérique »):

Ce concept, élaboré aux Etats-Unis en 2001 par Marc Prensky, désignait à l'origine les individus nés après 1980 avec le langage numérique, les ordinateurs, les jeux vidéos et Internet. Ce langage numérique était alors comparé à la langue maternelle de ces individus. Aujourd'hui, cette notion désigne l'intégration culturelle du numérique par les individus, tant par leur disposition à utiliser les technologies que par leur sensibilité à acquérir de l'information numérique et des technologies.

Dot-Com:

Désigne les entreprises qui tire profit de leurs usages d'Internet grâce à un site web appartenant au domaine de premier niveau : .com

Données relatives au trafic:

Selon l'article L. 32-18° du Code des Postes et des Communications électroniques: « *on entend par données relatives au trafic toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* ».

Dystopie:

Selon la définition du Dictionnaire Larousse: nom féminin - (d'après Utopie), Société imaginaire régie par un pouvoir totalitaire ou une idéologie néfaste, telle que la conçoit un auteur donné.

Feedback:

Au delà du simple retour sur expérience, ce concept signifie, dans un système cybernétique, la rétroaction de l'information

Free Flow of Information:

Doctrine américaine du libre flux de l'information, de la libre circulation de l'information élaborée au milieu du 20^{ème} siècle. Cette doctrine a inspiré la communauté internationale en matière de communication, et plus tard de technologie de l'information. Elle revêt plusieurs dimensions. Elle est à la fois représentative de la réaffirmation de la liberté d'expression au sens de la Déclaration

Universelle des Droits de l'Homme. A ce titre, elle représente un enjeu stratégique d'influence et d'intérêt dans un contexte où les relations internationales étaient marquées par la Guerre Froide. Elle est enfin la traduction d'un enjeu économique permettant aux entreprises américaines de s'internationaliser. La doctrine du free flow of information doit d'abord et avant tout permettre le libre échange (de l'information).

Google Street View:

Service de navigation virtuelle lancé le 25 mai 2007 afin de compléter Google Maps et Google Earth. Il permet de visualiser un panorama à 360° d'un lieu situé sur une voie urbaine ou rurale, sur laquelle aura préalablement circulé un véhicule chargé d'enregistrer les prises de vues.

Hard power:

Le Hard power est un concept qui rassemble les ressources traditionnelles de la puissance d'Etat: souveraineté, capacités militaires et économiques. En relations internationales, ce concept désigne la capacité du corps politique à imposer sa volonté à d'autres corps politiques à l'aide de moyens militaires et économiques.

Hardware:

Ensemble des éléments matériels d'un système informatique. Partie physique des appareils, des dispositifs de télécommunications, de stockage et des périphériques qui constituent un système informatique

Hub informationnel:

En matière informatique, sorte de concentrateur. A l'aide de la diplomatie, de la souveraineté et de la reconnaissance d'enjeu économique et stratégique globaux, ce concept désigne la capacité d'un Etat à se positionner comme un acteur central de la communication, des technologies de l'information, et du numérique.

In-sujet:

Pour André Tosel, traduction contemporaine du concept de Hannah Arendt concernant la superfluité humaine. André Tosel écrit ainsi que le nouveau sujet juridique « *est induit à désirer sans fin, à n'avoir d'identité subjective que dans le conformisme de ce désir général qui se satisfait par la possession de l'argent, cet équivalent général de toutes les marchandises. Le sujet ne vit que de*

cette subjectivité anonyme, insubjective, que produit dans l'hétéronomie la production-consommation capitaliste ». Et d'ajouter que l'individu contemporain « *se voit assigner de se définir par son désir de droit de consommer le droit et de renoncer librement à toute autre demande, de renoncer à toute insurrection proprement politique* ».

(Cf. TOSEL André, « Libres réflexions à partir de Hannah Arendt - Superfluité humaine et conformisme de l'insujet », in. CALLOZ-TSCHOPP Marie-Claire (dir.), *Lire Hannah Arendt aujourd'hui - Pouvoir, guerre, pensée, jugement, politique*, Actes du colloque international de Lausanne 11 - 12 mai 2007, Université de Lausanne, Institut d'Etudes Politiques Internationales, L'Harmattan, 2008, Paris, pp. 81 - 96)

Interconnexion:

Mise en relation de divers entités matérielles ou logicielles pour qu'elles travaillent ensemble (Larousse). Selon l'article L. 32 - 9° du Code des Postes et des communications électroniques, « *on entend par interconnexion la liaison physique et logique des réseaux ouverts au public exploités par le même opérateur ou un opérateur différent, afin de permettre aux utilisateurs d'un opérateur de communiquer avec les utilisateurs du même opérateur ou d'un autre, ou bien d'accéder aux services fournis par un autre opérateur. Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. L'interconnexion constitue un type particulier d'accès mis en œuvre entre opérateurs de réseaux ouverts au public* ».

Interopérabilité:

Capacité de matériels, de logiciels ou de protocoles différents à fonctionner ensemble et à partager de l'information (Larousse)

Knowledge-Based Society:

La société de la connaissance désigne l'une des caractéristiques des sociétés contemporaines où l'accès à la connaissance et à la culture est devenu primordial dans la dynamique internationale économique et politique mouvante. L'accès à la connaissance et la culture a, au-delà de sa dimension libertaire, une réelle ambition économique, car elle permet de stimuler l'innovation, l'esprit d'entreprise et le dynamisme de l'économie de la société.

Lean Startup:

Mode particulier de management d'entreprise où l'entrepreneur mène un certain nombre d'investigations auprès de ses potentiels futurs clients afin de recenser leurs points de vue par

rapport à un ou plusieurs produits donnés. Principalement fondée sur des procédés itératifs de validations des nouveaux produits et services, la lean startup met l'utilisateur au centre de ses préoccupations par l'obtention de retour d'expérience de la part de ces derniers.

Liveware:

Composante humaine d'un système informatique (utilisateurs, salariés de la direction des systèmes d'information).

Log:

Désigne un fichier, ou tout autre dispositif, permettant de stocker des événements attachés à un processus. Ces événements sont horodatés et constituent un véritable journal de bord d'un système donné (serveur, connexion, erreur).

« One Best Way »:

Dans la division du travail, et spécialement dans le Taylorisme, le « one best way » désigne l'établissement de la meilleure façon possible de produire. Dans le cadre des technologies de l'information et de la communication, le « one best way » permet selon Jacques Ellul de traduire « *la préoccupation de l'immense majorité des hommes de notre temps, de rechercher en toutes choses la méthode la plus efficace. (...). Il s'agit en réalité de trouver le moyen supérieur dans l'absolu, c'est-à-dire en se fondant sur le calcul* » et la rationalité dans la plupart des cas où la technique s'insère.

(Cf. ELLUL Jacques, *La Technique ou l'Enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990, p. 18 - 19)

Panoptique:

Se dit d'un bâtiment (pénitencier, hospitalier, ...) dont, d'un pont d'observation interne, on peut embrasser du regard tout l'intérieur (Larousse). Théorisée par Jérémy Bentham dans le cadre de sa réforme des systèmes carcéraux, l'idée principale du projet panoptique est celle de « voir sans être vu »: les prisonniers ne pourront à aucun moment voir les gardiens. Omniscience de la visibilité des prisonniers par le gardien et invisibilité du gardien donneront à la surveillance une nouvelle forme d'efficacité. Repris par Michel Foucault, le panoptique désigne également le modèle de la société disciplinaire. Fondée sur le contrôle social et la surveillance, la société disciplinaire permet d'imposer à la société toute entière une conduite à suivre.

Pop-Up:

Fenêtre qui surgit et s'affiche de manière intrusive et non sollicitée devant la page web consultée par l'utilisateur d'un navigateur.

Privacy by design:

La notion de protection de la vie privée dès la conception a été développée à l'initiative de la préposée à la protection des données de l'Etat d'Ontario au Canada, Ann Cavoukian. Elle signifie que chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation le plus haut niveau possible de protection des données. Selon l'article 25 du règlement général sur la protection des données personnelles: « 1. (...) le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. 2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, 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 ».

Privacy Shield:

Le privacy shield, autrement appelé bouclier de protection des données, est un mécanisme d'auto-certification pour les entreprises établies aux Etats-Unis en matière de protection des données personnelles. Ce dispositif a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux Etats-Unis.

Safe Harbor:

Ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne. Les Safe Harbor ont été invalidés par une décision de la Cour de Justice de l'Union européenne en date du 6 octobre 2015, et remplacés par le Privacy Shield.

Smart City:

Selon la CNIL, « *la ville intelligente est un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citoyens en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. Le périmètre couvrant ce nouveau mode de gestion des villes inclut notamment : infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms) ; transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied, etc.) ; les e-services et e-administrations* ».

Cf.: <https://www.cnil.fr/fr/definition/smart-city>

Smart power:

En relation internationale, exercice d'un pouvoir intelligent fondée sur la combinaison entre les stratégies de soft power et de hard power. Développée par Joseph Nye, cette notion doit être analysée à la fois comme une entreprise de communication menée par l'Etat et relayée par les entreprises, mais également comme la combinaison de tous les moyens d'actions possibles. L'exercice de ce smart power se matérialise principalement par l'élaboration de partenariats avec le secteur privé dans le but d'accroître les bénéfices liés au commerce international, principalement aidé par les technologies et l'innovation

Soft power:

Le soft power s'organise autour de la capacité d'un Etat à faire adhérer et participer pleinement les individus et d'autres Etats à une ambition politique et étatique plutôt que de les contraindre par la force. L'exercice d'un soft power par l'Etat correspond alors à une sorte de force de persuasion douce. Mis au service de la surveillance diffuse, ce soft power a permis de légitimer la priorité donnée par l'Etat aux développements technologiques. Et c'est dans ce cadre que la convergence

des intérêts du secteur public et du secteur privé a pu se développer

Software:

Partie logicielle d'un système informatique. Ensemble des moyens d'utilisation, programmes, procédures, documentation d'un système informatique.

Spam:

Courrier électronique non sollicité envoyé à un très grand nombre d'adresses électroniques, sans l'accord préalable des propriétaires des adresses.

Storytelling:

Sorte de mise en récit, le storytelling est une méthode de communication fondée sur une structure narrative d'un discours qui s'apparente à celle des contes, des récits. Le but de cette méthode est de gagner l'adhésion d'un public du fait même de la présentation narrative d'un objet, d'une personne, d'un concept.

Think Different:

Communication publicitaire créée pour la société Apple en 1997. L'utilisation de ce slogan du « penser différent » a été utilisée par la société jusqu'en 2002.

Think Tank:

Le concept de think tank désigne une entité de droit privé, à but non lucratif, destinée à produire des études et des réflexions concernant des questions liées aux domaines politique, économique, technologique et social. Supposée indépendante de la puissance publique et économique, cette institution regroupe des experts ou des professionnels de ces questions.

Welfare State

Autrement appelé Etat-Providence, cette expression désigne une conception de l'Etat, et du rôle de l'Etat. Dans cette conception, l'Etat étend son champ d'intervention et de régulation dans les domaines économiques et sociaux en vue d'assurer des prestations aux citoyens (redistribution des richesses, prise en charge des risques sociaux).

Well-Being

Anglicisme équivalent à l'expression française de bien-être. Employé dans le cadre de ce travail pour évoquer la doctrine du « Well-being of Nations », le Bien-être des Nations. Depuis le début des années 2000, cette notion est à rapprocher du rôle du capital humain et social. Si la définition du bien-être fait intervenir les concepts de prospérité, de santé et de bonheur; le concept de Bien-être des Nations fait intervenir, quant à lui, des indicateurs numériques afin de mesurer le bien-être général dans l'ensemble d'une société. Ces indicateurs sont économique et financiers, mais également sociaux (taille des ménages, temps destinés aux loisirs, qualité de l'environnement).

Tables des sigles et abréviations

ACLU: American Civil Liberties Union (Union américaine pour les libertés civiles)

ADN: Acide DésoxyriboNucléique

AFNOR: Association Française de NORmalisation

ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information

APLIUT: Association des Professeurs de Langues des Instituts Universitaires de Technologie

ARPANET: Advanced Research Projects Agency Network

ASIP: Agence des Systèmes d'Information Partagés

ASMP: Académie des Sciences Morales et Politiques

BDSG: BundesDatenSchutzGesetz (loi fédérale allemande sur la protection des données personnelles)

BGBI: BundesGesetzBlatt (journal officiel fédéral allemand)

BRUSA: British United States of America Communications Intelligence Agreement

CAC 40: Cotation Assistée en Continu

CADA: Commission d'Accès aux Documents Administratifs

CATO Institute: Institut Caton

CEDH: Cour Européenne des Droits de l'Homme

CERT: Computer Emergency Response Team

CJCE: Cour de Justice des Communautés Européennes

CJUE: Cour de Justice de l'Union Européenne

CNIL: Commission Nationale de l'Informatique et des Libertés

CNRS: Centre National de la Recherche Scientifique

CPL: Courant Porteur en Ligne

CSIRT: Computer Security Incident Response Team

DARPA: Defense Advanced Research Projects Agency

DADVSI: Droits d'Auteur et Droits Voisins dans la Société de l'Information

DICID: Revue Droit International, Commerce, Innovation et Développement

DMP: Dossier Médical Partagé

DSI: Directeur des Systèmes d'Information

EDVIGE: Exploitation Documentaire et Valorisation de l'Information Générale

EIVP: Etude d'Impacts sur la Vie Privée

GAFA: Google, Apple, Facebook, Amazon

GAFAM: Google, Apple, Facebook, Amazon, Microsoft

GPS: Global Positioning System

HTTP: HyperText Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

Ibid.: Ibidem

IP: Internet Protocol

ISO: International Organization for Standardization

JOCE: Journal Officiel des Communautés Européennes

JORF: Journal Officiel de la République Française

JOUE: Journal Officiel de l'Union Européenne

LDH: Ligue des Droits de l'Homme

LPM: Loi de Programmation Militaire

LOPSSI 2: Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure 2

MAC: Media Access Control

NIS: Network and Information Security

NOMIC: Nouvel Ordre Mondial de l'Information et de la Communication

NSA: National Security Agency

OCDE: Organisation de Coopération et de Développement Economique

OGM: Organisme Génétiquement Modifié

OIV: Opérateur d'Importance Vitale

OMC: Organisation Mondiale du Commerce

ONU: Organisation des Nations Unies

Op. cit.: Opere Citato

PET'S: Privacy-Enhancing Technologies

PIA: Privacy Impact Assessment

PIB: Produit Intérieur Brut

PNB: Produit National Brut

PNR: Passenger Name Record

PRISM: Planning tool for Ressource Integration, Synchronization and Management

PSSI: Politique de Sécurité des Systèmes d'Information

RATP: Régie Autonome des Transports Parisiens

RGPD: Règlement Général sur la Protection des Données

RSC: Revue de Science Criminelle

RFID: Radio Frequency IDentification

SACEM: Société des Auteurs, Compositeurs et Editeurs de Musique

SAFARI: Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus

SCPP: Société Civile des Producteurs Phonographiques

SDF: Sans Domicile Fixe

SFR: Société Française du Radiotéléphone

SFS: Svensk FörfattningsSamling (Recueil des lois du Royaume de Suède)

SNCF: Société Nationale des Chemins de fer Français

SSI: Sécurité des Systèmes d'Information

SSID: Service Set IDentifier

STE: Série des Traités Européens

STOA: Scientifical and Technological Options Assessment

TES: Titres Electroniques Sécurisés

TIC: Technologie de l'Information et de la Communication

UE: Union Européenne

UIT: Union Internationale des Télécommunications

UKUSA: United Kingdom – United States Communications Intelligence Agreement

UNESCO: United Nations Educational, Scientific and Cultural Organization / Organisation des Nations Unies pour l'Education, la Science et la Culture

WI-FI: Wireless Fidelity

Introduction générale

*« Il est au cœur du monde occidental un conflit sans espoir,
sous quelque forme que nous le découvrons.
Celui de l'homme et de ce qu'il a créé! ».*

*« Les utopies apparaissent comme bien plus réalisables qu'on ne le croyait autrefois.
Et nous nous trouvons devant une question bien autrement angoissante :
comment éviter leur réalisation définitive ?...
Les utopies sont réalisables. La vie marche vers les utopies.
Et peut-être un siècle nouveau commence-t-il,
un siècle où les intellectuels et la classe cultivée rêveront aux moyens d'éviter les utopies
et de retourner à une société non utopique, moins parfaite et plus libre² ».*

*« La technologie a envahi l'enceinte sacrée de la vie privée,
et l'exposition injustifiée de cette dernière a mis en péril notre sécurité,
notre dignité, et nos valeurs les plus fondamentales.
La législation doit se montrer à la hauteur de la situation et protéger nos droits³ » .*

1 MALRAUX André, La tentation de l'occident, in. Oeuvres complètes, tome 1, 1989, p. 109

2 BERDIAEFF Nicolas, cité par Aldous Huxley en épigraphe du roman *Le meilleur des mondes*. HUXLEY Aldous, *Le meilleur des mondes*, Cooltour, 25 avril 2015.

3 POKEMPNER Dinah, *Le droit dont l'heure est (re) venue - Le respect de la vie privée à l'ère de la surveillance*, in. Human Rights Watch Rapport annuel 2014, En ligne: https://www.hrw.org/sites/default/files/related_material/privacy_fr.pdf (dernière consultation: 5 mars 2018). Dinah PoKempner est directrice des affaires juridiques pour Human Rights Watch. Et de poursuivre son introduction par les mots suivants: « *Cela vous rappelle quelque chose ? Ainsi s'exprimaient Samuel Warren et Louis Brandeis dans leur article de la Harvard Law Review de 1890, proclamant « Le droit à la vie privée ». Nous sommes aujourd'hui à un nouveau tournant de ce genre. Les progrès technologiques que Warren et Brandeis considéraient comme des menaces – la photographie et l'avènement de la presse à grand tirage – nous semblent aujourd'hui assez désuets. Mais l'impact d'une exposition non souhaitée sur notre sécurité émotionnelle, psychologique et même physique est un enjeu tout aussi brûlant à l'ère numérique dans laquelle nous vivons ».* WARREN Samuel, BRANDEIS Louis, *The Right to Privacy*, Harvard Law Review, vol. 4, no. 5, 15 décembre 1890, pp. 193 - 220, En ligne: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> (dernière consultation: 5 mars 2018)

1. Ces trois citations donnent le ton et la mesure de la difficulté que représente un travail juridique sur le concept de surveillance. A l'évocation de ce terme, plusieurs référentiels se mettent en place en fonction des grilles d'analyses, des interprétations positives ou négatives posées sur ce concept, mais aussi en fonction de la focale choisie. Le philosophe évoquera ainsi sa référence à l'utopie⁴, à la dystopie⁵, encore appelée contre-utopie⁶. Le scientifique, comme le technicien, évoqueront les incroyables avancées du progrès, de la recherche et du développement, de la science appliquée, et les bénéfiques qu'ils apportent à notre société⁷. Le sociologue opérera par renvoi⁸ aux études de Bentham⁹, Deleuze¹⁰ et Foucault, et évoquera le panoptique, la société disciplinaire¹¹ et la

⁴ On notera en guise d'illustrations les références utopiques de Voltaire, dans les propos que Pangloss martèle à travers l'ensemble de cet ouvrage: « *tout est pour le mieux dans le meilleur des mondes possibles* », ou, plus spécialement, dans les chapitres 17 et 18 de *Candide*, lorsqu'il découvre, accompagné de Cacambo, son valet, l'Eldorado. in VOLTAIRE, *Candide ou l'optimisme*, Edition Libre, Bibebook, 2013, p. 105 à 125. Ou, plus récemment, voir: WERBER Bernard, *Le papillon des étoiles*, Albin Michel, 2006

⁵ A titre d'exemple, on pourra citer de manière non exhaustive: ZAMIATINE Evgueni, *Nous autres*, traduit du russe par B. Cauvet-Duhamel, Gallimard, Collection L'imaginaire, Paris, 1979, HUXLEY Aldous, *Le meilleur des mondes*, Cooltour, 25 avril 2015, BARJAVEL René, *Ravage*, Folio, Gallimard, 1972, ORWELL George, *1984*, Traduit de l'anglais par Amélie Audiberti, Folio, Gallimard, 2003, ou encore plus récemment, DAMASIO Alain, *La Zone du Dehors*, Folio - Science-Fiction n°350, Gallimard, 2014

⁶ Le Meilleur des mondes de Aldous Huxley, est un exemple de contre-utopie.

⁷ Pour une lecture critique de cette position, voir OPPENHEIMER Robert, *La science et le bon sens*, Traduit de l'anglais par Albert Colnat, Collection Idées, Gallimard, 1955

⁸ Pour preuve, voir: GALIC Masa, TIMAN Tjerk, KOOPS Bert-Jaap, *Bentham, Deleuze and beyond: an overview of Surveillance Theories from the Panopticon to Participation*, Mai 2016, Tilburg Institute for Law, Technology and Society, ou encore: SIMON Bart, *The return of Panopticism: Supervision, Subjection and the New Surveillance*, *Surveillance & Society*, 3 (1): 1-20, En ligne: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3317/3279> (dernière consultation: 5 mars 2018)

⁹ BENTHAM Jérémie, *Le panoptique, précédé de l'Oeil du pouvoir, entretien avec Michel Foucault*, Editions Belfond, 1977

¹⁰ DELEUZE Gilles, *Foucault*, Les Editions de Minuit, Paris, 2004; et du même auteur, *Post-scriptum sur les sociétés de contrôle*, Publié dans *Pourparlers*, Les Editions de Minuits, Paris, 1990, p. 240 - 247, En ligne: <https://infokiosques.net/IMG/pdf/Deleu.pdf> (dernière consultation: 5 mars 2018)

¹¹ FOUCAULT Michel, *Surveiller et punir - Naissance de la prison*, Editions Gallimard, (numérique), 2013; mais également FOUCAULT Michel, *Sécurité, Territoire, Population - Cours au Collège de France, 1977 - 1978*, Gallimard / Seuil, 2004. Selon l'auteur, la société disciplinaire est une société dans laquelle le commandement social s'organise en un système précis, combinant force et mesure, constitué par un réseau de dispositifs et d'appareils diffus qui produisent et régulent les comportements, les habitudes et les pratiques productives. Foucault écrit ainsi que « *toute l'activité de l'individu discipliné doit être scandée et soutenue par des injonctions dont l'efficace repose sur la brièveté et la clarté, l'ordre n'a pas à être expliqué, ni même formulé; il faut et il suffit qu'il déclenche le comportement voulu* » (in. *Surveiller et punir - Naissance de la prison*, Op. Cit., p. 291). Cette société permet d'assurer l'obéissance à la règle, à son mécanisme d'inclusion ou d'exclusion sociale, et est mise en oeuvre par des institutions disciplinaires (prison, usine, asile, hôpital, école, ...) qui structurent le terrain social et forme les comportements sociaux.

société de contrôle¹². Le romancier sera tenté d'évoquer, à l'image de Malraux, le conflit existant entre l'individu et ce qu'il a largement participé à créer¹³. Les Google, Amazon, Facebook, Apple et Microsoft (GAFAM) promettent non pas de la surveillance, mais une nouvelle forme de vie en société fondée sur l'accès à la culture et à la connaissance, le rapprochement des individus, la possibilité d'acheter et de vendre en ligne, par la mise en oeuvre de technologies de pointe permettant la synchronisation de l'ensemble des appareils connectés à Internet. Le politique verra en elle un moyen et une fin permettant une vie en société sécurisée dans un monde devenu dangereux¹⁴. L'individu, quant à lui, sera placé dans une double position. D'une part, il prétendra contrôler son usage des technologies, et donc maîtriser les avancées technologiques. Mais, il laissera des traces, des informations le concernant, il permettra la saisie de données personnelles, et laissera la possibilité à de nombreux acteurs d'entrer dans sa vie privée sous prétexte de facilités offertes par l'ère numérique. Tout en se contentant du sentiment de sécurité et de confort que procurent ces technologies. D'autre part, dans trop peu de cas, il s'offusquera de l'amoindrissement progressif de sa sphère privée, et d'une possible altération de sa liberté¹⁵. Pas une seule semaine ne se passe sans qu'un journaliste, ou une chaîne d'information en continu, n'évoquent un nouveau scandale de surveillance générale, massive, une fuite de données, un nouvel espionnage organisé par une sombre agence gouvernementale, ou par une entreprise. La surveillance est partout, sur toutes les lèvres, sous toutes les plumes.

¹² La société de contrôle prend place avec la fin des institutions disciplinaires traditionnelles. Ce concept désigne une société dans laquelle le contrôle des personnes s'opère en continu. Pour Hardt et Negri, nous devons comprendre la société de contrôle par contraste avec la société disciplinaire, dans laquelle les mécanismes de contrôle, de maîtrise se font « toujours plus « démocratique », toujours plus immanent du champ social, diffusés dans le cerveau et le corps des citoyens. Les comportements d'intégration et d'exclusion sociale proprement dits sont donc de plus en plus intériorisés au sein des sujets eux-mêmes. Le pouvoir est maintenant exercé par des machines qui organisent directement le cerveau (dans les systèmes de communication, les réseaux d'information, ...) et les corps (dans les systèmes de protection sociale, les activités surveillées, ...) vers un état d'autonomie du sens de la vie et le désir de créativité. La société de contrôle pourrait ainsi se caractériser par une intensification et une généralisation des dispositifs normatifs de l'interdisciplinarité qui orientent vers l'extérieur nos pratiques communes et quotidiennes, mais au contraire de la discipline, cette continuité s'étend à la structuration des institutions sociales à travers des réseaux flexibles et fluctuants ». in. HARDT Michel, NEGRI Antonio, *Empire*, Harvard University Press, Cambridge, Massachusetts - London, England, 2000, p. 23.

¹³ On pense ici notamment à Martin Heidegger et à ses développements concernant l'arrondissement de l'homme par la technique, in. HEIDEGGER Martin, *Essais et conférences -La question de la technique* ; traduction par André Préau, Éditions Gallimard, Collection Tel, 1988. On pense également au disciple de Martin Heidegger: Peter Sloterdijk et ses développements concernant « la domestication de l'être », in. SLOTERDIJK Peter, *Règles pour le parc humain, suivi de La domestication de l'Être*, Editions Fayard, Milles et une nuits, 2010.

¹⁴ Voir par exemple la Loi n° 2015 – 912 du 24 juillet 2015 relative au renseignement, JORF n°0171 du 26 juillet 2015 page 12735, texte n°2, En ligne: <http://www.legifrance.gouv.fr/eli/loi/2015/7/24/PRMX1504410L/jo/texte> (dernière consultation: 5 mars 2018)

¹⁵ On citera l'exemple récent des polémiques liés au Décret n° 2016 - 1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, JORF n° 0254 du 30 octobre 2016, texte n°18, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345&dateTexte=&categorieLien=id> (dernière consultation: 5 mars 2018)

2. Pourtant, la surveillance n'a aucune définition faisant l'objet d'un consensus réel - ni d'un point de vue international, européen ou national; ni d'un point de vue légal. Elle existe, et se développe encore et toujours plus dans notre société devenue globale. Elle interpelle le juriste, qui l'envisagera à travers un ensemble de référentiels - allant des libertés fondamentales, en passant par le rôle de l'Etat, et les questionnements liés à la force de la loi, à l'Etat de droit - les développements de la surveillance en matière d'enquête judiciaire¹⁶, d'application des peines¹⁷, ou encore, en matière de crime organisé. Il en nommera même les conséquences: amoindrissement et même perte progressive de certaines libertés individuelles du fait de l'organisation de « *la sûreté dans un monde dangereux*¹⁸ », qui, selon Mireille Delmas-Marty, ont été préparées grâce à la « *déshumanisation du droit pénal et, plus largement, d'une radicalisation du contrôle social*¹⁹ ». Ces premiers développements attirent l'attention sur deux idées souvent préconçues sur la question de la surveillance. D'une part, il semblerait que cette dernière soit l'apanage de l'Etat, des pouvoirs publics, d'un gouvernement qui pourraient, au travers du droit pénal, surveiller en permanence les moindres faits et gestes de ses citoyens. D'autre part, il apparaîtrait que les événements du 11 septembre 2001 soient devenus les révélateurs de la dangerosité du monde, ainsi que de l'apogée de la surveillance. Ces deux idées doivent nécessairement être questionnées.

3. Bien que l'Etat, et plus largement les autorités publiques, soient les acteurs privilégiés de la surveillance, il ne faut pas réduire la situation de surveillance contemporaine à ce seul acteur. L'Etat a traditionnellement la charge d'une forme de surveillance des comportements des individus au regard du droit, c'est-à-dire dans le cadre global de sa mission de garant de l'ordre public, de la sécurité nationale, de l'intégrité territoriale, de la sûreté publique, de la défense de l'ordre et de la prévention du crime. Réduire la surveillance contemporaine à ce seul acteur serait erroné. La surveillance contemporaine recouvre une multiplicité d'acteurs, les dernières évocations de ce

¹⁶ Systèmes d'écoutes téléphoniques, des contrôles judiciaires

¹⁷ Placement sous surveillance électronique mobile (bracelet électronique notamment), rétention de sûreté.

¹⁸ Nous empruntons ces termes à Mireille Delmas-Marty qui, à travers (l'avant propos de) son ouvrage consacré aux *libertés et à la sûreté dans un monde dangereux*, déclare que « *le point de départ de ce livre est la loi française relative à la rétention de sûreté, adoptée le 25 février 2008, qui permet de maintenir un condamné en détention, après exécution de sa peine, pour une durée d'un an, renouvelable indéfiniment, sur le seul critère de sa dangerosité* ». in. DELMAS-MARTY Mireille, *Libertés et sûreté dans un monde dangereux*, Editions du Seuil, Collection La couleur des idées, 2010, p.7

¹⁹ Mireille Delmas-Marty poursuit l'analyse précitée en notant: « *préparée depuis quelques années par une succession de lois sur la récidive, la rupture est ainsi consacrée dans la relation entre culpabilité, responsabilité et sanction, au risque d'une déshumanisation du droit pénal et, plus largement, d'une radicalisation du contrôle social* ». Ibid.

thème dans la presse ont tendance à largement prouver ce phénomène. Ces dix dernières années des affaires comme Wikileaks²⁰, Prism²¹, Silk Road²², Vault 7 Dark Matter²³ dénoncent le rôle des autorités publiques dans une forme de surveillance massive. Elles démontrent également que le secteur privé participe de manière consciente ou non à cette surveillance. Pour ce qui est de l'effet spécifique du 11 septembre 2001, il serait dangereux de céder à l'amalgame. Ainsi que le rappelle avec acuité Mireille Delmas-Marty, « *les dangers ont existé de tout temps et en tous lieux, mais les attentats du 11 septembre 2001 en ont peut-être changé la perception, et ont en tout cas modifié les réactions*²⁴ ».

4. En réalité ces deux idées préconçues relèvent d'un imaginaire collectif et de l'affiliation de la surveillance à la science-fiction. Le développement de l'informatique, des technologies de l'information et de la communication s'est accompagné d'une double représentation. D'une part, à la sortie de la Seconde Guerre mondiale, les technologies, et spécialement l'informatique, vont être considérées par les pouvoirs publics comme facteur positif d'une reconstruction sociale²⁵. A partir des années 70, avec l'émergence des créations en France et à l'international de fichiers informatisés dits administratifs²⁶, on passe progressivement à une représentation négative des nouvelles technologies. L'Etat, ou plutôt la possibilité d'un Etat totalitaire informatisé, est progressivement mis en cause, à travers l'image d'un Big Brother. Ces craintes se cristallisent alors autour de la notion de vie privée, puis progressivement autour de la notion de données personnelles. Elles sont parfaitement résumées par le Professeur Jean Frayssinet, lorsque ce dernier commentait, en 1989, le préambule de la loi n° 78 - 17 du 6 janvier 1978. Il écrivait alors: « *l'informatique doit être au service de chaque citoyen* » pose l'objectif (et le principe) fondamental ; la formule condense toute

²⁰ Pour une vision générale du sujet: NORMAND Grégory, *Wikileaks: cinq choses à savoir sur la surveillance de la CIA*, La Tribune, 8 mars 2017, En ligne: <http://www.latribune.fr/economie/international/wikileaks-cinq-choses-a-savoir-sur-la-surveillance-de-la-cia-656436.html> (dernière consultation: 5 mars 2018)

²¹ Pour une vision générale du sujet: SZADKOWSKI Michaël, LELOUP Damien, *Prism, Snowden, surveillance: 7 questions pour tout comprendre*, Le Monde, 2 juillet 2013, En ligne: http://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html (dernière consultation: 5 mars 2018)

²² Pour une vision globale du sujet: MASIMBERT Mailys, *Quand les ados menacent l'anonymat du e-commerce de la drogue*, Slate, 7 septembre 2013, En ligne: <http://www.slate.fr/monde/77682/ados-anonymat-web-drogue-silk-road> (dernière consultation: 5 mars 2018)

²³ Pour une analyse générale: Wikileaks, Darkmatter, 23 Mars 2017, En ligne: <https://wikileaks.org/vault7/darkmatter/> (dernière consultation: 5 mars 2018)

²⁴ Ibid. p. 12.

²⁵ Sur ce point voir infra. Première partie, titre 1, chapitre 1.

²⁶ On pense ici au fichier Safari, et aux fichiers de recensement informatisé qui éclosent progressivement dans le monde. Sur ce point voir infra. Première partie, titre 1, chapitre 1.

la problématique : de l'homme ou de l'ordinateur, lequel doit être subordonné à l'autre ?²⁷ »

5. Après avoir évoqués la possibilité de différents référentiels concernant le concept de surveillance, il apparaît nécessaire de prendre le temps de souligner en quoi il est intéressant de voir dans le concept de surveillance, un phénomène de société que l'on nommera: la surveillance diffuse, et d'énoncer ce que l'on entend par là. Ce dernier devra nécessairement être mis en confrontation avec les concepts juridiques de vie privée, de respect de la vie privée, et de droit des données personnelles. On constatera alors que les représentations qui prévalaient dans les années 1970 n'ont pas forcément évolué aujourd'hui. Toutefois, les possibilités techniques, les nouvelles technologies de l'information et de la communication permettent un accroissement indéniable des traitements, de la collecte de données²⁸. Ces éléments permettant alors à la surveillance de se diffuser dans nos sociétés par l'émission de toujours plus de nouvelles technologies dans la vie quotidienne des individus, et par la réception de toujours plus de flux de données par des acteurs divers, personnes physiques ou morales, publiques ou privées. A tel point que la notion même de donnée personnelle ne semble plus suffisante pour envisager la surveillance. De nos jours, la surveillance puise sa diffusion dans la puissance des moyens technologiques. Ces derniers permettent de stocker, d'appairer, de récupérer, de traiter, de commercialiser et de faire circuler ces données. De la donnée technique à la donnée personnelle, d'un chiffre, d'un nombre, d'un identifiant, d'un code, de l'ADN, des photographies, vidéos, tout aujourd'hui paraît être mis en collection dans la puissance de traitement des technologies de l'information et de la communication. Sonder ces notions d'informations et de communication semblent être au coeur de l'explication de la surveillance diffuse, et ce, bien plus, que la simple donnée personnelle.

6. Il apparaît nécessaire de justifier le recours au concept de surveillance diffuse, et d'en délimiter les contours définitionnels. Questionner ces notions juridiques et a-juridique permettra de mettre en lumière les tenants et les aboutissants de la problématique de la vie privée²⁹. Il est nécessaire, au vu du phénomène de surveillance diffuse que le Droit réagisse ! D'autant plus, lorsqu'on constate que de nombreux auteurs de doctrine comparent la situation actuelle à un

²⁷ FRAYSSINET Jean, « *L'utilité et les fonctions d'une formulation d'objectifs : l'exemple de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés* », Revue de la Recherche Juridique, n°4, 1989, p.904

²⁸ Nous développons ces éléments dans les sections suivantes de ce chapitre introductif.

²⁹ En ce sens, voir: MANACH Jean-Marc, *La vie privée, un problème de vieux cons?*, Limoges, Editions Fyp, collection Présence, 2010

« anthropocène numérique³⁰ », ou encore « à un moment décisif de notre histoire³¹ ». Ces mots traduisent le fait que la vie privée est aujourd'hui devenue l'enjeu du siècle de la surveillance diffuse (section 1). D'une fiction imaginaire, utopique ou dystopique, la surveillance diffuse est devenue une « *fiction instituante*³² » et pleinement instituée dans la société (section 2).

Section 1: La vie privée ou l'enjeu du siècle de la surveillance diffuse

7. Lorsque Jacques Ellul a écrit son oeuvre sur la Technique, il déclarait dès son premier chapitre: « *aucun fait social, humain, spirituel, n'a autant d'importance que le fait technique dans le monde moderne. Aucun domaine, pourtant, n'est plus mal connu*³³ ». Ce chapitre était précédé d'un avertissement où Ellul se défendait d'un jugement de valeur « *éthique ou esthétique sur la technique*³⁴ ». Et d'ajouter que, « *dans la mesure où l'on ne reste pas purement photographique, et dans la mesure où l'on est homme, une certaine prise de position peut transparaitre. mais elle n'est pas si éminente qu'elle empêche une objectivité plus profonde. La marque de celle-ci se trouvera sans doute en ce que les technolâtres jugeront cet ouvrage comme pessimiste, et les technophobes comme optimiste à l'égard de la technique*³⁵ ». Dire que nous vivons aujourd'hui au siècle de la surveillance diffuse réactive cet avertissement (paragraphe 1), et sous tend l'analyse des expressions de « moment historique décisif » et « d'anthropocène numérique » défendues notamment par Charbonneau et Ellul, Mireille Delmas Marty, Eric Sadin, ou encore Bernard Stiegler (paragraphe 2).

³⁰ Voir en ce sens: CHARBONNEAU Bernard, *Le système et le chaos – où va notre société ?*, préface de Daniel Cérézuelle, Éditions Sang de la terre – Medial, Collection *La pensée écologique*, 2012, 1973; CHARBONNEAU Bernard, *Pan se meurt*, « explication au lecteur », 1943; devenu *Le Jardin de Babylone*, Éditions de l'Encyclopédie des nuisances, 2002; STIEGLER Bernard, *La société automatique - 1. L'avenir du travail*, Éditions Fayard, 2015; Voir également l'usage de la notion d'anthropocène par Mireille Delmas-Marty. Cette dernière écrit que l'anthropocène doit être vu comme une « *force tellurique des humains* » et un « *appel aux forces imaginantes du droit* ». Elle précise ainsi que bien que « *le concept d'anthropocène n'est encore officiellement défini et homologué par l'Union Internationale des Sciences Géologiques, (...) il évoque déjà l'entrée dans une nouvelle phase de l'histoire géologique où l'espèce humaine devient une force capable d'interagir avec les autres forces géophysiques et de menacer la sûreté de la planète. (...) c'est donc tout l'assemblage des sociétés humaines que ce constat invite à recomposer: non seulement les processus économiques et politiques de gouvernement, mais encore les processus juridiques de construction et d'harmonisation des valeurs et de responsabilisation des acteurs* ». in. DELMAS- MARTY Mireille, *Aux quatre vents du monde - Petit guide de navigation sur l'océan de la mondialisation*, Éditions du Seuil, Version numérique réalisée par Nord Compo, Septembre 2016, p. 15 - 16

³¹ En ce sens, voir: SADIN Eric, *Surveillance globale - enquête sur les nouvelles formes de contrôle*, Flammarion, Climats, 2009, spécialement p. 8 à 13.

³² Nous empruntons ce concept à Lucien SFEZ. In. SFEZ Lucien, *technique et Idéologie - Un enjeu de pouvoir*, Éditions du Seuil, La couleur des idées, Paris, 2002, p. 221 - 307.

³³ ELLUL Jacques, *La Technique ou l'Enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990, p 1.

³⁴ Ibid. p. V

³⁵ Ibid. p. V - VI

Paragraphe 1: De l'utilité d'une démarche objective quant au concept de surveillance diffuse

8. La technologie, le progrès ont toujours eu leurs partisans et leurs détracteurs. Il en est de même pour la surveillance. Les technophiles évoqueront la sécurité que procure la surveillance; les technophobes déclareront vivre dans une société de plus en plus marquée par le totalitarisme feutré de la technologie. Ecrire que la vie privée est devenue l'enjeu du siècle de la surveillance diffuse n'est pas tout à fait la même chose, que de faire le constat de la diffusion de la surveillance et d'en lister ses effets. Ainsi que Jacques Ellul concluait son avertissement, il faut avec le plus d'honnêteté intellectuelle possible: « *essayer seulement de transcrire, de traduire au moyen d'une analyse globale une prise de conscience, à la fois concrète et fondamentale*³⁶ » du phénomène de surveillance diffuse dans son ensemble. Le premier objectif de cette thèse est donc d'observer et de traduire au moyen d'une analyse globale qui réunira le Droit, la sociologie et, parfois, la philosophie, ce qu'est la surveillance diffuse. Mais également, de transcrire la prise de conscience d'un changement de paradigme qui permet aujourd'hui de déduire d'un fait social, la surveillance, des éléments de transformation des droits et libertés, plus globalement du Droit.

9. Comprendre ce qu'est le phénomène de la surveillance diffuse et ses assises, c'est d'abord opérer un retour aux auteurs qui ont décrit le phénomène technique³⁷. Tout comme la technique, la surveillance est un phénomène auto-entretenu, de recherche permanente du moyen le plus efficace pour comprendre et régulariser notre Société. Elle se justifie par l'influence, la direction, la gestion et le contrôle qu'elle peut exercer sur cette dernière. Un processus de même ordre se retrouve dans la référence au concept de sécurité humaine, qui tend à envisager la construction d'une société la moins mauvaise possible. On comprend alors que l'ensemble de la société puisse se mettre à rêver de la construction d'une cité quasi utopique en acceptant de jouer un rôle dans l'organisation et la diffusion de la surveillance. Comprendre la surveillance, c'est aussi réactiver le double questionnement de Nietzsche – qui parle ? et d'où parle-t-il ? – pour l'appliquer aux concepts d'influence, de gestion, de direction et de contrôle de nos Sociétés, à la diffusion de l'idée d'organisation d'un « empire du moindre mal ». La surveillance n'est peut-être plus l'apanage d'un ensemble surveillant (États / entreprises), alors même que le rôle de ces acteurs a été déterminant

³⁶ Ibid. p. VI

³⁷ Partie 1, Titre 1, Chapitre 1

dans son avènement. Elle a été diffusée, par cet ensemble surveillant, dans nos sociétés modernes, dans chacune des activités de l'Homme ; jusqu'à la rendre acceptable.

10. L'emploi du terme « diffuse » dans le cadre de la surveillance représente la caractéristique essentielle de la surveillance contemporaine. Cette notion fait référence à la propagation des nouvelles technologies, mais également aux nouveaux usages permis grâce ou à cause de ces dernières. La diffusion suppose une émission et une réception. Appliqués à la surveillance, ces deux termes évoquent le fait pour cette dernière de s'être répandue par capillarité (émission) dans chacune de nos activités, en permettant la collecte (réception) de nombreuses informations, données personnelles, et détails sur nos vies. La diffusion progressive de la surveillance dans chacune des activités de l'homme a permis ensuite de le placer lui-même dans le champs d'observation de la surveillance; à faire en sorte qu'il « consente », ou du moins, qu'il accepte de donner toujours plus d'informations le concernant (émission facilitée) que le surveillant protéiforme va collecter et traiter (réception). S'attarder sur ces notions de diffusion, et cette inversion des rôles est importante en ce qu'elles caractérisent le passage d'une société panoptique, où la surveillance s'opère à sens unique, à la société catoptique, où la relation de surveillance est caractérisée par sa réciprocité. Le constat de la diffusion de la surveillance dans nos sociétés est alors alarmant. On observe, d'une part, que les notions classiques du Droit sont atteintes par ce phénomène : transformation des notions d'ordre public, de la démocratie, modification du rôle de l'État, « partenariats » toujours plus importants avec le secteur privé, nouveau langage et discours de légitimation de la surveillance. Développement d'éléments de langage et d'une forme de propagande, ayant pour conséquence un lissage des comportements de l'individu, une rationalisation de ses comportements, voire d'une déresponsabilisation de celui-ci. Evolution vers une domestication de l'être humain, passant du Loup décrit par Hobbes au chien de La Fontaine. Ces éléments représentent autant d'effets insidieux de la surveillance diffuse qu'il faut, dans le contexte de cette analyse, questionner.

11. D'autre part, l'évolution et la diffusion de la surveillance porte en elle plusieurs questionnements. Du fait de cette nouvelle docilité, l'homme est-il toujours libre ? Souvenons-nous ici, des mots de Benjamin Constant : *« le but des anciens était le partage du pouvoir social entre tous les citoyens d'une même patrie : c'était là ce qu'ils nommaient liberté. Le but des modernes est la sécurité dans les jouissances privées ; et ils nomment liberté les garanties accordées par les*

*institutions à ces jouissances*³⁸ » La vie privée, et par là, la protection des données personnelles, peuvent-elles être encore des concepts déterminants dans une société où la surveillance sera toujours légitimée, et ira toujours plus loin ? Quelles sont les conséquences réelles de cette diffusion toujours croissante de la surveillance ? On aurait pu penser que le passage de la société panoptique à la société catoptique, impliquant la réciprocité de la relation de surveillance aurait permis une meilleure organisation des relations sociales grâce une transparence de nos sociétés. Ce n'est pas le cas. Il apparaît au contraire, que la surveillance a permis l'organisation d'une forme de plasticité de nos sociétés aux dépens des individus.

12. S'interroger sur ces deux notions en évolution constante suppose que l'on se réfère à l'apparition de la surveillance diffuse et son développement dans notre société. Comprendre la surveillance diffuse en tant que phénomène d'auto-accroissement, et phénomène auto-entretenu permettra de saisir l'ampleur des effets qu'elle produit sur la notion de vie privée. Cette collision entre les concepts de protection de la vie privée et de surveillance diffuse nous conduira à un premier constat : les notions juridiques de données personnelles et de vie privée représentent l'enjeu essentiel de la surveillance diffuse. En ce qu'elle est recherche de toujours plus d'informations, de données (personnelles ou non) sur les individus, la surveillance s'immisce dans le vie privée. Par la réduction de l'individu à une trace, à une donnée statistique, la surveillance diffuse permet de rendre malléable, d'influencer, de diriger les individus. Il est alors nécessaire de prendre la mesure de cette plasticité sociale, et d'en comprendre ses effets.

Paragraphe 2: De l'utilité de la compréhension des concepts d'anthropocène numérique et de moments historique décisif : le siècle de la surveillance diffuse

13. Le siècle de la surveillance diffuse doit être analysé comme un moment historique décisif (B). La surveillance se fonde sur une philosophie nouvelle: la collecte de toujours plus d'informations et de données personnelles (ou non) sur les individus (A). L'enjeu du siècle de la surveillance réside dans la protection de la vie privée et des données personnelles.

³⁸ CONSTANT Benjamin, *De la liberté des anciens comparées à celle des modernes*, Discours prononcé à l'Athénée royal de Paris, 1819, En ligne: http://etienne.chouard.free.fr/Europe/Documents_conferences/Constant_Benjamin_Liberte_anciens_modernes_1819.pdf (dernière consultation: 5 mars 2018)

A. La philosophie de la surveillance diffuse

14. La collecte de toujours plus d'informations et de données sur les individus pourrait parfaitement illustrer la nouvelle philosophie de l'ère du numérique. Dans chaque secteur de notre vie, les technologies de l'information et de la communication se sont immiscées. De la protection de l'ordre public des États par l'installation de caméra de surveillance, à l'utilisation de plus en plus massive d'Internet, en passant par la domotique, les objets connectés, le cloud computing³⁹, et les Smart City, les technologies sont partout et sont présentées comme essentielles à notre vie.

15. Dans un univers d'interconnexion et de croisement des données, l'individu s'est, progressivement, mis à nu au bénéfice de différents acteurs dont les rôles dans l'acquisition des données semblent se rejoindre. Entre la sécurisation de la société et l'aspect économique des données personnelles, la vie privée, ou plutôt la conquête de la vie privée des individus devient un véritable enjeu dans lequel se sont lancées les multinationales du net, les États, et l'individu totalement conquis par les bienfaits des technologies. De nouvelles avancées technologiques et de nouveaux intérêts dans le mode de traitement des données sont apparues : Big Data⁴⁰, Data

³⁹ La définition de la notion de cloud computing a été permise grâce à une consultation publique lancée par la Commission Nationale de l'Informatique et des Libertés française ouverte entre octobre et décembre 2011. Selon les conclusions de cette consultation publique, la CNIL a déclaré que: « *l'expression « informatique en nuage » ou « Cloud computing » désigne le déport vers « le nuage Internet » de données et d'applications qui auparavant étaient situées sur les serveurs et ordinateurs des sociétés, des organisations ou des particuliers. Le modèle économique associé s'apparente à la location de ressources informatiques avec une facturation en fonction de la consommation »* (définition disponible sur le site de la CNIL à l'adresse suivante: <http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/> (dernière consultation: 5 mars 2018)). A la lecture de la synthèse des réponses à la consultation publique sur le Cloud et des recommandations pour les entreprises qui envisagent de souscrire à de tels services, l'analyse de la CNIL se précise. Il peut se définir comme un mécanisme de sous-traitance informatique, comportant en particulier : un service rendu au client sur base de ressources et d'équipements dont le client peut ignorer la localisation précise ; et un service fourni et facturé à la demande, capable de s'adapter immédiatement à l'évolution des besoins du client. Voir en ce sens: http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Synthese_des_reponses_a_la_consultation_publice_sur_le_Cloud_et_analyse_de_la_CNIL.pdf et concernant les recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing: http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf (dernière consultation de ces deux sites: 5 mars 2018)

⁴⁰ Le Big Data n'a pas encore réellement de définition. La CNIL française évoque un concept « encore flou et difficile à synthétiser » (in. Les cahiers IP, Innovation et prospective n°1, *Vie privée à l'Horizon 2020, Paroles d'expert*, CNIL, Direction des Études, de l'Innovation et de la Prospective, 2012, p.18). Il pourrait néanmoins être analysé comme « *un ensemble de technologies et de méthodes consistant à analyser, à des fins généralement prédictives, le flot de données produites par les entreprises, les organisations, et les individus, mais aussi les objets s'ils sont connectés, dans des volumes et à une vitesse sans précédent ; (...), et qui engloberait les mails, SMS, photos, vidéos, commentaires ou changements de statuts sur les réseaux sociaux, sessions de connexion, relevés d'étiquettes ou de capteurs électroniques, signaux de géolocalisation, ..., envoyés à foison chaque minute partout dans le monde »*. (définition envisagée par Delphine Cuny, auteur de l'article : *Big Data is Big Business vraiment*, in La tribune, le 3 avril 2013, En ligne: <http://www.latribune.fr/technos-medias/internet/20130403trib000757290/-big-data-is-big-business.-vraiment.html> (dernière consultation: 5 mars 2018)

Mining⁴¹, Open Data⁴² sont autant de nouvelles notions qui attestent de l'intérêt grandissant de différents protagonistes à l'égard de la Data, de la donnée, de l'information et des traces que les individus laissent parfois inconsciemment dans la société numérisée. La donnée personnelle et la vie privée deviennent un véritable enjeu de la civilisation de la surveillance diffuse, et sont comparées à un « *nouvel or noir*⁴³ » : la donnée personnelle, la vie privée, les données publiques, les données liées aux objets connectés sont devenues, comme le pétrole, une ressource naturelle susceptible de transformation, mais également et surtout susceptible d'exploitation. Cette ressource est même qualifiée de ferment d'une nouvelle révolution industrielle⁴⁴. Pour autant, cette métaphore est dangereuse. Les données ne sont pas produites par la nature. « *Elles s'articulent d'une manière ou d'une autre au réel, dont elles sont la trace, le symbole ou l'empreinte. Un réel qui peut parfois même être le fort intérieur de l'individu, inaliénable et incessible... Elles sont parfois extraites (comme le pétrole), mais le plus souvent produites et échangées librement par les individus. Ce ne sont pas des ressources rares. Non seulement elles ne s'usent pas quand on les utilise, mais elles prennent sans doute même de la valeur*⁴⁵ ». Dans une société où finalement tout peut faire l'objet d'une numérisation, et où la surveillance insidieuse des activités de l'individu se diffuse de plus en plus, l'exploitation des données devient pour les acteurs publics et privés, qui se cachent derrière cette métaphore, un véritable enjeu de pouvoir, économique, stratégique et politique.

16. L'article 8 de la Convention Européenne de Sauvegarde des Droits de l'Homme énonce que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa*

⁴¹ Le Data Mining peut se définir comme étant de l'exploration de données, du forage de données, de la prospection de données ou encore de l'extraction de connaissance à partir de données.

⁴² Données numériques ouvertes qui peuvent être d'origine publique ou privée, mise à la disposition du plus grand nombre selon une méthodologie spécifique. Le mouvement de l'Open Data est lié à des considérations philosophiques et idéologiques selon lequel l'intérêt public exige l'accès et/ou la publication de données gratuitement.

⁴³ De nombreux articles de presse ont récemment été publiés avec cette comparaison entre les données et le pétrole... Déjà dans son article précité, Delphine Cuny employait cette métaphore. On pourra également citer : un article de Perry Rotella, paru dans le magazine Forbes, le 4 février 2012 : *Is Data the new oil ?*, ou encore un dossier paru sur le site de l'inria intitulé *Data, le nouvel or noir ?*, avec un article de Stéphane Grumbach et Stéphane Frénot intitulé *les données, plus importantes que le pétrole*, En ligne: <http://www.inriality.fr/communication/data/donnees/data-le-nouvel-or/> (dernière consultation 5 mars 2018)

⁴⁴ Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 2 juillet 2014, *Vers une économie de la donnée prospère*, Com (2014), 442 final, p. 2. En ligne: <http://ec.europa.eu/transparency/regdoc/rep/1/2014/FR/1-2014-442-FR-F1-1.Pdf> (dernière consultation: 5 mars 2018). On pourra également citer l'avis du Comité économique et social européen *sur la communication au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions – Vers une économie de la donnée prospère*, Com (2014), 4442 final, 2915/C 242/11, paru au JOCE le 23 juillet 2015, C 242/61, En ligne: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C_.2015.242.01.0061.01.FRA&toc=OJ:C:2015:242:TOC (dernière consultation: 5 mars 2018)

⁴⁵ VERDIER Henri, *Non les données ne sont pas du pétrole*, blog en ligne, article disponible à l'adresse suivante : <http://www.henriverdier.com/2013/03/non-les-donnees-ne-sont-pas-du-petrole.html> (dernière consultation: 5 mars 2018)

correspondance ». La Convention est considérée par la Cour Européenne des Droits de l'Homme « *comme un instrument vivant à interpréter à la lumière des conditions de vie actuelle*⁴⁶ ». Cette interprétation dynamique et évolutive s'applique à l'article 8. De sorte que le champ de protection de cet article couvre, à l'heure actuelle, des domaines extrêmement variés, ce qui a contribué à en diluer la signification au point que le droit à la vie privée et familiale (par exemple) a pu être qualifiée de « *concept gigogne*⁴⁷ »: droit à l'intimité, droit à la vie privée sociale, protection des opinions, droit de vivre dans un environnement sain, droit à la santé, droit des membres des minorités à un mode de vie traditionnel, droit à connaître ses origines, liberté de vie sexuelle, droit au changement d'identité sexuelle, en passant par l'informatique et les données personnelle. Le droit au respect de la vie privée est ainsi un droit dynamique qui tente de prendre en compte l'évolution des conditions de vie actuelles, liée à l'informatisation de la société, et aux défis posés par la modernité technologique. Un exemple de cette dynamique apparaîtra dans la tentative de prise en compte des défis posés par la surveillance dans la proposition de règlement général de protection des données⁴⁸, puis dans sa version définitive⁴⁹.

17. La notion de vie privée est au cœur de la surveillance diffuse. Elle représente également l'enjeu de la nouvelle réglementation européenne. Il apparaît légitime de questionner le sens de la vie privée aujourd'hui, alors même que les intérêts des acteurs de la surveillance de la vie privée des individus convergent. Les instruments légaux de protection de la vie privée qui existent et ceux que l'on élabore sont-ils réellement efficaces face au phénomène de surveillance diffuse ? Ces questionnements, objets d'une interrogation plus vaste, pourraient se résumer ainsi : la surveillance diffuse, liée à l'utilisation de toujours plus de technologies et la collecte de toujours plus de données, est-elle réellement prise en compte dans l'évolution de la notion juridique de vie privée ? Et si tel est

⁴⁶ Voir par exemple l'arrêt de la Cour Européenne des droits de l'Homme n° 5856/72, 25 avril 1978, Tyrer contre Royaume-uni, par. 31, ou encore l'arrêt de la Cour Européenne des droits de l'Homme n° 15318/89, 23 mars 1995, Loizidou contre Turquie, par. 71

⁴⁷ SUDRE Frédéric, « Rapport introductif : la « construction » par le juge européen du droit au respect de la vie familiale », SUDRE Frédéric (dir.), *Le droit au respect de la vie familiale au sens de la Convention européenne des droits de l'Homme : actes du colloque des 22 et 23 mars 2002 organisé par l'Institut de droit européen des droits de l'Homme (UMR-CNRS 5415), Faculté de droit de l'Université Montpellier I*, Bruylant : Nemesis, Bruxelles, 2005, p. 27

⁴⁸ Proposition de règlement du Parlement européen et du Conseil du 25 janvier 2012 *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*, COM (2012) 11 final, Non publiée au JOCE. En ligne: <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012PC0011&from=FR> (dernière consultation: 5 mars 2018)

⁴⁹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, JOUE L 119 du 4 Mai 2016, P;1 - 88, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR> (dernière consultation: 5 mars 2018)

le cas, l'est-elle pour la préserver, la limiter ou la circonvenir ? La volonté première de cette thèse est de montrer que la surveillance qui évolue de manière autonome, ne peut se résumer à une simple prise en compte de telle ou telle mise en place technologique, de tel ou tel cadre juridique pour telle ou telle utilisation technologique dans tel ou tel lieu. La surveillance est bien un phénomène, et en tant que tel, elle devrait relever d'un cadre juridique clair. Cadre juridique qui devra, au vu des possibilités offertes par la surveillance technicisée (violation possible de la vie privée, captation de toujours plus de données...), prendre en compte les caractéristiques de la surveillance diffuse. Pour le dire autrement, le fondement de tout cadre juridique de la surveillance doit intégrer réellement les droits de l'homme, le droit au respect de la vie privée.

B. La surveillance diffuse:le nouvel ethos de la civilisation contemporaine

18. Pour la communauté internationale, il faudrait prendre acte aujourd'hui d'une modification sociale. Nous serions passés d'une société qui prônait l'accès à la connaissance et à l'information à une société de surveillance⁵⁰. Si cette expression reflète un changement de paradigme, il faut s'en détacher. L'expression « société de surveillance » ne permet pas de rendre compte de la réalité sociale, et de l'incorporation progressive de nouvelles technologies dans nos sociétés.

19. Dès l'introduction de son ouvrage consacré à la surveillance globale, Eric Sadin évoque un « *moment historique décisif*⁵¹ », puisque « *notre période est caractérisée par une accélération sans précédent de l'histoire de la technique, dont les effets sont particulièrement sensibles au prisme de quatre événements majeurs: 1/ extension ininterrompue du numérique; 2/ développement des réseaux de télécommunications; 3/ essor des nanotechnologies; 4/ recherches liées aux biotechnologies et aux manipulations génétiques*⁵² ». Plus loin, l'auteur poursuit son analyse en identifiant les éléments techniques et humains correspondants à ces événements, à ce « bouillon de culture »: « *généralisation de l'interconnexion, de la géolocalisation, de la vidéosurveillance; constitution de bases de données; développement de la biométrie, de logiciels d'analyses*

⁵⁰ A titre d'exemple: le 85ème congrès de la ligue des droits de l'Homme de 2009 est consacré à la « société de surveillance ». Ligue des Droits de l'Homme, Résolution adoptée lors du 85ème congrès de la LDH - Société de surveillance, vie privée et libertés, En ligne: http://www.ldh-france.org/IMG/pdf/Resolution_Societe_de_surveillance_-_85eme_congres_def_.pdf (dernière consultation: 5 mars 2018). Il est également nécessaire d'évoquer la 27 ème rapport d'activités de la CNIL de 2006 qui lance dès ses premières pages une « alerte à la société de surveillance »: CNIL, 27ème Rapport d'activités, 2006, La documentation française, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000422.pdf> (dernière consultation: 5 mars 2018)

⁵¹ SADIN Eric, Op. Cit. p. 7

⁵² Ibid.

*comportementales; miniaturisation des dispositifs; présence de plus en plus fréquente de capteurs et d'étiquettes radio (RFID); menace terroriste; agressivité marketing*⁵³ ». Ces éléments de lecture du phénomène de surveillance doivent être mis en lumière.

20. Selon les géologues, nous sommes en effet entrés dans une nouvelle ère: celle de l'Anthropocène. Cette ère géologique correspond à l'époque durant laquelle l'action humaine sur l'environnement a été telle que son impact a été à la fois significatif et dramatique pour l'écosystème. Bien qu'il y ait actuellement encore des débats au plan international sur la détermination du début de cette nouvelle ère, les géologues semblent arriver à un consensus selon lequel l'Anthropocène a commencé au milieu du 20^{ème} siècle, c'est-à-dire lors d'une mutation de la révolution industrielle. Dans cette nouvelle ère, *« l'homme est le facteur d'une dispersion sur tous les continents de certaines espèces animales et végétales, il en oriente l'évolution génétique, il est devenu le « top prédateur » sur terre et sur mer et les technologies qu'il a inventées marquent désormais la biosphère terrestre*⁵⁴ ». L'Anthropocène correspond donc à l'âge où le monde est saisi dans son intégralité par le Progrès, la science et la technique. En ce sens, il s'inscrit parfaitement dans ce que Mireille Delmas-Marty envisage sous ce concept⁵⁵: *« la force tellurique des humains »* devant nécessairement faire appel *« aux forces imaginantes du droit »*. En 1943, Bernard Charbonneau avait, quant à lui, qualifié ce phénomène de *« Grande Mue*⁵⁶ *»* de l'humanité. Il évoquait alors sa *« conscience d'un grand changement*⁵⁷ *»*. Rappelant que *« depuis deux siècles, le destin tourne. Ce n'est pas la civilisation seule qui change de base, c'est la société, c'est l'être humain dans ce qu'il a de plus intérieur. Présente à toutes les révolutions du passé qui pourtant étaient loin d'engager l'essentiel comme la crise actuelle, la conscience humaine défaille*

⁵³ Ibid.

⁵⁴ CHAUVEAU Loïc, *Les géologues du monde entier sont à la recherche du clou d'or*, Sciences et avenir, 1er Septembre 2016, En ligne: https://www.sciencesetavenir.fr/fondamental/geologie/les-geologues-du-monde-entier-sont-a-la-recherche-du-clou-d-or_104313 (dernière consultation: 5 mars 2018)

⁵⁵ DELMAS-MARTY Mireille, *Aux quatre vents du monde Op. Cit.*, p 15 et s.

⁵⁶ Charbonneau a écrit à plusieurs reprises à propos de ce qu'il qualifie de *« Grande mue »*. Nous retiendrons principalement cette citation: *« En 1930 la nature était immuable, en 1960 il est non moins sûr qu'il n'y en a pas ; mais dans les deux cas la plus grande aventure humaine de tous les temps ne met pas l'homme en cause, et il n'a pas à intervenir. La croissance technique et économique indéfinie est à la fois le fait et le dogme fondamental de notre temps, comme l'immutabilité d'un ordre à la fois naturel et divin fut celui de passé. La grande mue qui travaille les sociétés industrielles, et les autres à leur suite, est à la fois la réalité immédiate que nous pouvons appréhender dans le quotidien de notre vie et le moteur profond d'une Histoire que religions et idéologies s'époumonent à suivre ; chacun l'expérimente à chaque instant, et pourtant, par delà classes et frontières, elle met en jeu l'humanité »*, in. CHARBONNEAU Bernard, *Le système et le chaos – où va notre société ?*, préface de Daniel Cérézuelle, Éditions Sang de la terre – Medial, Collection *La pensée écologique*, 2012, 1973, p. 10.

⁵⁷ CHARBONNEAU Bernard, *Pan se meurt*, « explication au lecteur », 1943; devenu *Le Jardin de Babylone*, Editions de l'Encyclopédie des nuisances, 2002

aujourd'hui devant l'immensité de l'effort. Les glorifiant sous le nom de progrès, ou les subissant sous le nom de fatalité, l'homme s'abandonne aux avatars du devenir. Il fait pire. Il prétend appeler sans ce qui n'est que l'accident d'une évolution, et il travaille de toutes ses forces à accélérer la vitesse du mouvement qui l'entraîne. Non seulement il dénie à la pensée le droit d'orienter ce qu'il appelle l'action, mais il rejette avec horreur tout examen de celle-ci par la connaissance. Il n'est que la chose du courant brutal qui l'entraîne⁵⁸ ». Plus récemment, en 2015, Bernard Stiegler affirmait que « l'ère de l'Anthropocène, c'est l'ère du capitalisme industriel au sein duquel le calcul prévaut sur tout autre critère de décision et où, devenant algorithmique et machinique, il se concrétise et se matérialise comme automatisme logique, et constitue ainsi précisément l'avènement du nihilisme comme société computationnelle devenant automatique, téléguidée et télécommandée⁵⁹ ».

21. Par le recours à la notion d'Anthropocène, et par ces citations, on parvient à mieux comprendre le « moment historique décisif » dans lequel nous vivons actuellement. Pour reprendre les termes de Stiegler, l'ère dans laquelle nous vivons repose sur l'édification d'une société « automatique⁶⁰ », aidée par le capitalisme. Dans cette conception, la surveillance ne peut alors que devenir l'outil incontournable de « *l'automatisme logique algorithmique* », de l'ère du calcul, de la prévision et de la prévention. Plus globalement, la surveillance s'est construite par un ajout permanent de (sur) couches et d'usages technologiques différents engendrant la traçabilité des individus, et la normalisation de leurs comportements⁶¹, et permettant ainsi une forme d'anthropocène numérique⁶² où la surveillance diffuse devient incontournable. Pour autant, derrière

⁵⁸ Ibid.

⁵⁹ STIEGLER Bernard, *La société automatique - 1. L'avenir du travail*, Editions Fayard, 2015, p. 27

⁶⁰ Ibid.

⁶¹ La traçabilité des individus et la normalisation de leur comportement seront développées dans la suite de cette analyse.

⁶² Ce concept d'anthropocène numérique paraît prendre tout son sens à la lecture des déclarations de différents chercheurs et scientifiques de renom, tels que Stephen Hawking, Max Tegmark, Stuart Russell ou encore le prix Nobel de physique Frank Wilczek, qui dès 2014 interpellèrent la société civile dans le cadre d'un article consacré à l'intelligence artificielle. Ces chercheurs s'interrogeaient alors sur le fait de savoir si nous prenions suffisamment au sérieux l'intelligence artificielle. Hawking écrivait alors : « Réussir à créer une intelligence artificielle serait le plus grand événement dans l'histoire de l'homme. Mais ce pourrait aussi être le dernier. (...). L'impact à court terme de l'intelligence artificielle dépend de qui la contrôle. Et, à long terme, de savoir si elle peut être tout simplement contrôlée. (...). On peut imaginer que telle technologie déjoue les marchés financiers, dépasse les chercheurs, manipule nos dirigeants et développe des armes dont on ne pourra pas comprendre le fonctionnement ». In. HAWKING Stephen, RUSSELL Stuart, TEGMARK Max, WILCZEK Frank, *Stephen Hawking: Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough ?*, The Independent, 1er Mai 2014, En ligne: <http://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence-but-are-we-taking-9313474.html> (dernière consultation: 5 mars 2018)

le singulier du recours à l'expression de surveillance diffuse ou de surveillance contemporaine; sous l'image préconçue d'un Big Brother totalitaire, d'une surveillance tentaculaire exercée dans un but précis, par un acteur déterminé, se manifeste en réalité la pluralité de technologies, et leurs imbrications pour des finalités diverses. Les technologies mises en place dans les sociétés contemporaines ne correspondent pas toutes à une finalité de surveillance. Et, si tel est le cas, ces technologies sont souvent à l'origine, sans recoupement apparent.

Section 2: La surveillance diffuse: une « fiction instituante »?

22. Mettre de côté l'approche fictionnelle de la surveillance dans le cadre de ce travail revêt une importance capitale. Dans la mesure du possible, nous nous efforcerons de ne pas mentionner cet aspect dans le coeur de ce travail de recherches. Pour autant, il semble nécessaire dans le cadre de ce chapitre introductif de réactiver cette représentation. Ainsi que le rappelle François Ost, « *les mythes et les grands archétypes de la littérature universelle*⁶³ » peuvent nous renseigner sur « *l'origine et le destin du Droit*⁶⁴ ». Evoquant « *la donation de la loi du Sinai, l'invention de la justice chez Eschyle, la révolte de la conscience chez Antigone, la souveraineté de l'individu chez Robison Crusoé, les paradoxes de la liberté chez Faust, la déchéance de la loi chez Kafka*⁶⁵ », François Ost démontre qu' « *entre le « tout est possible du récit » et le « tu ne dois pas » de la loi, l'institution du social ne cesse de s'inventer des formes inédites*⁶⁶ ». Citant Platon, l'auteur affirme alors sa volonté de mettre en lumière « *la puissance proprement « constituante » de l'imaginaire littéraire, à la source des montages politiques et des constructions juridiques*⁶⁷ ».

23. Partant de ces mots et de l'imaginaire fictionnel qui a permis de diffuser la surveillance dans nos sociétés contemporaines, il est nécessaire, dans un premier temps, de mettre l'accent sur les mythes littéraires qui entourent ce concept, ce phénomène (paragraphe 1), ou pour reprendre les termes de François Ost de mettre en lumière leur « *puissance proprement constituante* ». Ces éléments permettront, dans un second temps, de mieux appréhender l'institutionnalisation de la surveillance diffuse dans nos sociétés et de tenter d'en donner une définition (paragraphe 2).

⁶³ OST François, *Raconter la loi - Aux sources de l'imaginaire juridique*, Odile Jacob, 2004, Quatrième de couverture.

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ Ibid.

⁶⁷ Ibid. p. 11.

Paragraphe 1: Des mythes littéraires qui entourent le phénomène de surveillance

24. L'un des points de départ de cette analyse concernant la nécessité de réactiver les mythes littéraires, les oeuvres de science-fiction qui entourent le concept de surveillance a été la lecture attentive d'un livre écrit par Neil Postman, intitulé « *se distraire à en mourir*⁶⁸ ». Alors qu'il réactive « *l'avertissement de Huxley*⁶⁹ » et le compare aux prophéties d'Orwell (A), l'auteur cherche à démontrer la difficulté de s'opposer à une tyrannie douce, à la lente édification d'un meilleur des mondes devenu réalité. La surveillance diffuse ne peut être comprise sans ce détour nécessaire. Ceux qui élèvent la voix actuellement pour démontrer ce problème sont catégorisés comme des paranoïaques, des fous, se situant dans le sillage des théoriciens du complot⁷⁰. Or, par bien des aspects, la surveillance diffuse met en cause les fondements du Droit, de la démocratie, d'une vie en société libre. De là, un autre mythe littéraire semble devoir être activé: celui de l'oeuvre de Kafka, et de sa démonstration permanente de la disparition progressive du Droit (B).

A. Les « prophéties » de Georges Orwell et de Aldous Huxley : « 1984 » Versus « Le meilleur des mondes »

25. La prise en compte de ces deux ouvrages de science-fiction dans le cadre de l'analyse de la surveillance ne relève pas d'un passage obligé. En effet, dans le cadre de cette analyse, la surveillance diffuse ne doit pas être envisagée comme une simple activation de la figure d'un « Big Brother⁷¹ ». Il faut au contraire se détacher à tout prix de cette image fautive, puisque ne traduisant pas la réalité de la société contemporaine. Bien que cette figure d'un Big Brother omniscient ne soit

⁶⁸ POSTMAN Neil, *Se distraire à en mourir*, Traduit de l'américain par Thérèse de Chérissey, Préface de Michel Rocard, Editions Fayard, Collection Pluriel, 2010.

⁶⁹ Ibid. p. 231 - 242. Pour une compréhension rapide de cet avertissement, voir l'excellente illustration de ce dernier en bande dessinée réalisée par Stuart Mc Millan et traduit par Jessica Aubin, en mai 2009, MC MILLAN Stuart; *Se distraire à en mourir - BD: Aldous Huxley & George Orwell par Neil Postman*, traduction Jessica Aubin, Mai 2009, En ligne: <http://partage-le.com/2016/08/se-distraire-a-en-mourir-bd-huxley-orwell-par-neil-postman/> (dernière consultation: 5 mars 2018)

⁷⁰ Postman écrit d'ailleurs à ce propos que: « *ceux qui évoquent ce problème doivent élever la voix au risque de paraître hystériques et de se voir accuser d'empoisonner le monde* », Ibid. p. 232. Un autre ouvrage paru récemment opère la même conclusion: « *c'est un sentiment diffus, presque imperceptible, et que nous sommes de plus en plus nombreux à partager. Comme ce petit caillou dans la chaussure, qui ne blesse pas mais dont la présence se rappelle sans cesse à nous, et que les Romains appelaient « scrupule ». Un sentiment qu'on évite de partager pour n'être pas aussitôt rangé dans la catégorie des complotantes ou des paranoïaques. Le sentiment que, par bien des aspects, nous ne sommes plus tout à fait dans ce qu'on peut appeler un régime démocratique* » in. POLONY Natacha & Le Comité Orwell, *Bienvenue dans le PIRE DES MONDES - Le triomphe du soft totalitarisme*, Editions Plon, Paris, 2016, p. 8.

⁷¹ ORWELL George, *1984*, Traduit de l'anglais par Amélie Audiberti, Folio, Gallimard, 2003,

pas représentatif de la réalité, l'ouvrage d'Orwell et celui de Huxley traduisent d'un lien palpable entre le droit et la littérature. Ainsi que le rappelle François Ost, « *tout se passe comme si, parmi toute la gamme des scénarios qu'imagine la fiction, la société sélectionnait une intrigue type qu'elle normalisait ensuite sous forme de règle impérative assortie de sanctions*⁷² ». De l'adage « *ex facto ius oritur*⁷³ », on passerait progressivement à l'adage « *ex fabula ius oritur*⁷⁴ ». Cette hypothèse se vérifie pleinement avec le concept de surveillance, sa normalisation⁷⁵, sa banalisation⁷⁶.

26. L'introduction de l'ouvrage de Neil Postman précité s'inscrit dans la vérification de cette hypothèse. L'auteur écrit ainsi: « *Orwell craignait ceux qui interdisaient les livres. Huxley redoutait qu'il n'y ait même plus besoin d'interdire les livres car plus personne n'aurait envie d'en lire. Orwell craignait ceux qui nous priveraient de l'information. Huxley redoutait qu'on ne nous en abreuve au point que nous en soyons réduits à la passivité et à l'égoïsme. Orwell craignait qu'on ne nous cache la vérité. Huxley redoutait que la vérité ne soit noyée dans un océan d'insignifiantes. Orwell craignait que notre culture ne soit prisonnière. Huxley redoutait que notre culture ne devienne triviale, seulement préoccupait de fadaïses. Car, comme le faisait remarquer Huxley dans *Brave New World Revisited*, les défenseurs des libertés et de la raison, qui sont toujours en alerte pour s'opposer à la tyrannie, « ne tiennent pas compte de cet appétit quasi insatiable de l'homme pour les distractions ». Dans *1984*, ajoutait Huxley, le contrôle des gens s'exerce en leur infligeant des punitions; dans *Le Meilleur des Mondes*, il s'exerce en leur infligeant du plaisir. En bref, Orwell craignait que ce que nous haïssons ne nous détruise; Huxley redoutait que cette destruction ne nous vienne plutôt de ce que nous aimons. Le thème de cet ouvrage repose sur l'idée que Huxley avait vu plus juste qu'Orwell*⁷⁷ ». Ce retour à la fiction permet à l'auteur, dans le cadre de son analyse, de critiquer avec vigueur nos sociétés modernes « désenchantées⁷⁸ », entièrement tournées vers le divertissement, la consommation d'information, de culture, voire plus globalement de

⁷² OST François, *Raconter la loi - Aux sources de l'imaginaire juridique*, Odile Jacob, 2004, p. 30

⁷³ Ibid. (le droit tire son origine du fait)

⁷⁴ Ibid. (c'est du récit que sort le droit)

⁷⁵ Voir en ce sens *Infra* Partie 1, Titre 1.

⁷⁶ Voir en ce sens *Infra* Partie 1, Titre 1, Chapitre 1, Section 2, Paragraphe 2.

⁷⁷ POSTMAN Neil, Op. Cit., p. 14

⁷⁸ Nous empruntons ce terme à Max Weber, qui, dans le cadre d'une critique de la modernité, déclarait que cette dernière conduisait au désenchantement du monde. (Voir en ce sens *infra* Partie 1, Titre 1, Chapitre 1, Section 1, Paragraphe 1).

distraktion⁷⁹.

27. Ce premier point d'analyse, dans la réactivation de ces deux fictions, permet de comprendre qu'il est fondamental de placer l'individu au centre de l'analyse de la surveillance diffuse. Ainsi que le rappelait Aldous Huxley dans la préface de son ouvrage, *le meilleur des mondes*, « *le thème du Meilleur des mondes n'est pas le progrès de la science en tant que tel; c'est le progrès de la science en tant qu'il affecte les individus humains*⁸⁰ ». La vision anthropologique de la surveillance permet, d'une part, d'analyser l'individu comme participant pleinement, de manière consciente ou non, à la diffusion de cette dernière⁸¹. Ainsi que le démontre fort justement Postman, nous sommes entrés dans une civilisation qui correspond à la vision décrite par Huxley: un meilleur des mondes dominé par la Science, la technique, les technologies de l'information et de la communication; plus globalement un monde dominé par la croyance dans le Progrès scientifique et technologique. Le citoyen, les individus transformés en consommateur d'informations, de culture, de divertissement tendent alors à consommer toujours plus de technologies de l'information et de la communication.

28. Deux idées clés sont à la source de nos sociétés modernes et expliquent la diffusion de la surveillance. L'économie du numérique, qui a permis à la surveillance diffuse de naître, est fondée sur une logique d'offres permanentes, sans cesse renouvelées, et de création de nouvelles demandes, de nouveaux besoins⁸². Placé dans une position de consommateur, l'individu doit consommer toujours plus de technologies. Ainsi, quand un individu accepte un nouveau dispositif socio-technique - caméra, smartphone, puce RFID, carte de fidélité - , ou un nouvel usage de ces

⁷⁹ Ces éléments font l'objet d'un vaste questionnement concernant la relation de l'individu avec son milieu social technicisé. Nous démontrons que l'individu s'est adapté à la diffusion de la surveillance en l'embrassant pleinement. Passant d'un homo-numericus fasciné par les nouvelles technologies de l'information et de la communication, l'individu devient progressivement un citoyen-consommateur de surveillance, ou pour reprendre les termes d'Hannah Arendt, un philistin cultivé, numérisé, et narcissique. (Voir *infra* Partie 1, Titre 1, Chapitre 1, Section 2, Paragraphe 2.

⁸⁰ HUXLEY Aldous, *Le meilleur des mondes*, Cooltour, 25 avril 2015, p. 8

⁸¹ Voir *Infra* Partie 1, Titre 1, Chapitre 2

⁸² Le numérique augmente en effet la vitesse de réaction de son économie, offre et demande se produisent concurremment par et pour le numérique. Pour illustrer le propos, on notera les propos de Nicolas Curien et Eric Brousseau qui notaient en 2001 que: « *l'économie propre au « système » Internet, en suscitant des relations et des coordinations originales entre les agents économiques et les acteurs sociaux, agit comme un catalyseur de mutations dans la structure des marchés et celle des hiérarchies, synthétisant - comme dans un laboratoire - le modèle d'une future économie numérique en cours de gestation* » in. BROUSSEAU Eric, CURIEN Nicolas, *Introduction: Economie d'Internet, Economie du numérique*, Revue économique, Numéros Hors-série 2001, Economie de l'Internet, pp. 7 - 36, En ligne: http://www.persee.fr/doc/AsPDF/reco_0035-2764_2001_hos_52_1_410273.pdf (dernière consultation: 5 mars 2018)

dispositifs - de la simple recherche sur Internet, au *quantified self*⁸³ -, cela force d'autres personnes à accepter ces mêmes usages. L'illustration de ce propos par l'usage exponentiel des réseaux sociaux, devenu effet de mode, il y a une dizaine d'année est assez frappant de réalité. L'exemple plus récent de l'installation de l'application *Pokemon Go* témoigne lui aussi de cet effet de mode cyclique que porte en son sein le progrès, la technique, les technologies de l'information et de la communication. De ces usages nouveaux, ou de cette nouvelle offre du marché du numérique, découlent une conséquence qui sert la surveillance diffuse. A partir du moment où ces nouveaux usages s'ancrent dans la société, et donc, à partir du moment où les usagers - consommateurs acceptent de dévoiler leurs données personnelles, leurs informations, alors le fait de ne pas dévoiler les siennes, de ne pas participer à cette mode devient sujet à critique, et est même considéré comme anormal. Il n'est pas rare d'entendre des propos empreints de critiques sur l'absence d'usage des réseaux sociaux, ou encore d'applications de remise en forme, de mesure de son activité sportive qui elles-mêmes engendrent offre de nouveaux capteurs, et demande de toujours plus d'informations techniques ou personnelles.

29. D'autre part, à travers son analyse, Postman décrit un individu totalement tourné vers la distraction, le divertissement. Il met en opposition Orwell et Huxley sur la notion de contrôle social organisé pour l'un autour de la punition; pour le second, autour du plaisir. N'est ce pas là la description de nos sociétés contemporaines? Le plaisir procuré par les usages technologiques, le confort, ou la sécurité qu'ils permettent, tendent à éluder la dangerosité potentielle de ces dispositifs en terme de libertés, de vie en société, de démocratie. Notons à titre d'illustration, l'absence de réactions, voire de révoltes réelles face à « *la grande surveillance*⁸⁴ », « *la globalisation de la*

⁸³ La CNIL française propose l'explication suivante pour tenter d'appréhender la notion du *quantified self* . « *En Français, on a tendance à traduire *quantified self* par « auto-mesure de soi ». L'élaboration d'un « soi » commensurable car « chiffré », renvoie bien à l'obsession contemporaine pour une objectivité qui passe par la mise en nombres. Pourtant, la quantification et la mesure sont deux idées très différentes. Comme l'expliquait Alain Desrosières, quantifier consiste à « exprimer et faire exister sous une forme numérique ce qui, auparavant, était exprimé par des mots et non par des nombres » alors que « l'idée de mesure implique que quelque chose existe sous une forme déjà mesurable (...) comme la hauteur de la Tour Eiffel ». La « bonne santé », la « bonne humeur », ne sont pas des choses qui se laissent facilement « mesurer » indépendamment de conventions d'équivalences préalablement définies. Le phénomène du *quantified self* relève d'une démarche non pas de mesure mais de quantification continue, en temps réel, – contribuant à la production sociale de normes de comportements, de performance et de santé, éminemment évolutives... et permettant la visualisation et, éventuellement, la mise en comparaison de leurs progrès respectifs par les utilisateurs reliés directement à l'Internet à travers les capteurs qui les « quantifient ».* in. CNIL, Cahiers IP n°02, *Le corps, nouvel objet connecté – Du *quantified self* à la M-Santé : les nouveaux territoires de la mise en données du monde*, CNIL, Mai 2014, p. 4, En ligne: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL_CAHIERS_IP2_WEB.pdf (dernière consultation: 5 mars 2018)

⁸⁴ VADROT Claude-Marie, *La grande surveillance - Caméras, ADN, portables, Internet...*, Collection L'Histoire immédiate, Editions du Seuil, 2007

*surveillance*⁸⁵ », ou encore à l'avènement d'une « *société de surveillance*⁸⁶ ». Pour exemple, on aurait pu penser que les révélations d'Edward Snowden quant aux programmes de surveillance mis en place par des agences gouvernementales américaines auraient amené de vives réactions de la part des citoyens, des individus. Ce n'est pas le cas⁸⁷. Hormis quelques initiatives isolées⁸⁸, l'ampleur des problématiques posées en terme de liberté, et ce qu'elles traduisent des sociétés contemporaines en terme de démocratie, d'Etat de Droit, est totalement éludé. Par l'omniprésence médiatique de la lutte contre le terrorisme, de la sécurité, les questionnements sous-jacents liés à la surveillance de masse organisée par les Etats-Unis en collectant d'innombrables données sur des citoyens ordinaires du monde entier sont mises au rebut. Pire encore, les gouvernements⁸⁹ s'efforcent de détourner l'attention des citoyens des vrais problématiques en attirant l'attention sur la trahison de ces lanceurs d'alerte.

30. Ces éléments, concernant la vision anthropologique de la surveillance diffuse, font des individus des « *Little brother*⁹⁰ » candide. Du « *tout va pour le mieux dans le meilleur des mondes*

⁸⁵ MATTELART Armand, *La globalisation de la surveillance - Aux origines de l'ordre sécuritaire*, Editions la découverte, 2007

⁸⁶ Conférence Internationale des commissaires à la protection des données personnelles et à la vie privée, Communiqué de fermeture de la 28ème Conférence des 2 et 3 novembre 2006, *Une société de surveillance?*, Londres, Grande Bretagne, En ligne: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/06-11-03_London_Communique_EN.pdf (dernière consultation: 5 mars 2018), Ligue des Droits de l'Homme, *Résolution adoptée lors du 85ème congrès de la LDH - Société de surveillance, vie privée et libertés*, En ligne: http://www.ldh-france.org/IMG/pdf/Resolution_Societe_de_surveillance_-_85eme_congres_def.pdf (dernière consultation 5 mars 2018), FOREST David, *Abécédaire de la société de surveillance*, Éditions Syllepse, 2009, Ligue des droits de l'Homme, *Une société de surveillance ? L'état des droits de l'Homme en France*, La découverte, édition 2009

⁸⁷ Voir en ce sens: LYON David, *Surveillance after Snowden*, Polity Press, 2015. Voir également, infra Partie 1.

⁸⁸ On pense notamment au groupe de Hacker Anonymous, ou à la montée en puissance d'un parti politique: le parti pirate.

⁸⁹ Peu de temps après les révélations de Snowden concernant les programmes (PRISM et XKeyscore) de la NSA (juin 2013), on apprend en juillet 2013 qu'il existerait un « prism à la française » organisé par la DGSE qui serait, selon l'un des dirigeants de la DGSE, non pas illégal, mais « a-legal ». La CNIL française s'est évertuée à prouver de l'illégalité d'un Prism à la française, attestant que « *le régime juridique des interceptions de sécurité interdit la mise en œuvre par les services de renseignement, d'une procédure telle que Prism. Chaque demande de réquisition de données ou d'interception est ciblée et ne peut pas être réalisée de manière massive, aussi quantitativement que temporellement. De telles pratiques ne seraient donc pas fondées légalement* ». Voir en ce sens: FOLLOROU Jacques, JOHANNES Franck, *Révélation sur le Big Brother français*, Le Monde, 4 Juillet 2013, En ligne: http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (dernière consultation: 5 mars 2018), CLAIROUIN Olivier, *Il y a un vrai Prise à la française*, Le Monde, 4 Juillet 2013, En ligne: http://www.lemonde.fr/societe/video/2013/07/04/il-y-a-un-vrai-prism-a-la-francaise_3441637_3224.html (dernière consultation: 5 mars 2018). Et concernant les révélations d'Edward Snowden et l'affaire Prism: SZADKOWSKI Michaël, LELOUP Damien, *Prism, Snowden, surveillance: 7 questions pour tout comprendre*, Le Monde, 2 juillet 2013, En ligne: http://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html (dernière consultation: 5 mars 2018)

⁹⁰ DOCTOROW Cory, *Little Brother*, Pocket Jeunesse, Janvier 2012, ou plus récemment, ENTHOVEN Raphaël, *Little Brother*, Editions Gallimard, Collection Blanche - Essais, 2017.

*possibles*⁹¹ » à l'édification d'un « *meilleur des mondes*⁹² », la fiction semble prendre le pas de la réalité. Et déjà, des auteurs alertent sur l'avènement d'un « *empire du moindre mal*⁹³ » et la naissance du « *Monstre doux*⁹⁴ » de Tocqueville⁹⁵, ou encore, souhaitent aux individus la « *Bienvenue dans le pire des mondes*⁹⁶ » qui consacre « *le triomphe du soft totalitarisme*⁹⁷ ». Au delà des titres de ces ouvrages, qui semblent relever de la fiction, ces auteurs, journalistes, philosophes ou sociologues contemporains, appellent à la conscience des individus, afin qu'ils échappent à « *l'amour de leur servitude*⁹⁸ » organisée par quelques géants de la Silicon Valley.

B. Kafka, Little brother et la désinstitution progressive du Droit

31. Les prophéties d'Orwell et de Huxley, en ce qu'elles participent à une logique d'anticipation politique, doivent nécessairement être approfondies dans le sens où ces deux utopies dépeignent la disparition du Droit au profit de la constitution d'une dictature totalitaire pour l'un; dictature du bonheur et du plaisir pour le second. C'est en cela que ces utopies doivent être confrontées nécessairement à l'oeuvre de Kafka, et dépasser l'idée de la disparition du Droit, au profit de sa désinstitution par la norme.

32. Que ce soit dans *1984* ou dans *Le Meilleur des mondes*, l'asservissement des individus par

⁹¹ Voltaire, *Candide*, op. cit.

⁹² Op. Cit.

⁹³ MICHEA Jean-Claude, *L'empire du moindre mal - Essai sur la civilisation libérale*, Editions Flammarion, Collection Champs Essai, 2010

⁹⁴ En ce sens voir: LAVENUE Jean-Jacques, « Gouvernance des données et naissance du « monstre doux » », in. BOUHADANA Irène, Gilles William (sous la direction de), *Droit et gouvernance des données publiques et privées à l'heure du numérique*, Les Editions Imodev, Février 2015, pp. 33 - 55; mais également: SIMONE Raffaele, *Le Monstre doux - L'Occident vire-t-il à droite ?*, traduit par Katia Bienvenu, Collection Le Débat, Gallimard, 2010

⁹⁵ DE TOCQUEVILLE Alexis, *De la démocratie en Amérique II*, (3ème et 4ème parties), Collection Garnier-Flammarion, Editions Flammarion, 1999, p. 146 et s.

⁹⁶ POLONY, Op. Cit.

⁹⁷ Ibid.

⁹⁸ La préface du *Meilleur des Mondes* de Aldous Huxley est frappante de réalisme et de bon sens. Ce dernier écrit: « *Il n'y a, bien entendu, aucune raison pour que les totalitarismes nouveaux ressemblent aux anciens. Le gouvernement au moyen de triques et de pelotons d'exécution, de famines artificielles, d'emprisonnements et de déportations en masse, est non seulement inhumain (cela, personne ne s'en soucie fort de nos jours); il est - on peut le démontrer - inefficace: et, dans une ère de technologie avancée, l'inefficacité est le péché contre le Saint-Esprit. Un Etat totalitaire vraiment « efficace » serait celui dans lequel le tout-puissant comité exécutif des chefs politiques et leur armée de directeurs auraient la haute main sur une population d'esclaves qu'il serait inutile de contraindre, parce qu'ils auraient l'amour de leur servitude. La leur faire aimer - telle est la tâche assignée dans les Etats totalitaires d'aujourd'hui aux ministères de la propagande, aux rédacteurs en chef de journaux, et aux maîtres d'école* ». in. HUXLEY Aldous, *Le meilleur des mondes*, Cooltour, 25 avril 2015, p. 12. Voir également: VION - DURY Philippe, *La nouvelle servitude volontaire - Enquête sur le projet politique de la Silicon Valley*, FYP Editions, 2016

une forme de dictature a été rendue possible par l'effacement progressif des libertés, de toutes références au passé, à l'histoire, ainsi que par la disparition totale du Droit. Ces sociétés s'organisent autour d'une nouvelle croyance: le progrès scientifique et technique, et ce qu'il a engendré: stabilité, bonheur, divertissement, abolition de toutes formes de conflits, contrôle social, censure, délation, manipulation orchestrée par des discours politiques, propagande. La technique dans ces utopies, les technologies de l'information et de la communication dans nos sociétés, sont présentées comme la nouvelle doxa. Elles forment la société à la croyance commune de la toute puissance libératrice⁹⁹ de l'usage des outils technologiques, et à la maîtrise de nos comportements. Cette doxa amène nos contemporains à se placer d'eux-mêmes dans le champs d'observation de la surveillance, sans questionner la potentielle dangerosité, en termes de libertés et de droits fondamentaux que porte en son sein ce nouveau mode de vie.

33. Ainsi que le démontre François Ost, « *Huxley éradiquait l'hétérodoxie par la manipulation génétique et le conditionnement psychologique; Orwell parvient au même effet par la stérilisation du langage: quand « les mots pour le dire » viennent à faire défaut, c'est la pensée elle-même qui est condamnée à l'étouffement. A la fin, c'est le langage normatif lui-même qui aura disparu - et avec lui le droit, le crime, la justice, le pardon, et toutes ces sortes de choses: ainsi s'exprime O'Brien, un séide de Big Brother qui s'emploie à laver le cerveau de Winston Smith, qui aura tenté, bien vainement, de s'opposer: « Le commandement des anciens despotisme était: « tue ne dois pas ». Le commandement des totalitaires était: « Tu dois ». Notre commandement est: « Tu es ». Aucun de ceux que nous amenons ici ne se dresse plus jamais contre nous¹⁰⁰ »*. Dans nos sociétés contemporaines, le mythe du « je n'ai rien à cacher, je n'ai rien à me reprocher » et la mise en donnée du monde ont permis de faire taire toute hétérodoxie possible. La réduction de l'individu à la dynamique du calcul et de la prévision, que porte en sein la surveillance diffuse, a engendré le passage du « tu ne dois pas » du Droit, en tant que « technique de l'interdit¹⁰¹ », au « tu es » d'une société faussement libérale-libertaire, et profondément narcissique.

34. Ce passage du « tu ne dois pas » au « tu es » emporte des conséquences sur le Droit. D'une part, ce dernier se voit, dans nos sociétés contemporaines, de plus en plus, subjectivé, individualisé.

⁹⁹ En ce sens, voir BRETON Philippe, *L'utopie de la communication - le mythe du village planétaire*, Collection Essais, Editions La Découverte / Poche, 1997.

¹⁰⁰ OST François, *Raconter la loi - Aux sources de l'imaginaire juridique*, Odile Jacob, 2004, p. 553.

¹⁰¹ Voir en ce sens, SUPIOT Alain, *Homo juridicus - Essai sur la fonction anthropologique du Droit*, Editions du Seuil, Collection La couleur des idées, 2005, p. 26

Prenant appui sur la doctrine Law and Economics, Alain Supiot démontre que « *les juristes eux-mêmes sont ainsi atteints par la rage du calcul et cherchent à leur tour à réduire la société des hommes à la somme de leurs utilités individuelles. Dans cette perspective, il n'est de droits qu'individuels. Toute règle est commuée en droits subjectifs: droit à la sécurité, à l'information, au respect de la vie privée, à la dignité, à l'enfant, au procès équitable, à la connaissance des origines, ... On distribue les droits comme on distribuerait des armes, et ensuite que le meilleur gagne*¹⁰² ». D'autre part, là où la « *règle ne peut pas être commuée en droits subjectifs* », la norme remplace le droit. Qu'il s'agisse des messages publicitaires sponsorisés par le gouvernement exhortant les individus à « manger 5 fruits et légumes par jour », « manger, bouger », « arrêter de fumer »; ou encore de méthodes plus douce telles que les « nudges¹⁰³ » autrement qualifiés de « paternalisme libertarien »; qu'il s'agisse également de normes et de standards liés aux nouvelles formes de management privé ou public, ou encore des normes proprement techniques qui obligent l'individu à fournir ses données personnelles pour user d'un service, d'une application ou d'un dispositif socio-technique; force est de constater que la norme est partout. De fait, le Droit s'adapte à ces nouvelles formes de normativité, et/ou est réduit de plus en plus, voire désinstitué¹⁰⁴.

35. Ceci n'est pas sans rappeler les questionnements des oeuvres de Kafka quant à la perversion du Droit, ou à son imposture¹⁰⁵. Dans *le Procès*, Kafka met en scène Joseph K. mis en état

¹⁰² Ibid. p. 22

¹⁰³ Selon les penseurs de cette méthode, le nudge est une méthode douce permettant d'inspirer la bonne décision. Ainsi le comportement individuel s'altère quelque peu, dans un sens prévisible, du fait d'une incitation douce mise en place par des acteurs publics ou privés. On oriente l'individu vers des choix, des actions d'intérêt individuel ou collectif. Les nudges ont été théorisés comme une réponse au manque de rationalité des individus, et s'inscrivent dans le cadre plus global des théories de l'économie comportementale. Voir: THALER Richard, SUNSTEIN Cass, *Nudge - Improving Decisions about Health, Wealth and Happiness*, Penguin Books, 2012. Ces auteurs sont tous deux des universitaires américains: le premier est économiste à la Chicago University, le second est professeur de droit à Harvard.

¹⁰⁴ Voir en ce sens: SUPIOT Alain, *Homo juridicus - Essai sur la fonction anthropologique du Droit*, Editions du Seuil, Collection La couleur des idées, 2005, et, OST François, *A quoi sert le Droit ? - Usages, Fonctions, Finalités*, Editions Bruylant, Collection Penser le Droit, 2016.

¹⁰⁵ KAFKA Franz, *Le Procès*, Editions Gallimard, Collection Folio Classique, 1987. Dans ses romans clés (*Le procès*, *Le Château*, et *la Métamorphose*), Kafka dénonce la modernité de nos sociétés et ses conséquences pour l'individu. On notera également une analyse de François Ost: « *on pourrait dire, pour reprendre encore les catégories de Ricoeur, que cet univers est celui d'une « morale sans éthique »: un monde où la loi, faute d'être intériorisée dans la réciprocité des reconnaissances mutuelles, faute donc de faire sens commun, se donne sous la forme des plus sévères interdits. Si l'éthique est le monde des valeurs, et la morale le domaine des interdits, alors une « morale sans éthique » est un monde où, littéralement, les « interdits sont sans valeur ». Ce pourrait être, rigoureusement, la formule de l'univers où évoluent les héros de Kafka: un monde d'implacables commandements totalement dépourvus de sens et de valeur positive (libératrice) pour leurs destinataires. Un monde où la défaillance des relais de la loi contraint le « je » à une oscillation sans fin entre l'irresponsabilité et l'autoaccusation - celle de ce « maître intérieur » dont parlait saint Augustin et que Freud qualifiera de « surmoi ». Un surmoi, « automate imbécile », qui, dans l'imaginaire inconscient, ne donne accès qu'aux plus archaïques formes du commandement. un commandement sans commandant vital, sans médiateur réel. Texte absurde, sans appel et sans réponse (donc sans responsabilité) - automatisme aveugle d'une loi de nécessité qui ne peut qu'engendrer terreur et culpabilité. Loin d'arracher le sujet à l'état de nature, une telle loi l'y maintient ou l'y fait régresser* », in. OST François, *Raconter la loi (...)*, Op. Cit. p 576 - 577.

d'arrestation au saut du lit. Rien n'est écrit quant aux raisons de cette arrestation¹⁰⁶. Bien que condamné, K., reste en liberté, et conserve sa vie sociale. A travers son ouvrage, Kafka questionne la signification de cette liberté, devenue outil au service d'un pouvoir, d'une bureaucratie sans nom. L'assujettissement à notre propre liberté, à la volonté égoïste de préserver un espace d'autonomie fondé sur un auto-contrôle, sont autant de sujets que dénoncent Kafka. La surveillance diffuse, en ce qu'elle se fonde sur un triptyque de sécurité- protection, liberté - principalement réduite à son versant économique, la consommation - , et le bien-être, tire son pouvoir d'une forme nouvelle de gouvernance des individus. Cette nouvelle manière de gouverner n'est pas sans rappeler la critique de Kafka, et l'assujettissement à notre propre conception de la liberté. La fiction semble ici à nouveau prendre le pas de la réalité. Ainsi que le rappelait Neil Postman dans la conclusion de son livre, consacrée à « *l'avertissement de Huxley* »: « *l'esprit d'une culture peut se flétrir de deux manières. Dans la première - celle de Orwell -, la culture devient une prison. Dans la seconde - celle de Huxley -, la culture devient une caricature*¹⁰⁷ ». Bien que l'auteur évoque dans cet ouvrage l'institutionnalisation des médias et de la télévision dans la société américaine du milieu des années 80, son analyse trouve application à l'ensemble des sociétés occidentales¹⁰⁸, mais également à la surveillance diffuse. Selon Postman, les médias ont un impact direct sur nos sociétés: l'avènement d'une culture du divertissement, créant ainsi un espace public entièrement tourné vers la distraction, et des individus « *traités comme des enfants, priés de se divertir sans rien prendre au sérieux*¹⁰⁹ ». La question se pose alors de savoir si le droit n'est pas en train de devenir une caricature, à l'image de la culture décrite par Postman, au vu de la diffusion de la surveillance, de son institutionnalisation.

36. Afin de conclure ces propos concernant la fiction et le Droit, reprenons la définition de l'utopie. Selon Leszek Kolakowski, le contenu de l'utopie: « *c'est la certitude eschatologique, la foi en une société où non seulement les sources du mal, du conflit ou de l'agression sont écartées mais où se réalise une réconciliation totale entre ce que l'homme est, ce qu'il sait, ce qu'il devient et ce*

¹⁰⁶ Qui l'accuse ? De quoi est-il accusé ? Qui sont les agents qui procèdent à cette arrestation ?

¹⁰⁷ Ibid. p. 231.

¹⁰⁸ Comme le rappelle Michel Rocard dans la préface du livre de Postman précité: « *nous sommes sous le régime américain, et l'essentiel de ce livre vaut pour nous, Européens* ». in. POSTMAN Neil, *Se distraire à en mourir*, Traduit de l'américain par Thérèse de Chérisey, Préface de Michel Rocard, Editions Fayard, Collection Pluriel, 2010, p. 10

¹⁰⁹ Ibid. Quatrième de couverture.

*qui l'entoure*¹¹⁰ ». Le discours politico-juridique concernant l'usage des technologies dans la société contemporaine s'inscrit pleinement dans cette « *certitude eschatologique, cette foi* ». L'avènement des concepts de sécurité, plus globalement de sécurité humaine, de prévention, de menaces, de dangers, leurs reconnaissance par le Droit national et international, tout tend dans notre société à l'institutionnalisation de la surveillance diffuse, et l'individu n'en a pas forcément conscience. Bien qu'il faille s'éloigner de la dimension fictionnelle, les avertissements de Postman et de François Ost ont une résonance particulière lorsqu'ils sont appliqués à nos sociétés contemporaines. Ces avertissements doivent être gardés à l'esprit, afin de comprendre si la surveillance diffuse, c'est-à-dire la réalité contemporaine, a pris le pas sur la fiction.

Paragraphe 2: La surveillance diffuse: une fiction pleinement instituée dans nos sociétés

37. Présenter le lien qu'entretient la surveillance contemporaine avec un imaginaire lié à la science-fiction, en tirer les enseignements sur les politiques-fictions et le Droit-fiction, est nécessaire pour appréhender les prémices de l'institutionnalisation de la surveillance dans nos sociétés. Néanmoins, il importe d'aller un peu plus loin pour comprendre en quoi la surveillance diffuse est devenue progressivement une fiction instituante (A). Si la surveillance diffuse s'est pleinement instituée dans nos sociétés, il faut également envisager son lien avec la surveillance classique, et ce, afin de tenter de définir ce concept, de comprendre son sens, sa portée, ses objectifs (B). L'un des premiers constats à opérer est alors celui de la défaillance du Droit dans l'appréhension de ce phénomène. On se tournera vers la sociologie qui, depuis les années 2000, pense la surveillance contemporaine comme un phénomène en évolution constante.

A. L'institutionnalisation progressive d'une fiction dans les sociétés contemporaines: la diffusion de la surveillance

38. Depuis le début du 21^{ème} siècle, la surveillance traditionnelle, liée à une forme de contrôle social et aux théories de Foucault, Deleuze et Guattari, se transforme. Elle n'est plus seulement liée à la simple notion de contrôle social, et semble être partout. Elle n'est plus associée à un acteur défini: l'Etat. Elle est produite par tout un chacun: l'Etat, les entreprises, les entreprises et l'Etat, nous, les individus d'une société mondiale obnubilée, fascinée par le confort et la sécurité que

¹¹⁰ KOLAKOWSKI Leszek, *L'esprit révolutionnaire, suivi de marxisme : utopie et anti-utopie*, traduction de l'anglais, de l'allemand et postface Jacques Dewitte, Editions Complexe, Presses Universitaires de France, 1978, p. 131

produisent des systèmes socio-techniques. En ce sens, et à l'inverse de l'étude du panoptique réalisée par Foucault, la surveillance diffuse n'obéit à aucun dessein prédéfini. Il n'y a en effet pas de projet unifié, envisagé par un acteur unique, visant la surveillance de tout un chacun. La surveillance diffuse n'est, en premier lieu, que la poursuite logique d'un projet de société, la société de l'information et de la communication. Elle est ensuite un concept permettant de rendre compte d'un ensemble de stratégies de développement et de déploiement technologique non coordonnées, permettant la collecte, l'enregistrement et le traitement de nombreuses données personnelles ou non. Enfin, elle est la conséquence ultime du paradigme technologique qui bon an mal an a permis la mise en données du monde et la réduction de l'individu à ses traces, ses données, ses informations.

39. De nos téléphones géolocalisés, leurs caméras et appareils photos dernières générations; de nos connexions et relations sur les réseaux sociaux, à nos cartes bancaires, de fidélités; des caméras de vidéo-protection à l'organisation d'une e-police qui à travers les radars automatique nous envoie des amendes lorsque nous ne respectons pas le code de la route; de l'organisation d'une véritable e-administration voire d'une e-démocratie; un sentiment gênant d'observation constante nous envahit. Pourquoi cette observation constante? L'individu est-il devenu à ce point « un loup¹¹¹ » pour lui même et pour les autres qu'il faille qu'il soit sous observation constante? Les exemples précités témoignent de ce qu'est devenue la surveillance aujourd'hui. Le monde est si dépendant des technologies de l'information et de la communication qu'il ne s'est pas rendu compte qu'il avait créé une surveillance globale, massive, généralisée à tous nos usages. La vie quotidienne est l'objet de l'examen minutieux, du contrôle et de l'attention d'un ensemble de dispositifs. Il n'est plus possible aujourd'hui d'échapper à l'oeil diffus de la surveillance qu'elle soit effectuée par des dispositifs de traçage, de marquage, d'écoute, d'enregistrement, de vérification en vue d'assurer un bénéfice quelconque allant de la sécurité à l'accès à la connaissance, et plus loin à la

¹¹¹ Nous empruntons ces mots à Thomas Hobbes qui dès le 17^{ème} siècle écrivait: « *Il ne fait aucun doute que les deux formules sont vraies : l'homme est un dieu pour l'homme, et l'homme est un loup pour l'homme. La première, si nous comparons les citoyens entre eux, la seconde, si nous comparons les États entre eux. Là, l'homme parvient, par la justice et la charité, qui sont des vertus de paix, à ressembler à Dieu ; ici, même les hommes de bien doivent, à cause de la dépravation des méchants et s'ils veulent se protéger, recourir aux vertus guerrières – la force et la ruse – c'est-à-dire à la rapacité des bêtes. Or même si les hommes, par un penchant inné, s'imputent mutuellement cette rapacité dont ils font grief, en jugeant leurs propres actes dans la personne des autres comme on juge devant un miroir la gauche être la droite et la droite être la gauche, le droit naturel ne permet toutefois pas que ce qui provient de la nécessité de sa propre préservation soit un vice* ». in. HOBBS Thomas, *Du Citoyen*, présentation et traduction par Philippe Crignon, Editions Flammarion, Collection G.F. 1442, 2010, p. 75 - 76. On pourrait également tester ces deux formules à notre époque. D'une part, les progrès technologiques permettent en effet de pouvoir traiter de l'individu comme un Dieu qui, rêvant de l'immortalité, s'organise pour « s'augmenter » (transhumanisme), pour s'implanter des puces dans le cerveau (Elon Musk et l'entreprise Neuralink), se transforme en terminal (l'entreprise suédoise Epicenter), ou envisage d'être aussi intelligent que l'intelligence artificielle. D'autre part, les progrès technologiques font ressortir la rapacité de l'individu décrite par Hobbes: violation de la vie privée, rationalisation de l'ensemble des activités humaines, société de la peur et de l'attention permanente.

reconnaissance. De fait, et pour paraphraser quelque peu Lucien Sfez, la surveillance diffuse parvient à s'élever au rang de fiction instituante et pleinement instituée; là où la technique et le progrès ne représentaient qu'un essai instituant .

40. En effet, ainsi que l'écrivait Lucien Sfez, « *Attention: « fiction » ne veut pas dire « illusion ». La fiction n'est pas hors de la réalité. Elle se réalise à tout moment. Nous l'appelons quelquefois « utopie », bien obligés de reconnaître après un moment que cette utopie s'est réalisée et devient un élément de la réalité. Ou encore, on peut constater que , malgré les réalités mises en place, les germes d'utopie ne sont pas absents de ces réalisations¹¹² » . Les liens entre fiction et réalité ayant été démontrés, il faut retenir de ces mots l'intégration de la fiction dans la réalité: la surveillance diffuse est un élément de notre réalité, de la société contemporaine. Alors qu'hier elle était une mesure d'exception visant à contrôler des populations présentées comme « à risque », la surveillance est aujourd'hui devenue banale et globale. Ces deux éléments s'expliquent entièrement par la diffusion des technologies de l'information et de la communication. L'explosion du numérique a multiplié les usages quotidiens des technologies. Ces derniers ont permis la collecte, le traitement, plus globalement la réception par différents acteurs, de toujours plus d'informations, de données techniques et personnelles. Présentées comme un véritable projet de société par le politique, l'information et la communication ont engendré la surveillance diffuse. Puis, l'individu, réduit à sa position de consommateur dans ce projet de société, s'est placé de lui-même dans le champs d'observation de la surveillance. Cette dernière est alors passée d'une approche cloisonnée (Etat versus secteur privé) à une approche systémique combinant secteur privé, public et individu. Ainsi, en tant que système, la surveillance diffuse, est de moins en moins visible dans ses effets et ses enjeux. A moins d'une révélation publique, médiatisée, nous n'avons pas conscience de faire l'objet d'une surveillance constante.*

41. Ces éléments témoignent de l'institutionnalisation progressive de la surveillance diffuse dans nos sociétés. D'une part, ils vérifient l'hypothèse de départ de l'analyse de Lucien Sfez. Ce dernier, souhaitant renouveler les analyses concernant le Progrès, la technique et la technologie, écrit: « *en tenant compte des dispositifs actuels , on constate non pas seulement un changement dans les rapports entre technique et politique, mais bien plus: un véritable renversement. Alliée de la politique en un mariage morganatique, la technique est devenue la servante-maîtresse (...). Alors*

¹¹² SFEZ Lucien, *technique et Idéologie. Un enjeu de pouvoir*, Editions du Seuil, La couleur des idées, Paris, 2002, p. 13

*il n'est plus question de voir la technique ou la technologie isolées, neutres, faisant seulement ce qu'elles ont à faire : innover, expérimenter, nous fournir des commodités pour vivre, en somme incarner le progrès. Pas plus de continuer à considérer le politique comme le gouvernail de cette merveilleuse alliée (quand d'ailleurs on veut bien prendre en compte le poids du politique, ce qui n'est pas le fait de tous les discours, loin de là)¹¹³ ». La surveillance diffuse, en ce qu'elle est continuité du projet de la société de l'information et de la communication prônée par le politique et désirée par le secteur privé, est alors organisée par les institutions¹¹⁴. D'autre part, ces éléments contredisent les conclusions de Lucien Sfez. En effet, prenant appui sur deux fictions qu'il considère comme instituante - le Capital de Marx et le contrat social de Rousseau - l'auteur de « *Technique et idéologie - un enjeu de pouvoir* », énumère les conditions pour qu'une fiction soit instituante. Il écrit alors : « 1. la visée de ces fictions traverse tout le corps social et subsume sous sa loi toutes les activités; la visée d'unification que transmet la fiction n'est pas une visée séparée de l'ensemble et ne fait pas l'objet d'une institution spéciale. 2. C'est l'intérêt général qui est visé, non comme un ingrédient dans une composition socio-politique, mais comme l'essence même du politique et du social. Cet intérêt général doit se confondre avec la conscience de tous les individus et réfléchir leur condition entière. 3. La fiction instituante présente une fin souhaitable, une véritable finalité capable de susciter le désir; devient un sujet d'amour et engage le dévouement. Elle est porteuse de valeurs, voire de la valeur¹¹⁵ ». Poursuivant son analyse, l'auteur déclare que la technique « traverse tout le corps social, toutes les activités¹¹⁶ », devenant ainsi une « discipline qui gère les autres secteurs, de telles sortes qu'ils ne peuvent plus s'en passer¹¹⁷ ». Pourtant, il conclut à l'absence d'institutionnalisation de la technique, en tant que fiction, dans nos sociétés. Il déclare que la technique ne passe pas « inaperçue en tant qu'institution séparée¹¹⁸ », qu'elle ne se confond pas « avec la conscience de l'homme en société¹¹⁹ », qu'elle ne réfléchit pas « sa condition entière¹²⁰ ». Il ajoute également qu'elle ne se confond pas avec l'intérêt général, « elle n'est qu'une*

¹¹³ SFEZ Lucien, *Technique et Idéologie. Un enjeu de pouvoir*, Editions du Seuil, La couleur des idées, Paris, 2002, p.12

¹¹⁴ Ce que Lucien Sfez appelle: « *l'amour de l'Etat-nation se confond avec l'amour de la technique* ». Ibid. p. 244

¹¹⁵ Ibid. p. 264

¹¹⁶ Ibid.

¹¹⁷ Ibid.

¹¹⁸ Ibid.

¹¹⁹ Ibid.

¹²⁰ Ibid.

*partie qui veut se faire passer pour un tout*¹²¹ ». Enfin, elle ne représente pas une finalité en soi, mis à part celle « *d'un progrès indéfini, indifférent aux humains qu'il prétend surplomber*¹²² ».

42. Pour parachever son étude, Lucien Sfez l'accentue par une dernière condition également manquante: la symbolique de la technique en tant que fiction. Son argumentation finale semble alors quelque peu hésitante. Bien que, selon lui, « *la fiction de la technique n'est pas et ne peut être fondatrice, puisqu'elle n'est pas et ne peut être instituante*¹²³ », elle s'inscrit pleinement dans des « *macro-systèmes de pouvoir et de profit*¹²⁴ ». L'objectif de l'auteur était de démontrer les enjeux économiques et politiques qui se cachent derrière le concept de technique. En cela, ces conclusions sont frappantes de réalisme. Toutefois, à travers l'évolution contemporaine de la surveillance, on ne peut être qu'en désaccord avec l'épilogue de Lucien Sfez. Si, à la lecture de l'ouvrage précité, la technique est présentée comme un essai instituant, la surveillance diffuse, qui s'inscrit dans la poursuite du phénomène technique, a « transformé » l'essai. On peut effectivement conclure à l'institutionnalisation de la surveillance dans nos sociétés contemporaines. Cette dernière, pour reprendre les conditions de la fiction instituante dégagées par Lucien Sfez, « *traverse tout le corps social, gère les autres secteurs*¹²⁵ ». Elle est devenue indispensable dans nos sociétés, passant inaperçue, se confondant « *avec la conscience de l'homme*¹²⁶ » et l'intérêt général, visant à assurer sécurité, bien être et liberté. La surveillance diffuse devient aujourd'hui une véritable finalité, en capacité de « symboliser », c'est à dire de s'instituer, « *d'unifier sous un seul registre les différents composants d'une société: les diverses activités, les divers corps, ceux qui gouvernent et ceux qui sont gouvernés, les intentions, les usages et les comportements des individus, les valeurs qui les animent*¹²⁷ ».

B. La surveillance diffuse aujourd'hui: sens, portée et objet

43. Evoquer le concept de surveillance diffuse suppose d'en comprendre le sens et la portée,

¹²¹ Ibid.

¹²² Ibid. p. 265

¹²³ Ibid. p. 273

¹²⁴ Ibid. p.274

¹²⁵ Ibid. p. 264

¹²⁶ Ibid.

¹²⁷ Ibid. p. 265.

ainsi que son objet réel (2). L'ensemble de ces éléments doit nécessairement être mis en abîme par rapport au concept et à la définition même de la surveillance (1). La surveillance, tout comme la surveillance diffuse, n'ont pas reçu de définition juridique. Il faut alors se tourner vers la sociologie, et les travaux en évolution constante de David Lyon sur ce point. Du fait de son institutionnalisation dans nos sociétés, la surveillance diffuse doit nécessairement être appropriée par le Droit. Les travaux de David Lyon permettent de réaliser cet objectif.

1. De la surveillance...

44. En 2001, David Lyon offrait la première définition de la surveillance. Selon cet auteur, la surveillance devait être entendue comme « *toute collecte et traitement de données personnelles, permettant d'identifier ou non une personne, aux fins d'influencer ou de gérer ceux dont les données ont été recueillies*¹²⁸ ». David Lyon poursuivait alors son analyse en précisant ce qu'il entendait par le terme « donnée personnelle » dans le cadre de cette définition. L'usage de ce terme est spécifiquement envisagé afin d'éliminer de la définition une surveillance incarnée, de personne à personne. Depuis 2001, David Lyon est devenu un auteur de référence en ce qui concerne la surveillance et il n'a eu d'enrichir cette définition. Son travail de recherche dédié à ce sujet représente une grille d'interprétation utile du phénomène de surveillance diffuse, qu'il est nécessaire d'évoquer ici.

45. Dans son premier ouvrage concernant la société de surveillance¹²⁹, l'auteur tente de livrer un aperçu des recherches en cours et des développements en matière de surveillance. Il constate une prolifération de cette dernière, que ce soit d'un point de vue strictement technologique, mais également au vu d'une forme de dépendance, créée par elle-même, en matière de sécurité, de commodité quotidienne et d'efficacité. Il établit également les premiers développements d'une définition claire de la surveillance qu'il décrit comme une nouvelle forme de pouvoir, une sorte de phénomène de société. Selon David Lyon, la surveillance doit être analysée comme « *une attention concentrée sur les détails personnels en vue de gérer ou d'influencer ceux dont les vies sont surveillées. Elle peut impliquer une forme d'égard envers quelqu'un, et plus souvent un contrôle.*

¹²⁸ LYON David, *Surveillance society: monitoring everyday life*, Open University Press, Buckingham, Philadelphia, 2001, p. 2, traduction libre de l'auteur des propos suivants: « *What is surveillance? In this context, it is any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered* ».

¹²⁹ LYON David, *Surveillance Society - Monitoring Everyday Life*, Open University Press, Buckingham - Philadelphia, 2001

C'est, en d'autres termes, le pouvoir de classification, de tri social. (...). Le pouvoir de surveillance n'est donc pas directement ou nécessairement lié à la coercition et à la violence, pas plus que le pouvoir traditionnel ne donne le sentiment de devoir se soumettre à l'autorité. (...) En tant que puissance classificatrice, elle s'engage dans un tri social qui peut être sévèrement panoptique, mais qui peut également être productif¹³⁰ ». A travers ces mots, on voit l'importance de livrer une analyse objective de ce qu'est la surveillance. On voit également l'ambition de mêler plusieurs sciences humaines: le droit, la philosophique, la sociologie. David Lyon construit son développement par référence à Jérémy Bentham, à Michel Foucault, mais également à Zygmunt Bauman. Il les dépasse également en prenant en compte une double dimension de la surveillance: la sécurité/coercition, l'économie/production.

46. David Lyon ne fait pas forcément appelle au contrôle social classique mais à une forme douce d'obligation et de classification pesant sur les individus. En 2007, il peaufine sa définition à travers un nouvel ouvrage à propos des recherches liées à la surveillance¹³¹, et écrit: « *la surveillance (...) est l'attention ciblée, systématique et régulière des détails personnels à des fins d'influence, de gestion de direction et de protection. La surveillance porte en effet son attention sur les individus (même par l'agrégation de données, telles que celles disponibles dans le domaine public, pouvant être utilisées pour dresser une toile de fond). Elle est focalisée. Par le recours à la notion de systématique, je veux dire que cette attention aux détails personnels n'est pas aléatoire, occasionnelle ou spontanée; elle est délibérée et dépend de certains protocoles et techniques. Au delà de ces éléments, la surveillance est devenue routinière; une partie « normale » de la vie quotidienne dans toutes les sociétés qui dépendent de l'administration bureaucratique et de certaines technologies de l'information. La surveillance quotidienne est endémique aux sociétés*

¹³⁰ Ibid. p. 152. Traduction libre de l'auteur des mots suivants: « *what kind of power are we up against when it comes to question of surveillance? As I observed at the beginning, surveillance is a focused attention to personal life details with a view to managing or influencing those whose lives are monitored. It may involve care, and more often, control. It is, in other words, the power of classification, of social sorting. (...). So surveillance power is not directly or necessarily connected with coercion and violence, nor is it the power of tradition that would yield a sense of having to submit to authority. Still less is it the power of love, with its strong sense of obligation and even sacrifice for the other person or persons. As a classificatory power it engages in social sorting which may at the severe end be panoptic, but which may equally be productive. As I have reiterated several times, surveillance always has two faces. Even its social sorting strength runs the gamut from suspicion to seduction. The one induces fear and the other desire* ».

¹³¹ LYON David, *Surveillance Studies - An Overview*, Polity Press, 2007

*modernes*¹³² ».

47. Cette longue citation a le mérite de montrer que toute analyse portant sur la surveillance devrait effectuer des liens avec la technique, le progrès mais également la sociologie de Max Weber. La recherche de David Lyon souligne la nécessité de mener une étude de la société où se développe la surveillance, de conduire une analyse anthropologique de cette dernière. Car finalement la cible de la surveillance est, et a toujours été, l'individu. A travers les analyses de David Lyon, l'usage d'un matériau de recherches large se justifie. Ses analyses montrent également un développement constant de la surveillance, qu'il faut analyser comme un phénomène de société.

2. ... A la surveillance diffuse

48. Bien que la première définition de la surveillance proposée par David Lyon soit convaincante et représentative de la réalité sociologique, son évolution conceptuelle, sans cesse enrichie par l'auteur, témoigne d'un premier point d'analyse important. Hier l'informatique posait la question des fichiers administratifs; aujourd'hui les algorithmes et les potentialités de l'intelligence artificielle posent la question de la prédiction des comportements humains, et soulève des enjeux éthiques importants¹³³.

49. En dix ans, David Lyon n'a eu de cesse de faire évoluer sa conception de la surveillance. Et ces évolutions témoignent de la prise en compte des possibilités sans cesse renouvelées qu'offrent le progrès, la science et la technique. Ce premier point constitue une base essentielle dans toute réflexion sur la surveillance. Il faut en effet prendre en considération les innovations technologiques

¹³² Ibid. p 14. Traduction libre de l'auteur des mots suivants: « *So what is surveillance? For the sake of argument, we may start by saying that it is the focused, systematic and routine attention to personal details for purposes of influence, management, protection direction. Surveillance directs its attention in the end to individuals (even though aggregate data, such as those available in the public domain, may be used to build up a background picture). It is focused. By systematic, I mean that this attention to personal details is not random, occasional or spontaneous; it is deliberate and depends on certain protocols and techniques. Beyond this, Surveillance is routine; it occurs as a « normal » part of everyday life in all societies that depend on bureaucratic administration and some kinds of information technology. Everyday surveillance is endemic to modern societies* ».

¹³³ En ce sens, voir: CNIL, *Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique - Comment permettre à l'Homme de garder la main ? - Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017, En ligne: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf (dernière consultation: 5 mars 2018). D'un point de vue factuel, on évoquera les problèmes posés par le big data dans le cadre des présidentielles américaines. En ce sens, voir: BOYER Philippe, *De l'influence du Big data sur les élections américaines*, La Tribune, 25 février 2016, En ligne: <https://www.latribune.fr/opinions/tribunes/de-l-influence-du-big-data-sur-les-elections-americaines-553346.html> (dernière consultation: 5 mars 2018), ou encore: D'ALMEIDA Pierre, *Google est-il capable de truquer une élection ?*, Le Figaro, 2 septembre 2015, En ligne: <http://www.lefigaro.fr/secteur/high-tech/2015/09/02/32001-20150902ARTFIG00091-google-est-il-capable-de-truquer-une-election.php> (dernière consultation: 5 mars 2018)

qu'offre le progrès, mais également et surtout leur diffusion, leur accessibilité dans la société. La proposition d'envisager un nouveau concept: la surveillance diffuse s'insère dans ce premier constat. L'emploi du terme « diffuse » dans le cadre de la surveillance représente la caractéristique essentielle de la surveillance contemporaine. Cette notion fait référence à la propagation des nouvelles technologies, mais également aux nouveaux usages permis grâce ou à cause de ces dernières. La diffusion suppose une émission et une réception. Appliqués à la surveillance diffuse, ces deux termes évoquent le fait pour cette dernière de s'être répandue par capillarité (émission) dans chacune de nos activités, en permettant la collecte (réception) de nombreuses informations, données personnelles, et détails sur la vie des individus. La diffusion progressive de la surveillance dans chacune des activités de l'homme a permis ensuite de le placer lui-même dans le champs d'observation de la surveillance; à faire en sorte qu'il « consente », ou du moins, à ce qu'il accepte de donner toujours plus d'informations le concernant (émission facilitée) que le surveillant protéiforme va collecter, traiter, stocker (réception). S'attarder sur ces notions de diffusion, et cette inversion des rôles est importante en ce qu'elles caractérisent le passage d'une société panoptique, où la surveillance s'opère à sens unique comme une discipline s'imposant à l'individu, à, ce que certains auteurs qualifient de société catoptique¹³⁴, où la relation de surveillance est caractérisée par sa réciprocité. Si la vérification de cette dernière hypothèse s'avère délicate, il faut, à tout le moins, conclure à la banalisation de la surveillance du fait même de sa diffusion.

50. On constate également que la surveillance diffuse va bien au delà d'un simple banalisation ou d'un simple phénomène. En 2015, à la suite des révélations d'Edward Snowden, David Lyon définit la surveillance comme « *une attention systématique et routinière des détails personnels, spécifiques ou agrégés, dans un but précis. Ce but, l'intention pratique de la surveillance, peut aller de la protection, à la compréhension, en passant par le fait de prendre soin, d'assurer le droit, de contrôler, de gérer ou d'influencer des individus ou des groupes*¹³⁵ ». Au-delà de cette nouvelle définition, l'ensemble de ce nouvel ouvrage tend à la démonstration de l'émergence d'une culture de la surveillance fondée sur deux éléments antagonistes la liberté d'expression que prône Internet, et la suspicion qu'a engendré le 11 septembre et les pratiques de la NSA mises au jour par Snowden. avec l'ensemble des différents panels de sentiments liés à cela: suspicion, force de séduction. Cette

¹³⁴ En ce sens, voir: GANASCIA Jean-Gabriel, *Voir et pouvoir : qui nous surveille ?*, Editions Le Pommier, Collection Les Essais 2009

¹³⁵ LYON David, *Surveillance after Snowden*, Polity Press, 2015, p. 17. Traduction libre de l'auteur des mots suivants: « *a systematic and routine attention to personal details, whether specific or aggregate, for a defined purpose. That purpose, the intention of the surveillance practice, may be to protect, understand, care for, ensure entitlement, control, manage or influence individuals or groups* ».

réalité d'une culture de la surveillance correspond à ce que nous envisageons sous l'expression de la surveillance diffuse. Elle n'est plus cette pratique coercitive envisagée sur les individus mais bel et bien une culture à laquelle nous avons tous souscrits fortement influencés par les médias, la communication, les leaders du numérique et les politiques sécuritaires menées globalement à l'échelle mondiale.

51. Ces prolégomènes ayant permis de justifier le recours au concept de surveillance diffuse, il est alors utile de comprendre l'objectif de ce travail de recherches. Son but essentiel est de comprendre comment la surveillance diffuse s'intègre dans l'évolution des notions juridiques de vie privée et de données personnelles. A l'inverse de la littérature foisonnante¹³⁶ sur le thème de la surveillance, il ne s'agit pas en effet dans cette thèse de mettre en avant la nécessité de trouver un équilibre entre la surveillance entendue dans sa dimension sécuritaire et la protection de la vie privée et des données personnelles, en ce qu'elle constitue une liberté fondamentale reconnue par les institutions françaises et européennes. Cette recherche d'une balance équilibrée entre sécurité et liberté doit nécessairement être dépassée, et ce, pour plusieurs raisons.

52. Dans un premier temps, l'étude du concept même de surveillance, pousse le juriste à interroger sa nature juridique et sociologique. Le premier problème posé par cette interrogation est qu'il ne semble pas qu'à l'origine la surveillance revête une quelconque connotation juridique. Bien au contraire, cette notion est avant tout un mythe littéraire dont l'idée et le sens général se sont progressivement diffusés dans nos sociétés contemporaines. Cette diffusion a été rendue possible grâce aux nouvelles technologies de l'information et de la communication, progressivement détournées de leur objectif principal (l'information, la communication) pour y préférer des objectifs sécuritaires et économiques. Et c'est dans ce glissement des usages liés aux TIC que réside le second problème de l'étude de la surveillance. Devenant un phénomène de société, un fait social et plus loin un fait juridique, la surveillance diffuse cherche à porter son attention sur l'ensemble des activités humaines, réduisant ainsi les individus à une trace numérique, à un objet d'étude. La surveillance n'est plus la simple activité de recherche de renseignements concernant un individu potentiellement dangereux. Elle s'inscrit plutôt dans la poursuite de ce que Hannah Arendt qualifie de « crise de la culture ». La surveillance diffuse est même l'une des caractéristiques de la culture contemporaine dominée par la peur, la consommation et l'aliénation par les technologies. L'individu

¹³⁶ Qu'elle soit juridique, sociologique, politique et littéraire

placé dans une position de consommateur de sécurité et de technologies ne questionnent plus l'efficacité des mesures technologiques prises par le politique, ni même l'invasion des technologies dans sa vie privée souhaitées par les acteurs privés et publics. Il participe alors à la diffusion de la surveillance dans la société, à sa banalisation, mais également à son institutionnalisation dans nos sociétés. Les conséquences de cette institutionnalisation de la surveillance sont alors palpables en termes de contrôle social muté en attention, de transformation des espaces publics et privés, mais également en terme d'exercice du pouvoir, principalement fondé sur la mise en données du monde, les algorithmes informatiques et l'automatisme du choix technologique.

53. En face de la notion de surveillance se situent les concepts juridiques de vie privée et de données personnelles. Les événements récents (Snowden, Prism, terrorisme) forcent la doctrine et les organisations protectrices des libertés à alerter l'opinion publique quant aux dérives sécuritaires, au soft totalitarisme engendré par la surveillance, à la perte progressive de sens des notions d'Etat de Droit et de démocratie. Bien que ces éléments soient parfaitement représentatif de la situation actuelle, ils n'en relèvent pas moins d'une simple prise en considération d'une balance à trouver entre sécurité et liberté. Or, l'étude de la notion même de surveillance démontre qu'elle n'est pas uniquement le propre de la sécurité, d'un droit à la sécurité. Elle est à la fois attention bienveillante contre le terrorisme, mais également contre les maladies, le nombre de calories ingérées dans une journée, le nombre de cigarettes fumées. Ainsi, réduire la problématique de la surveillance à cette recherche d'équilibre entre la sécurité et la liberté relève d'un non-sens. La confrontation de la surveillance diffuse aux concepts juridiques de données personnelles et de vie privée force le juriste à s'interroger, dans un second temps, sur le carburant essentiel de la surveillance. D'aucuns évoquent le fait que la donnée personnelle serait un nouvel or noir. Cette assertion est fautive. La surveillance, en tant que principal moyen d'exercice d'un contrôle social attentionnel et d'un pouvoir algorithmique, engendre principalement traitement d'informations non personnelles.

54. Or, les législations informatique et libertés, qu'il s'agisse de la loi française de 1978, de la directive de 1995¹³⁷, mais aussi des Safe harbor, n'envisagent que le simple traitement de données personnelles, et méconnaissent par là les enjeux de la surveillance diffuse. En réalité, c'est souvent par un truchement technologique, ou par interconnexion de bases de données, que l'information va

¹³⁷ 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*, Journal officiel n° L 281 du 23 novembre 1995, p. 0031 - 0050, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046> (dernière consultation: 5 mars 2018)

revêtir à nouveau son caractère personnel. De là, la question de savoir si le juriste doit se saisir de l'entier processus, ou comme l'indique la loi, uniquement du traitement de données à caractère personnel, doit être posée. L'étude des jurisprudences européennes à ce propos, qu'il s'agisse des données de connexion, de trafic ou encore des métadonnées, et de leurs traitements, contribuent à brouiller, dans l'esprit du juriste, la détermination du champ d'application de la loi. Manque d'adéquation des principes fondamentaux de la protection des données personnelles, conception des données personnelles par référence à la notion de vie privée en perte d'efficacité contre l'idéologie sécuritaire, mise en cause des Safe Harbor, sont autant d'éléments qui poussent à conclure à une intégration de la surveillance facilitée par la loi.

55. Aussi, l'évolution récente des notions juridiques de vie privée et de données personnelles, qu'elle soit envisagée sous l'angle des nouvelles législations européennes ou internationales, ne règle pas cette question. Au contraire, l'analyse des textes tendent à démontrer une intégration parfaite de la surveillance diffuse dans l'évolution de ces notions. Dans les faits, la réduction du droit des données personnelles au simple consentement de la personne dont la donnée est traitée participe d'une méconnaissance pleine et entière des effets de la surveillance sur la vie privée. L'ensemble des législations récentes sur ce point, qu'il s'agisse du règlement européen sur la protection des données personnelles, du Privacy Shield, ou de la réglementation à venir sur la libre circulation des données non personnelles, participent de la finalisation de la création du marché du numérique. Et c'est dans la réduction du droit des données personnelles, et, plus loin, de la vie privée, à un Droit libéral - entendu dans son acception économique - que le législateur désinstitutionnalise la place du droit des données personnelles, de la protection de la vie privée et, plus généralement, du Droit au profit de l'institutionnalisation de la surveillance dans nos sociétés.

56. Reste alors à comprendre les effets de cette désinstitution du Droit au profit de la norme qu'est devenue la surveillance diffuse. Il faut alors questionner d'une part la modification même du sens de la liberté par cette nouvelle norme sociale. Car, ainsi que le rappelle, Dominique Quessada, *« ce qui définit la surveillance contemporaine globale, c'est de ne pouvoir être séparée des procédures quotidiennes par lesquelles nous travaillons, consommons, communiquons, nous déplaçons : « Plus on voyage ou on achète (...), plus s'amassent les volumes de données évaluables. La plus grande liberté est la condition paradoxale et contemporaine de la plus grande surveillance » . La surveillance contemporaine établit une stricte équivalence entre vivre et être surveillé. Vivre,*

c'est désormais être surveillé globalement sans rupture par les rets de plus en plus affinés et allant toujours s'étrécissant d'un maillage électronique invisible et omniprésent¹³⁸ ».

57. La description de l'ensemble de ces phénomènes sera envisagée sous l'angle de l'intégration de la surveillance diffuse dans le Droit. Cette dernière semble modérée sous l'empire des premières législations informatique et libertés, en ce compris, la directive de 1995 et la loi française de 1978¹³⁹ du fait d'un déficit de conscience des enjeux de la surveillance diffuse, mais également d'un déficit d'effectivité de ces premières législations (Partie 1). A la lecture des nouveaux instruments européens, il apparaît que la surveillance diffuse s'intègre parfaitement au droit des données personnelles et à la vie privée (Partie 2). Si cette formulation peut laisser présumer d'un renforcement des droits et libertés des individus, il n'en est rien en réalité. La surveillance diffuse est pleinement intégrée aujourd'hui du fait de la reconnaissance de ces deux objectifs principaux au travers du Droit: la sécurité et l'économie fondée sur la donnée.

¹³⁸ QUESSADA Dominique, *De la sousveillance - La surveillance globale, un nouveau mode de gouvernamentalité*, Multitudes, 2010/1 n°40, p55

¹³⁹ Loi du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004, En ligne: https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive-annotee.pdf (dernière consultation: 5 mars 2018)

Partie 1 : Une intégration de la surveillance diffuse modérée sous l'empire de la loi de 1978 et de la directive de 1995

58. Sans qu'il soit nécessaire de recourir à une archéologie du concept de surveillance qui pourrait nous faire remonter à Argos Panoptès, l'un des événements déclencheur de la prise en considération contemporaine d'une mise en place d'une surveillance des individus a été le 11 septembre 2001, la menace terroriste mais également, un sentiment global d'insécurité. A cette date, des notions a-juridiques ont eu une nouvelle résonance : risque¹⁴⁰, danger¹⁴¹, prévention, suspicion et sécurité ont progressivement fait leur apparition dans les discours des différents gouvernements, et, dans la mobilisation internationale contre le terrorisme. *« Avec le 11 septembre, la logique fondée sur l'argument du « scénario du pire » (worst case scenario) a gagné beaucoup de crédit auprès des gouvernements et des médias: on ne peut pas attendre le prochain attentat, car il sera tellement dévastateur que la conception du policier comme « pompier du crime » - c'est à dire la vieille image de la police criminelle – ne peut suffire. On assiste ainsi à une dévalorisation profonde de la logique policière en tant que justice criminelle au profit de la proactivité ou de la prévention. Une prévention non pas au sens d'éliminer les facteurs structurels encourageant à la violence, mais au sens d'« agir avant que l'autre n'agisse ». Autrement dit une logique de guerre, dans laquelle la suspicion et l'urgence constituent des pièces centrales. Le danger étant toujours présenté comme imminent, on observe également une coalescence de figures de la menace, allant de la « bombe atomique dans le sac à dos d'un fanatique religieux », image canonisée du « scénario du pire », jusqu'au migrant et au réfugié¹⁴² » .*

59. Les événements du 11 septembre 2001 n'ont pas nécessairement joué le rôle de déclencheur de l'apparition de la surveillance diffuse. Ils ont, au mieux, permis de changer la perception de certaines logiques discursives, politiques, économiques, en relation avec la surveillance, et plus

¹⁴⁰ Sur cette notion, voir le livre d'Ulrich Beck, *La Société du Risque – Sur la voie d'une autre modernité*, Collection Champs, Éditions Flammarion, 2001

¹⁴¹ En tant que juriste, il est nécessaire de préciser ici que la dangerosité ne doit pas être considérée comme une notion juridique. Elle est une notion criminologique, pérenne. Cette vision est d'ailleurs partagée par Jean Danet : *« La dangerosité n'est pas un concept juridique. Ni l'origine de la notion, ni son histoire, ni ses définitions ne peuvent la rattacher au droit pénal. C'est bien une notion criminologique (...) et un opérateur externe au droit »*. in, *La dangerosité, une notion criminologique, séculaire et mutante*, DANET Jean, *La dangerosité, une notion criminologique, séculaire et mutante*, in. Champ pénal/ Penal field, Vol. V, 2008, mis en ligne le 11 juin 2008, En ligne: <http://champpenal.revues.org/6013> (dernière consultation: 5 mars 2018)

¹⁴² BIGO Didier, BONELLI Laurent et DELTOMBE Thomas (sous la direction de), *Au nom du 11 septembre ... Les démocraties à l'épreuve de l'antiterrorisme*, éditions La découverte, 2008, p. 6

globalement avec la notion de sécurité. Le monde étant devenu dangereux, il fallait agir. La surveillance permettrait alors d'appréhender les risques, les dangers, de rendre ce monde un peu moins « imprévisible », de rendre la société un peu moins vulnérable. Ainsi que l'analyse Didier Bigo, dans son ouvrage « *Au nom du 11 septembre ... Les démocraties à l'épreuve de l'antiterrorisme* », il est nécessaire de « *relativiser la supposée « nouveauté » des préoccupations antiterroristes (les continuités l'emportent souvent), tout en pointant l'effet d'aubaine qu'a parfois pu constituer la mobilisation internationale contre le terrorisme pour durcir les lois nationales et rogner sur les tolérances – notamment politiques – induites par une conception ouverte des libertés publiques*¹⁴³ ». Les notions a-juridiques précitées (risque, danger, prévention, sécurité) ont progressivement fait leur entrée dans le droit des différents États¹⁴⁴, et ont par voie de conséquence permis de durcir les droits nationaux, tout en faisant reculer petit à petit les « tolérances » liées aux libertés publiques.

60. Évoquer le processus d'apparition de la surveillance diffuse, déconstruire ce phénomène peut apparaître de prime abord comme un travail a-juridique (Titre 1). Pourtant, il est nécessaire de comprendre ce phénomène et de garder en tête son histoire et son lien avec le phénomène technique. La confrontation de la surveillance diffuse aux notions juridiques de vie privée et de données personnelles telles que définies par les premières législations informatiques et libertés est également nécessaire (Titre 2). Si la surveillance diffuse s'intègre pleinement dans nos sociétés, ces premières législations donnent le sentiment d'une intégration délicate d'un point de vue juridique de la surveillance diffuse.

¹⁴³ Ibid. p. 8

¹⁴⁴ A titre d'exemple, le législateur français a affirmé à trois reprises l'expression : « *la sécurité est un droit fondamental* » : article 1^{er} alinéa 1^{er} des lois du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, du 15 novembre 2001 relative à la sécurité quotidienne, et du 18 mars 2003 pour la sécurité intérieure.

Titre 1: L'institutionnalisation progressive de la surveillance diffuse: naissance et développement d'un phénomène de société

61. « Arrive une troupe d'enfants : aussitôt les voilà courants après ce papillon dont ils ont tous envie. Chapeaux, mouchoirs, bonnets servent à l'attraper ; l'insecte vainement cherche à leur échapper. Il devient bientôt leur conquête. L'un le saisit par l'aile, un autre par le corps ; un troisième survient, et le prend par la tête : il ne fallait pas tant d'efforts pour déchirer la pauvre bête. Oh ! Oh ! Dit le grillon, je ne suis plus fâché ; il en coûte trop cher pour briller dans le monde, combien je vais aimer ma retraite profonde ! Pour vivre heureux, vivons cachés¹⁴⁵ ». Alors qu'il y a encore 10 ans¹⁴⁶ cette citation de Florian était ancrée dans nos sociétés, aujourd'hui l'explosion des réseaux sociaux, de l'usage d'internet comme outil de connaissance et de communication, plus globalement, l'informatique et les nouvelles technologies ont fait en sorte que l'individu exhibe l'ensemble des aspects de sa vie quotidienne et privée en ligne.

62. En 2007, Jean Malaurie déclarait que nous étions entrés « dans une civilisation technique si puissamment dominée par les sciences dures aux remarquables avancées certes mais si peu maîtrisées, qu'avant peu, nous serons nous hommes, numérisés, sans repères spirituels et culturels¹⁴⁷ ». Ces repères culturels que sont la vie privée et l'intimité¹⁴⁸ ont été remplacés par l'exhibitionnisme et le dévoilement de soi. L'individu est devenu à la fois ce papillon et ces enfants souhaitant briller dans le monde par la numérisation de sa vie privée, et par l'étalage des moindres détails de cette dernière sur internet. Par ailleurs, les États et les entreprises se sont lancés dans la

¹⁴⁵ Extrait de la fable de Jean-Pierre Claris de Florian, *Le Grillon*, II, 2, 1783 disponible en ligne à l'adresse suivante : http://poesie.webnet.fr/lesgrandsclassiques/poemes/jean_pierre_claris_de_florian/le_grillon.html (dernière consultation: 5 mars 2018)

¹⁴⁶ Facebook, par exemple, a été créé en 2004, et a connu son avènement commercial en 2006. Sous couvert de slogans publicitaires évocateurs, les réseaux sociaux, ainsi que l'évoquent Wolfgang Sofsky ou David Lyon, organisent l'exhibition de l'individu, sa mise à nu (par exemple : « Facebook vous permet de rester en contact avec les personnes qui comptent dans votre vie »). Voir également: SOFSKY Wolfgang, *Le citoyen de verre - entre surveillance et exhibition*, Traduit de l'allemand et préfacé par Olivier Mannoni, Editions de l'Herne, Paris, 2011; BENNETT Colin, HAGGERTY Kevin, LYON David, STEEVES Valérie (sous la direction de), *Vivre à nu: la surveillance au Canada - Projet sur la nouvelle transparence*, Athabasca University Press, 2014

¹⁴⁷ MALAURIE Jean, *Terre Mère*, Paris, CNRS éditions, 2008, p. 13 et s. Cette citation, issue d'un discours prononcé à l'UNESCO en 2007, reflète bien les problèmes posés par la société de l'information bouleversée par les nouvelles techniques, maîtrisées ou non, qui s'imposent dans notre société moderne. La technique n'est pas en elle-même remise en cause, mais les difficultés qu'elle génère dans son appropriation par la science, le droit, et plus loin, par l'homme sont de plus en plus palpables. Et, l'homme si tant est qu'il soit réellement « numérique » n'a pas conscience de l'empiétement de la technique sur son environnement et ses libertés. Dans ce contexte, les techniques de surveillance, leur encadrement juridique, et les impacts de ces dernières sur l'individu ne font que confirmer ce propos.

¹⁴⁸ Le principe du respect de la vie privée est inscrit à l'article 9 du Code Civil (loi du 17 juillet 1990) qui déclare : « 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 ».

course au numérique pour des raisons diverses et des enjeux économiques forts. L'informatique, les nouvelles technologies ont évolué, se sont combinés ; de la mémoire toujours plus importante des espaces de stockages, en passant par l'interopérabilité et l'interconnexion des systèmes, aux innovations technologiques (caméra de surveillance, géolocalisation, puces RFID, nanotechnologie), nous sommes devenus identifiables, identifiés, profilés.

63. Étudier la diffusion de la surveillance dans notre société (chapitre 1) est une tâche complexe du fait de la diversité des facteurs de diffusion de ce phénomène, des acteurs et des discours de justification du recours parfois insidieux à la surveillance. Il est toutefois nécessaire de le faire en observant comment est apparu le phénomène de surveillance diffuse ? On constatera alors que les éléments structurels (précités) ne suffisent pas à expliquer l'imprégnation toujours plus importante de la société par la surveillance diffuse. La diffusion de la surveillance, en tant que phénomène sociétal, est apparue dans un contexte d'évolution et d'ambitions créés par le numérique. Ces ambitions et évolutions sont le fruit d'un ensemble d'acteurs qui semblent être, consciemment ou non, au service de la surveillance diffuse. Evoquer ces acteurs multiples (chapitre 2) revient également à s'interroger sur la relation qu'entretient l'individu avec ce milieu social nouveau.

Chapitre 1: La diffusion de la surveillance dans la société numérique

64. Comprendre l'emprise de la surveillance sur la société revient à s'interroger sur le processus d'apparition et d'imprégnation de la société par la surveillance diffuse. La surveillance diffuse est avant tout un phénomène ayant une affiliation forte avec le phénomène technique. Ainsi que le rappelle Stéphane Vial, « *comme toutes les révolutions techniques précédentes, elle [la révolution numérique] est une révolution phénoménologique, c'est-à-dire une révolution de la perception : elle ébranle nos habitudes perceptives de la matière et, corrélativement, l'idée même que nous nous faisons de la réalité*¹⁴⁹ ».

65. Avant toute tentative de définition potentielle de la surveillance diffuse, il apparaît nécessaire d'adopter une approche phénoménologique de cette dernière (section 1). On constatera alors que les études concernant le phénomène de surveillance sont principalement partagées entre deux courants de pensées: la technophobie et la technophilie. Limiter une étude globale de la surveillance à ces deux courants de pensées serait restrictif, il faudra alors comprendre les stratégies discursives qu'elles utilisent pour clarifier l'analyse, en préférant une approche pragmatique et démythifiée de la diffusion de la surveillance (section 2).

Section 1: Approche phénoménologique de la surveillance diffuse : un phénomène issu du phénomène technique

66. Dans son acception commune, la surveillance n'est pas un champ de recherche nouveau. Toutefois, la diffusion toujours plus importante de cette notion dans la société contemporaine est un objet de réflexion nouveau en prises directes avec la sociologie, la philosophie, le politique et le droit. L'analyse de la diffusion mondiale de la surveillance en témoigne (paragraphe 1). L'adoption d'une approche phénoménologique dans le cadre d'une étude juridique peut sembler paradoxale. Les études juridiques se veulent empiriques. La démarche empirique s'appuie sur l'analyse d'un sujet qui raisonne sur son objet de recherche. Dans ce cadre, un premier filtre réflexif est déjà posé sur l'objet de la réflexion. Les sociologues, les historiens, les philosophes, les juristes ont évoqué

¹⁴⁹ VIAL Stéphane, *L'être et l'écran – Comment le numérique change la perception*, préface de Pierre Lévy, PUF, Paris, 2013, p. 97. Stéphane Vial est un philosophe et un enseignant-chercheur français spécialisé dans l'approche philosophique du design et des technologies numériques. Docteur en philosophie, il est maître de conférence en design à l'université de Nîmes.

cette notion à plusieurs reprises¹⁵⁰. Des filtres d'analyses ont donc déjà été posés sur cette dernière. Un imaginaire entoure même ce concept du fait de sa relative connotation fictionnelle. Il faut alors comprendre ce concept, le déconstruire, et le concevoir comme un phénomène de société, mais également un phénomène technique (paragraphe 2).

Paragraphe 1: Analyse de la diffusion mondiale de la surveillance: entre phénomène social et phénomène juridique

67. La diffusion de la surveillance dans nos sociétés doit être comprise pour ce qu'elle est vraiment. Elle est en premier lieu un phénomène social et sociologique (A). Par l'émergence des lois relatives à la protection de l'informatique et des libertés, elle est devenue progressivement un phénomène juridique (B).

A. La diffusion de la surveillance dans les sociétés contemporaines

68. La diffusion de la surveillance est d'abord un fait social. Elle ne suit pas un plan linéaire, et ne va pas du simple au complexe mais à l'inverse: du complexe - par l'éclosion de la surveillance de manière éparse - , au simple: le phénomène de surveillance diffuse. Ainsi que le rappelle Gabriel Tarde, dans son livre intitulé *les lois de l'imitation*, il faut toujours considérer dans l'analyse d'un fait social, que l'hétérogène est antérieur à l'homogène¹⁵¹. L'étude du phénomène de surveillance diffuse passe alors dans un premier temps par l'évocation de quelques repères historiques agrémentés de la littérature du Parlement européen (1). Ce bref point historique permettra la mise en lumière, dans un second temps, de la filiation de la surveillance au phénomène technique, entendu comme étant tout ce que nos sociétés industrielles ont englobé sous la notion de progrès technologique et de ce qu'il engendre (2).

¹⁵⁰ Notamment: Jacques Ellul, Martin Heidegger, Gilles Deleuze, Michel Foucault, Hannah Arendt, Kant, Max Weber, ou encore plus récemment : Lucien Sfez, Jean-Claude Guillebaud, Dominique Bourg, Serge Latouche, Patrick Chastenet, L'Encyclopédie des Nuisances, Peter Sloterdijk, Jean-Luc Porquet.

¹⁵¹ « La loi de différenciation intervient donc ici. Mais il n'est pas inutile de faire remarquer que l'homogène sur lequel elle s'exerce, sous trois formes superposées, est un homogène superficiel, quoique réel, et que notre point de vue sociologique nous conduirait, par le prolongement de l'analogie, à admettre dans le protoplasme des éléments aux physionomies très individuelles sous leur masque uniforme, et dans l'éther lui-même, des atomes aussi caractérisés individuellement que peuvent l'être les enfants de l'école la mieux disciplinée. L'hétérogène et non l'homogène est au cœur des choses. Quoi de plus invraisemblable, ou de plus absurde, que la coexistence d'éléments innombrables nés co-éternellement similaires ? On ne naît pas, on devient semblables. Et d'ailleurs la diversité innée des éléments, n'est-ce pas la seule justification possible de leur altérité ? ». in, TARDE Gabriel, *Les lois de l'imitation – Étude sociologique*, 7ème édition, Paris, Librairie Félix Alcan, 1921, p. 77 - 78

1. De quelques repères historiques nécessaires: la surveillance ou l'informatisation progressive de l'activité de renseignements

69. L'idée d'une surveillance technicisée, informatisée, s'est lentement instillée dans nos sociétés. Fortement liée à l'activité de renseignements des Etats, la surveillance permet d'obtenir des informations à l'encontre d'une catégorie de population, présentée comme à risque, mais également de combattre un ennemi en temps de guerre, ou de profiter d'un avantage concurrentiel dans le domaine économique. Ainsi que l'écrit Thomas Bausardo, « *le renseignement a toujours été une donnée fondamentale de l'art de gouverner. Depuis l'institutionnalisation et la bureaucratisation de véritables administrations du et de renseignement au sein des Etats tout au long du XIXe siècle, il est une des caractéristiques fondamentales de la modernité politique*¹⁵² ».

70. L'informatisation de l'activité de renseignement trouve son origine dans la coopération entre la US Navy des Etats-Unis et le Government and Cypher School de l'Angleterre pendant la Seconde Guerre Mondiale¹⁵³. Le 17 mai 1943, les Etats-Unis et l'Angleterre encadrent cette activité en signant un accord de coopération : le *British-U.S. Communications Intelligence Agreement*¹⁵⁴ (BRUSA). Avec la guerre froide, les préoccupations concernant le renseignement en temps de guerre glissent vers une course à l'obtention et à l'accès aux informations économiques, à l'intelligence économique¹⁵⁵. C'est dans ce cadre que le traité UKUSA¹⁵⁶ (*United Kingdom –*

¹⁵² BAUSARDO Thomas, « Quel passé pour Prism et Snowden ? », *Vacarme* 2014/1 (n°66), p. 142 - 157, p. 145, En ligne: <https://www.cairn.info/revue-vacarme-2014-1-page-142.htm> (dernière consultation: 5 mars 2018)

¹⁵³ De cette collaboration, on retiendra particulièrement le déchiffrement par Alan Turing du code employé dans le cadre des messages allemands transmis via ENIGMA, une machine électromagnétique portable servant au chiffrement et déchiffrement d'informations.

¹⁵⁴ The British-U.S. Communications Intelligence Agreement (BRUSA), 17 Mai 1943, En ligne: <http://discovery.nationalarchives.gov.uk/details/r/C11536914> (dernière consultation: 5 mars 2018). Ce traité permettait l'obtention et l'accès à des informations et des renseignements dont les sources étaient des signaux électromagnétiques.

¹⁵⁵ La notion anglaise de « *communications intelligence* » contenu dans les intitulés des accords BRUSA et UKUSA va plus loin que la seule intelligence économique. En effet, l'Agence de Sécurité Nationale Américaine (NSA) vient définir cette notion comme étant « *une activité industrielle permettant la recherche et l'interception globale de toutes communications (électroniques) étrangères* ». Cette définition est contenue dans un document top secret déclassifié en 2015 et intitulé : *National Security Council Intelligence – Directive n°6 – Signals Intelligence*, et datant du 17 février 1972, p. 1-2, En ligne: <https://fas.org/irp/offdocs/nsCID-6.pdf> (dernière consultation: 5 mars 2018). Pour autant, il a bien été démontré que suite à la guerre froide, l'intérêt majeur des États-Unis à poursuivre sa recherche électronique de communications était d'obtenir un avantage concurrentiel important, voire une position quasi dominante sur le marché économique. Pour une étude plus poussée de cette affirmation, voir : CAMPBELL Duncan, *Development of surveillance technology and risk of abuse of economic information – Part. 2/5 : The state of the art in communications Intelligence (COMINT) of automated processing for Intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition*, Working Document for the STOA Panel, Luxembourg, Octobre 1999, et spécialement p. 17 – 18.

¹⁵⁶ The United Kingdom – United States Communications Intelligence Agreement (UKUSA), 5 Mars 1946, En ligne: <http://discovery.nationalarchives.gov.uk/details/r/C11536921> (dernière consultation: 5 mars 2018)

United States Communications Intelligence Agreement) voit le jour en 1951. Ce nouvel accord permet d'étendre la liste des pays signataires¹⁵⁷ et d'envisager une surveillance technicisée. Cet accord envisage en effet le passage de l'obtention de renseignements d'origine électromagnétique à la possibilité d'obtenir des informations et des renseignements dont les sources proviennent de toutes formes de communications. En réalité, ces deux accords ont permis de jeter les premières bases du réseau Echelon, le système global d'interceptions des communications privées et publiques révélé par Duncan Campbell en 1988¹⁵⁸. Avec l'élargissement progressif des acteurs du réseau d'interception Échelon, l'intérêt pour le renseignement, et plus particulièrement pour la surveillance technicisée ne cesse de s'accroître. Les dépenses en recherche et développement des différents pays membres du UKUSA¹⁵⁹, puis plus globalement de l'ensemble des pays occidentaux et des entreprises augmentent de manière exponentielle en matière de technologies, d'innovations et de progrès techniques. Interception et recherches automatisées de communications électroniques, amélioration des communications (course à l'espace et lancement des premiers satellites de communications), création de l'ARPANET qui évoluera quelques années plus tard en phénomène Internet, intelligence économique sont autant de nouvelles utilisations et de nouveaux usages technologiques permis par la production d'équipements toujours plus sophistiqués.

71. La technicisation de l'activité de renseignement, puis de la police et de la surveillance a été relevée très tôt par le Parlement européen. Le 6 janvier 1998, son bureau d'évaluation des options techniques - Scientific and Technological Options Assessment (STOA)¹⁶⁰ - a publié un rapport

¹⁵⁷ L'Australie, la Nouvelle-Zélande et le Canada sont considérés comme des pays partenaires au Pacte UKUSA. Cet accord a d'ailleurs été rendu public en 2010 et est disponible dans les archives nationales anglaises, En ligne: <http://www.nationalarchives.gov.uk/ukusa/> (dernière consultation: 5 mars 2018).

¹⁵⁸ CAMPBELL Duncan, *Somebody's listening – They've got it taped*, The New Statesman, 12 août 1988, p. 10 – 12, En ligne: <http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf> (dernière consultation: 5 mars 2018)

¹⁵⁹ Une étude écrite par Duncan Campbell en 1999 pour le S.T.O.A. démontre que depuis les prémices de l'interception de communications électroniques, les moyens d'intercepter les communications ont considérablement évolué, allant jusqu'à employer pour la première fois le concept de surveillance de masse. Cette amélioration des systèmes d'interceptions de communication est due aux dépenses en recherche et développement : 15 à 20 milliards d'euros dépensés par les pays anglo-saxon du traité UKUSA chaque année. CAMPBELL Duncan, *Development of surveillance technology and risk of abuse of economic information – Part. 2/5 : The state of the art in communications Intelligence (COMINT) of automated processing for Intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition*, Working Document for the STOA Panel, Luxembourg, Octobre 1999, et spécialement p. 6.

¹⁶⁰ Le S.T.O.A. est un service de la direction générale des recherches du Parlement européen chargé de mener, sous la direction d'un groupe de députés européens, des études sur les aspects techniques et scientifiques des politiques communautaires.

d'évaluation des technologies de contrôles politiques¹⁶¹. Ce rapport s'intéressait particulièrement au rôle et aux fonctions des technologies de contrôle politique, incluant dans sa grille d'analyse les innovations et tendances récentes¹⁶², ainsi que l'évolution des technologies de surveillance¹⁶³. Les premières pages de ce rapport sont particulièrement éclairantes quant au développement de la surveillance technicisée. Les auteurs s'inquiètent ainsi de « *la prolifération rapide et pratiquement incontrôlée des dispositifs de surveillance et de ses fonctions tant pour le secteur privé que le secteur public*¹⁶⁴ ».

72. Plus que les simples dispositifs de surveillance, l'Union européenne recommande de soumettre « *toutes les technologies, opérations et pratiques de surveillance à: (i) des procédures garantissant la responsabilité démocratique; (ii) des codes de bonne pratique conformes à la législation sur la protection des données personnelles afin de prévenir des abus ou des erreurs délibérées; (iii) des critères convenus sur ce qui constitue des cibles de surveillance légitimes, et ce qui ne l'est pas, et comment ces données de surveillances sont stockées, traitées et partagées*¹⁶⁵ ». Ces qualificatifs liés à la surveillance - technologiques, opérationnels et pratiques - sont importants pour la bonne compréhension du concept de surveillance, et attestent de l'intérêt d'analyser la notion de technique, telle qu'entendue par Jacques Ellul et Martin Heidegger. Bien que la surveillance représente une opération, ainsi qu'une pratique, elle est aujourd'hui fortement liée à la technique, à la technologie, et plus globalement au progrès.

2. La filiation de la surveillance au phénomène technique

73. A l'occasion de son rapport de 1998¹⁶⁶, le bureau d'évaluation des options techniques du Parlement européen a souhaité définir les concepts opérants, et spécialement la notion même de technologies. Selon ce dernier, « *le concept de technologies recouvre des interprétations diverses et*

¹⁶¹ WRIGHT Steve, *An appraisal of technologies of political control*, S.T.O.A., Working document, PE 166.499, 6 Janvier 1998, En ligne: <http://aei.pitt.edu/5538/1/5538.pdf> (dernière consultation: 5 mars 2018)

¹⁶² Notamment au regard de la globalisation, de la militarisation des équipements de police, de la convergence des systèmes de contrôle déployés au niveau mondial, des dérives possibles.

¹⁶³ Incluant les nouvelles formes d'interceptions de communications au niveau local, national et international, ainsi que la création d'outils de reconnaissance et de traçage humain. Ce rapport s'intéressait également aux innovations liées au contrôle des foules, l'émergence des prisons gérées de manière privatisées, l'utilisation de la science et des technologies à des fins d'amélioration des modes d'interrogatoires de prisonniers et de tortures.

¹⁶⁴ WRIGHT Steve, Op. Cit., p. 3

¹⁶⁵ Ibid.

¹⁶⁶ Ibid.

variées. (...). La définition adoptée, pour la bonne conduite de ce travail, englobe non seulement « le hardware » (...); mais également les standards et procédures d'exploitations associés, les programmes, les compétences et les techniques (le software ou la partie logicielle) ; ainsi que toutes formes connexes d'organisations sociales et humaines rationalisées, les systèmes et les réseaux (le liveware) de n'importe quel programme de contrôle politique. En d'autres termes, il ne suffit pas de décrire le progrès dans un sens purement technique, il est aussi nécessaire de considérer ces technologies comme des facteurs sociaux et politiques¹⁶⁷ ». Ainsi que le démontre cette définition du Parlement européen, la technologie ne peut pas se limiter à une simple conception limitée d'appareils, d'instruments informatiques et de systèmes informatisés. Elle doit plutôt s'entendre comme tout ce qui a été permis par les avancées de la science et les innovations de la recherche dans un temps donné et dans une société donnée. En cela, cette définition impose un regard analytique du concept de technique, entendu comme étant tout ce que nos sociétés industrielles ont envisagé sous la notion de progrès technologique et de ce qu'il engendre. Connectées à la surveillance contemporaine, cette définition de la technologie et l'analyse du phénomène technique permettront de comprendre pourquoi et comment elle a pu connaître une diffusion aussi importante dans nos sociétés.

74. La critique de cette notion s'est d'abord développée avec la révolution industrielle à l'encontre du développement de l'urbanisation, de l'industrialisation croissante permise par le machinisme, des progrès de la Science, de l'hypertrophie de l'appareil d'État, et de son pendant : la bureaucratie¹⁶⁸. Des principaux penseurs de la technique moderne et du progrès¹⁶⁹, les ouvrages

¹⁶⁷ WRIGHT Steve, *Op. Cit.*, p. 1

¹⁶⁸ Les premières protestations contre la technique, et spécialement contre la généralisation de l'utilisation des machines dans l'industrie textile, eurent lieu en Angleterre avec le mouvement des Luddites en 1811 - 1817. Pour comprendre ce mouvement : BOURDEAU Vincent, JARRIGE François, VINCENT Julien, *Le passé d'une désillusion : les luddites et la critique de la machine*, Actuel Marx 1/2006 (n° 39) , p. 145-165, En ligne: <http://www.cairn.info/revue-actuel-marx-2006-1-page-145.htm> (dernière consultation: 5 mars 2018), ou encore : SALE Kirkpatrick, *La révolte luddite – Briseurs de machines à l'ère de l'industrialisation*, Traduit de l'anglais par Célia Izoard, Editions L'échappée, Collection Dans le feu de l'action, 2006. C'est seulement quelques années plus tard que des oeuvres littéraires et intellectuelles critiquant ce sujet vont se multiplier. Voir en ce sens THOREAU Henry-David, *Walden ou la vie dans les bois*, Traduction de Louis Fabulet, Éditions Gallimard, Collection L'imaginaire, 1990 (rédigé en 1854 et qui prône un retour à la nature) ; MARX Karl, *Le Capital, critique de l'économie politique*, Presses Universitaires de France, Collection Quadrige Grands Textes, 2009 (publié en 1867 et où Marx évoque l'asservissement des individus que porte en son sein l'industrialisation et le machinisme). On pourrait même évoquer ici la satire du monde industrialisé dépeinte par Charlie Chaplin en 1936 dans sa comédie intitulée Les Temps Modernes. Voir également: WEIL Simone, *Réflexions sur les causes de la liberté et de l'oppression sociale*, Les Éditions Gallimard, Collection Idées, 1955 (Première édition en 1934).

¹⁶⁹ Que sont Bernard Charbonneau, Jacques Ellul, Ivan Illich, Lewis Mumford, Martin Heidegger et ses disciples: Günther Anders et Hannah Arendt.

récents¹⁷⁰ renvoient principalement aux critiques développées par Jacques Ellul¹⁷¹ et par Martin Heidegger¹⁷² ; soit en ne faisant référence à seulement l'un d'entre eux¹⁷³, soit en opérant une mise en opposition de leurs thèses respectives¹⁷⁴. Il faut préciser que les textes fondateurs de ces deux critiques de la technique sont publiés la même année¹⁷⁵, soit en 1954¹⁷⁶. Sans doute, la pensée de Martin Heidegger est-elle complexe et ses commentateurs sont rarement d'accord entre eux. Concernant son analyse de la technique, on pourrait néanmoins retenir que selon lui « *la technique n'est pas la même chose que l'essence de la technique*¹⁷⁷ », et que « *l'essence de la technique n'est absolument rien de technique*¹⁷⁸ ». L'essence de la technique est selon Heidegger l'arrondissement (le *Gestell*) de l'homme par la technique. Pour comprendre cette notion, il faut reprendre l'illustration qu'en donne Heidegger : « *la centrale électrique est mise en place sur le Rhin. Elle le somme de livrer sa pression hydraulique, qui somme à son tour les turbines de tourner. Ce mouvement fait tourner la machine dont le mécanisme produit le courant électrique, pour lequel la centrale régionale et son réseau sont commis aux fins de transmission*¹⁷⁹ ».

¹⁷⁰ Voir par exemple SERIS Jean-Pierre, *La technique*, Presses Universitaires de France, 2000, WEYEMBERGH Maurice, *J. Ellul et M. Heidegger. Le prophète et le penseur*, in. TROUDE-CHASTENET Patrick (sous la direction de.), *Sur Jacques Ellul – un penseur de notre temps*, Éditions L'esprit du temps, Collection Philosophie, 1994, ou encore PORQUET Jean-Luc, *Jacques Ellul – L'homme qui avait (presque) tout prévu*, Editions Recherche Midi, Collection Documents, 2012

¹⁷¹ Voir les trois livres majeurs sur la technique de Jacques Ellul : *La technique ou l'Enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990. *Le Système Technicien*, Calmann-Lévy, 1977 ; réédition, Le Cherche-Midi, 2012. *Le Bluff Technologique*, Hachette, 1988 ; réédition Hachette Littératures, collection « Pluriel », 2004

¹⁷² HEIDEGGER Martin, *Essais et conférences - La question de la technique* ; traduction par André Préau, Éditions Gallimard, Collection Tel, 1988, P. 9-48

¹⁷³ Voir SERIS Jean-Pierre, *Op. Cit.*

¹⁷⁴ Voir PORQUET Jean-Luc, *Op. Cit.*

¹⁷⁵ ELLUL Jacques, *La technique ou l'Enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990 ; HEIDEGGER Martin, *Essais et conférences - La question de la technique* ; traduction par André Préau, Éditions Gallimard, Collection Tel, 1988, P. 9-48

¹⁷⁶ Ainsi que le précise Jean-Luc Porquet, « *entre eux, donc, nulle influence mutuelle. Par la suite, l'un et l'autre se sont regardés en chiens de faïence : Ellul n'aime guère les philosophes, pas plus Heidegger que les autres, à qui il reproche d'agiter des concepts trop éloignés du réel. De son côté, Heidegger n'apprécie guère la démarche d'Ellul, qui d'après lui reste prisonnier du Gestell puisqu'il utilise une méthode sociologique qui relève de la science* ». In. PORQUET Jean-Luc, *Op. Cit.*, p. 317. L'auteur vient résumer plus loin la définition du *Gestell*, notion chère à Martin Heidegger. Jean-Luc Porquet écrit : « *Qu'est ce que le Gestell ? C'est ici que commencent les difficultés. Certains le traduisent par « arrondissement », d'autre préfèrent ne pas traduire le terme. En quoi consiste le Gestell ? Pour l'illustrer, Heidegger prend l'exemple d'une centrale hydroélectrique sur le Rhin et note que le fleuve y est réduit au rôle de réservoir d'énergie qu'on capte, stocke et redistribue. Le Rhin est donc « arraisonné » par la technique. Et cela vaut pour la nature entière, l'homme y compris : elle et lui ne sont plus considérés que comme stock d'énergie, élément d'un circuit, matière première. En heideggerien dans le texte, cela donne quelque chose comme : la technique réduit l'être aux seuls états convocables aux exigences de l'utilitaire... Mais le Gestell est, plus profondément, la force qui fait que l'homme, après avoir longtemps vu la nature comme l'expression d'un mystère, la soumet désormais à l'examen de la raison et de la volonté* » in. PORQUET Jean-Luc, *Op. Cit.*, p. 318.

¹⁷⁷ *Op. Cit.* p. 9

¹⁷⁸ *Ibid.*

¹⁷⁹ *Ibid.* p. 14

75. L'analyse de Jacques Ellul, quant à elle, reconnaît que la modernité de nos sociétés laissent une place prépondérante à la technique¹⁸⁰. Pour situer le phénomène technique, Ellul vient poser quelques repères en le définissant par défaut. La technique ne peut être réduite à la machine, au progrès technologique, ou encore à la science, et même la science appliquée. L'auteur précise ensuite ce qu'il entend par la technique moderne : « *Le phénomène technique est la préoccupation de l'immense majorité des hommes de notre temps de rechercher en toutes choses la méthode absolument la plus efficace. Car on est actuellement passé à la limite dans les deux sens. Ce n'est plus aujourd'hui le moyen relativement le meilleur qui compte, c'est-à-dire comparé à d'autres moyens également en action. Le choix est de moins en moins affaire personnelle entre plusieurs moyens appliqués. Il s'agit en réalité de trouver le moyen supérieur dans l'absolu, c'est-à-dire en se fondant sur le calcul, dans la plupart des cas*¹⁸¹ ». Et d'ajouter, « *nous voyons que cette double intervention dans le monde technique qui produit le phénomène technique peut se résumer comme « la recherche du meilleur moyen dans tous les domaines ». C'est ce « one best way » qui est à proprement parler le moyen technique et c'est l'accumulation de ces moyens qui donne une civilisation technique*¹⁸² ». C'est bien le critère d'efficacité qui est premier dans la définition de la technique. Progressivement ce critère de recherche d'efficacité s'impose à tous, et permet le développement de la technique. Aussi, selon Jacques Ellul, l'essor de la technique peut s'expliquer par la réunion de cinq faits : « *une très longue maturation ou incubation technique, sans à-coups décisifs ; l'accroissement démographique, la situation du milieu économique ; une plasticité presque parfaite de la société, malléable et ouverte à la propagation de la technique ; une intention technique claire qui unit toutes les forces à la poursuite de l'objectif technique*¹⁸³ »

76. Bien qu'il soit possible de comprendre que les thèses de Martin Heidegger et de Jacques Ellul soient souvent mises en opposition dans leur description du phénomène technique, il semble néanmoins qu'il faille réunir leurs analyses. Tous deux se rejoignent, en effet, pour affirmer

¹⁸⁰ Pour preuve l'introduction (p. 1) tirée du chapitre 1, intitulé Techniques, de son livre *la technique ou l'enjeu du siècle* : « *Aucun fait social, humain, spirituel, n'a autant d'importance que le fait technique dans le monde moderne. Aucun domaine, pourtant, n'est plus mal connu* ».

¹⁸¹ ELLUL Jacques, *La technique ou l'enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990, pp.18-19.

¹⁸² Ibid.

¹⁸³ Ibid. p. 55

l'autonomie¹⁸⁴, voire l'auto-accroissement¹⁸⁵ de la technique dans nos sociétés. Ce rapprochement des analyses de Jacques Ellul et de Martin Heidegger sur la notion de la technique ; et spécialement cette conclusion sur leur affirmation respective de l'autonomie et de l'auto-accroissement de cette dernière doit nécessairement être rapportée au phénomène de surveillance diffuse. A la lecture de ces lignes sur le phénomène technique, on constate un retentissement fort sur le concept de surveillance diffuse. La diffusion de la surveillance ne correspond-elle pas aux notions d'autonomie et d'auto-accroissement de la technique décrites par ces deux auteurs ? La surveillance s'est développée de manière totalement autonome, et s'auto-entretient. Aucune action de l'homme n'a été nécessaire pour permettre son utilisation, ou plutôt son recours. Elle est devenue universelle dans son approche, dans son impact et dans ses conséquences¹⁸⁶. La surveillance est, nous dit-on, mise en place pour assurer la prévention, la sécurité et la protection de l'individu. N'est-ce pas là une recherche d'efficacité ? Elle est présentée comme le meilleur moyen pour parvenir à ce but. Un ensemble de discours de légitimation est mis en place pour pérenniser l'ancrage de la surveillance. N'est-ce pas là ce que Jacques Ellul avait envisagé à travers la notion de rationalité¹⁸⁷ ?

77. Enfin, concernant l'unicité de la technique, il est là aussi tout à fait possible d'y voir des interactions avec la surveillance diffuse. A titre d'exemple, Jacques Ellul avait pressenti les effets de la technique sur la logique policière par le perfectionnement des méthodes, et donc par le recours à la surveillance. Il écrivait ainsi que « *la police ne peut avoir sa plénitude technique que si elle est un*

¹⁸⁴ La notion de *Gestell* prônée par Heidegger dans son analyse de la technique n'est rien d'autre que l'affirmation de l'autonomie de cette dernière. Jean-Luc Porquet, dans son ouvrage intitulé *Jacques Ellul – l'homme qui avait (presque) tout prévu*, résume d'ailleurs parfaitement cette affirmation : « *La technique est indissolublement liée au destin de l'homme. Mais son sens originel s'est perdu. Au siècle des Lumières, le Gestell était encore soumis à des fins humaines : la raison technoscientifique ambitionnait d'apporter à l'homme la liberté (en le débarrassant de la superstition et de l'obscurantisme) et le bonheur (en mettant la nature à son service et en se libérant des malédictions que sont les maladies et les catastrophes naturelles). Désormais le Gestell n'a plus de but, et il va son chemin, force aveugle et autonome. (...). L'homme n'a donc plus qu'à reconnaître l'existence de cette force qui va, cette volonté de puissance qui s'exprime, cette « volonté de volonté » inscrite au cœur de la nature* » (PORQUET Jean-Luc, Op. Cit., p 318-319).

¹⁸⁵ L'auto-accroissement est un terme employé par Jacques Ellul dans sa « *caractérologie de la technique* » (chapitre 2 de son ouvrage fondateur intitulé *la technique ou l'enjeu du siècle*, Op. Cit.). Selon Jacques Ellul, les caractères principaux de la technique sont : l'artificialité (la technique s'oppose à la nature), la rationalité qui exclut toute spontanéité et création personnelle, l'universalité et l'automatisme (Ellul démontre, en effet, que puisque l'efficacité (le « *one-best way* ») est le critère prédominant de la technique, ou du moins son effet principal, il n'y a qu'une meilleure technique, c'est la technique la plus efficace), l'insécabilité de la technique, mais aussi et surtout son auto-accroissement.

¹⁸⁶ Les événements récents comme l'affaire Prism ne peuvent que prouver cette affirmation.

¹⁸⁷ Jacques Ellul écrit en effet: « *Cette rationalité qui se voit particulièrement bien dans les faits de rationalisation, de division du travail, de création des standards ou des normes de production, implique en réalité deux mouvements : d'abord l'intervention, dans toute opération, d'un « discours », sous les deux aspects que ce terme peut prendre (d'un côté l'intervention d'une réflexion volontaire, d'un autre côté l'intervention de moyens d'un terme à un autre). (...). L'autre aspect de ce mouvement consiste à réduire ce discours à sa seule dimension logique. Toute intervention de la technique est, en effet, une réduction au schéma logique, des faits, des pulsions, des phénomènes, des moyens, des instruments* » in. ELLUL Jacques, *La technique ou l'enjeu du siècle*, Op. Cit., p. 73.

contrôle total. (...). En réalité l'aspect objectif domine de plus en plus, c'est-à-dire la pure technique, créant un milieu, une atmosphère, un environnement, et même un modèle de comportement dans les relations sociales ; il est sûr que la police doit tendre à la prévention : il faut arriver au point où il sera inutile d'intervenir, ce qui s'obtient de deux façons – d'abord par une surveillance constante (on sait d'avance les intentions nocives ; la police agira donc avant que le mal prémédité soit fait), ensuite par un climat conformiste. Pareil but suppose la surveillance paternelle de tous, mais aussi l'étroite connexion avec toutes les techniques administratives, organisatrices et psychologiques¹⁸⁸ ». Ces mots ne sont-ils pas représentatifs de la situation que connaît notre société, dominée par des programmes de surveillance de masse, par une surveillance quotidienne de nos « intentions nocives » qu'elle soit organisée par l'individu, l'entreprise ou l'Etat, sous couvert d'une recherche de sécurité, de protection et d'efficacité ?

B. La surveillance diffuse: un phénomène juridique en devenir corrélé à l'émergence des législations informatiques et libertés

78. Avec la fin de la guerre froide, et les différents travaux du Parlement européen concernant le réseau Échelon, il aurait été plausible de penser que la diffusion de la surveillance à l'échelle planétaire aurait été mise à mal. Il n'en est pourtant rien. Du réseau Échelon aux révélations de Edward Snowden de juin 2013¹⁸⁹ concernant le nouveau programme de la NSA – PRISM¹⁹⁰ – la surveillance n'a eu de cesse de se propager ; passant de l'activité de renseignements des signaux d'origine électromagnétiques, à l'interception possible de toutes formes de communications numériques. Afin d'analyser au mieux ce décalage entre les années 80 – l'affaire Echelon – et l'implosion de la surveillance dans nos sociétés contemporaines, il est nécessaire de poursuivre l'esquisse chronologique et juridique de ce phénomène. En réalité, il faut nécessairement penser la diffusion de la surveillance en corrélation avec l'émergence des législations informatiques et libertés (1). Les législations informatiques et libertés représentent bien la volonté de moderniser dans les années 1970 l'activité de l'Etat tout en prenant en compte la vie privée des citoyens. Par la reconnaissance d'une protection offerte à toute personne dont les données seraient traitées, le

¹⁸⁸ Ibid. p. 93

¹⁸⁹ C'est en effet dès le début du mois de juin 2013 que des journaux anglo-saxon (et plus particulièrement *The Guardian*, et le *Washington Post*) révèlent que la NSA, via un nouveau programme de renseignements, accède aux données des serveurs des principales entreprises américaines leader de l'Internet. Ces données concernent tout autant des citoyens américains, que des citoyens européens

¹⁹⁰ Cet acronyme signifie : *Planning tool for Ressource Integration, Synchronization and Management*.

législateur a malencontreusement donné une assise juridique à la prolifération technologique et à la surveillance (2).

1. L'émergence des législations informatique et libertés comme facteur de diffusion de la surveillance

79. Parallèlement aux nouveaux usages permis par les technologies et la technique, en ce compris le progrès, l'appareil bureaucratique des États techniciens¹⁹¹ s'est développé¹⁹². Evoquant le principe de libre administration qui désigne la possibilité pour une entité publique ou privée d'adapter ses moyens à ses fins, Nicolas Ochoa écrit qu'il implique « *d'utiliser des moyens humains, financiers et matériels pour l'accomplissement de son idée d'oeuvre. Au titre de ces moyens matériels, se trouve l'informatique. En soi, cet aspect particulier de l'informatique qu'est l'ordinateur ne constitue que l'amélioration et non le point de départ du procédé de traitement rationnel de l'information. Or, la pertinence du traitement de cette information conditionnant l'équilibre interne de l'institution, la rationalisation de cette fonction apparaît comme une condition de la survie même de toute institution. L'histoire des fichiers établis par la puissance publique en France en atteste: ces derniers n'apparaissent de manière systématique qu'au moment où l'Etat développe un savoir sur ses moyens dans le but d'accroître sa puissance sur ses rivaux*¹⁹³ ». Le constat opéré par Ochoa concernant l'utilisation de l'informatique et l'histoire des

¹⁹¹ Voir WEBER Max, *Économie et société – 1. Les catégories de la sociologie*, Traduit de l'allemand par J. Freund (et al.), Éditeur Pocket, Collection Pocket Agora, 1995. Dans cet ouvrage Weber décrit ce qu'il faut entendre par la notion d'État. Selon lui, l'État doit être vu comme une « entreprise institutionnelle ». L'auteur écrit en effet : « *Nous dirons d'un groupement de domination qu'il est un groupement politique [politischer Verband] lorsque et tant que son existence et la validité de ses règlements sont garanties de façon continue à l'intérieur d'un territoire géographique déterminable par l'application et la menace d'une contrainte physique de la part de la direction administrative. Nous entendons par État une « entreprise politique de caractère institutionnel » [politischer Anstaltsbetrieb] lorsque et tant que sa direction administrative revendique avec succès, dans l'application des règlements, le monopole de la contrainte physique légitime* » (Op. Cit. p. 97). La direction administrative de cette entreprise institutionnelle est assurée par la bureaucratie. Dans ce même ouvrage, on peut lire plus loin (Op. Cit. p. 323) : « *La domination légale peut admettre des formes très différentes, (...), la structure la plus purement dominatrice de la direction administrative : celle du « fonctionnariat », de la « bureaucratie »* ».

¹⁹² On pourra citer l'exemple des États-Unis qui, dès les années 50, créent la NASA (National Aeronautics and Space Administration – Agence gouvernementale de l'aéronautique et de l'espace, chargée du programme spatial civil des États-Unis, a été créée en 1958), la NSA (National Security Agency – Agence Nationale de la Sécurité, liée au Département de la Défense américain, a été créée en 1952. Ses principales missions sont d'assurer l'activité de renseignement américain via des sources multiples (renseignements d'origine électromagnétique, traitement de données, sécurité des systèmes d'information)), ou encore la DARPA (Defense Advanced Research Project Agency – Agence pour les projets de recherche avancée de défense, liée au Département de la Défense des États-Unis, a été créée en 1958, et est à l'origine de nombreux de projets de recherche et développement en matière de nouvelles technologies à usage militaire (exemple de l'Arpanet)). Ces autorités publiques ont toutes en commun un intérêt important au développement de l'informatique en termes de recherches et développement, de sécurité, de communications.

¹⁹³ OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Droit. Université Paris 1 Panthéon-Sorbonne, 2014, p. 97. Français. HAL Id: tel-01340600, En ligne: <https://tel.archives-ouvertes.fr/tel-01340600> (dernière consultation: 5 mars 2018)

fichiers en France pourrait trouver application au phénomène de surveillance diffuse. Il faudrait même aller plus loin que la simple crainte liée à l'usage de l'informatique par la puissance publique. Entre l'histoire de l'utilisation des fichiers en France et le phénomène de surveillance diffuse, il y a, en effet, un même dénominateur. L'émergence des législations informatiques et libertés et la volonté du législateur d'offrir une protection à toute personne fichée sont dans les faits à l'origine même de la diffusion de la surveillance. Elles traduisent en effet de l'ambition de la société des années 1970 de s'inscrire dans la révolution de l'informatique.

80. A l'international, les premières craintes liées au développement de l'informatique s'inscrivent dans l'acte final de la Conférence internationale des Droits de l'homme de Téhéran¹⁹⁴ de 1968, qui consacrent une section entière aux droits de l'Homme et aux progrès scientifiques et techniques. Cette section invite expressément le Secrétaire Général des Nations-Unis à mener une étude des problèmes soulevés par le développement de la science et des technologies au regard des Droits de l'Homme, et plus particulièrement du point de vue du respect de la vie privée, des « utilisations de l'électronique qui peuvent affecter les droits de la personne et les limites que devraient comporter ces utilisations dans une société démocratique ; (...) plus généralement, de la balance qui devrait être établie entre, d'une part, le développement technologique et scientifique, et, d'autre part, les progrès de l'humanité d'un point de vue intellectuel, spirituel, culturel et moral¹⁹⁵ ». En 1971, l'Organisation de Coopération et de Développement Économique (OCDE) publie une étude relative à « l'information numérique et la protection des libertés individuelles¹⁹⁶ ». Outre ces exhortations à agir contenues dans les rapports et études d'organisations internationales, c'est aussi dans les années 70 que l'on a pu assister à une première période de tentative de régulation de l'activité informatique sur le plan international, américain, mais également et surtout au niveau européen. Quatre cas d'études doivent être envisagés: les Etats-Unis, la Suède, l'Allemagne et la France. Ces quatre exemples ont en commun la même impulsion: une inquiétude

¹⁹⁴ United Nations, A/CONF.32/41, *Final Act of the International Conference on Human Rights – Teheran, 22 April to 13 May 1968*, United Nations Publication, New York 1968, En ligne: http://legal.un.org/avl/pdf/ha/fatchr/Final_Act_of_TehranConf.pdf (dernière consultation: 5 mars 2018). Sur la question des droits de l'Homme et du progrès scientifique et technique, voir plus précisément p. 12, point 11 de l'acte final précité.

¹⁹⁵ Ibid. p.12. :« Recommends that the organizations of the United Nations family should undertake a study of the problems with respect to human rights arising from developments in science and technology, particularly with regard to : (a) Respect for privacy in view of recording techniques ; (b) Protection of the human personality and its physical and intellectual integrity in view of the progress in biology, medicine and biochemistry ; (c) the uses of electronics which may affect the rights of the person and the limits which should be placed on its uses in a democratic society ; (d) More generally, the balance which should be established between scientific and technological progress and the intellectual, spiritual, cultural and moral advancement of humanity ».

¹⁹⁶ OCDE, *L'information numérique et la protection des libertés individuelles*, Paris, 1971, 76 pages

forte de l'opinion publique et du législateur face aux traitements automatisés de données effectués par l'Etat.

81. Dès les années 70, les Etats-Unis se trouvent confrontés à la problématique de l'informatique et des libertés dans le contexte de l'affaire du Watergate¹⁹⁷ et de jugements rendus contre les fichiers informatisés détenus par des institutions gouvernementales¹⁹⁸. Le 31 décembre 1974, le Congrès des États-Unis adopte le *Privacy Act*¹⁹⁹. Les buts affichés de cette loi sont de protéger la vie privée des citoyens contre l'utilisation abusive de fichiers automatisés fédéraux, de prévoir que les individus soient autorisés à accéder à des dossiers contenant des informations les concernant détenus par les agences fédérales, et d'établir une commission d'étude sur la protection de la vie privée. Les débats introductifs à cette loi devant le Congrès sont d'ailleurs particulièrement éclairant quant à la prise de conscience face à la problématique de l'informatisation de la société, et la protection de la vie privée face aux fichiers et traitements automatisés de l'État. Le sénateur Ervin déclarait alors : « *Si nous avons appris quelque chose de cette année écoulée et du Watergate, c'est qu'il doit y avoir des limites à ce que le gouvernement peut savoir sur chacun de ses citoyens. Chaque fois que nous abandonnons un peu d'informations sur nous-mêmes au gouvernement, nous renonçons à une partie de notre liberté. Plus le gouvernement ou toute institution en connaît sur nous, plus il a de pouvoir sur nous. Lorsque le gouvernement connaît tous nos secrets, nous sommes nus devant tout pouvoir officiel. Dépouillés de notre vie privée, nous perdons nos droits et*

¹⁹⁷ Pour une étude intéressante du sujet, voir le site internet du Washington Post, et spécialement sa page dédiée à l'affaire du Watergate : <http://www.washingtonpost.com/wp-srv/politics/special/watergate/> (dernière consultation: 5 mars 2018)

¹⁹⁸ L'histoire de l'élaboration de la loi sur la vie privée américaine de 1974 ne se limite pas seulement à cette affaire politique. Pour s'en convaincre, voir : The Privacy Protection Study Commission, *The Report of the Privacy Protection Study Commission - Personal Privacy in an information Society*, July 1977, En ligne: <https://www.ncjrs.gov/pdffiles1/Digitization/49602NCJRS.pdf> (dernière consultation: 5 mars 2018), et spécialement ses pages 6 à 13, où la Commission évoque deux arrêts représentatifs du problème de la relation entre les droits des citoyens américains et les fichiers informatisés des institutions gouvernementales (State ex rel. *Tarver v. Smith* 78 Wash. 2d 152, 470 P.2d 172, cert. denied, 402 U.S. 1001 (1971); *United States v. Miller*, 425 U.S. 435 (1976)). Il faut préciser que le *Privacy Act* a un champ d'application assez restreint. Cette loi se limite en effet aux fichiers détenus par les administrations fédérales américaines, et prévoit un droit d'accès pour les citoyens.

¹⁹⁹ *The Privacy Act of 1974*, S.3418, Public Law 93-579, *An act to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.* December 31, 1974 ; version initiale En ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf> (dernière consultation: 5 mars 2018)

privilèges. Le projet de loi qui suit devient alors crucial²⁰⁰ ».

82. L'enjeu des législations informatiques et libertés, telles qu'envisagées dans les années 1970, est donc bien d'offrir un garde fou aux citoyens face à une potentielle surveillance étatique. Plus clairement, ces législations ambitionnent de protéger la vie privée des citoyens face aux usages de l'informatique des Etats et des entreprises. Cette assertion se vérifie également en Europe, qui prend conscience, à la même époque, des risques causés par l'informatisation de la société, les traitements automatisés de données, et la multiplication possible de fichiers informatiques. Ainsi, en Allemagne, et plus particulièrement dans le Land de Hesse, une loi fut adoptée dès 1970 en réaction contre un projet de recensement du gouvernement fédéral²⁰¹. Il faudra attendre 1977 pour que le gouvernement fédéral allemand se dote d'une protection similaire²⁰². A l'identique de la situation du Land de Hesse, la Suède²⁰³ se dotera d'une loi permettant de réguler les traitements automatisés de données le 11 mai 1973²⁰⁴. En France, une première proposition de loi est déposée à l'Assemblée Nationale française en novembre 1970 par le député Michel Poniatowski. Cette dernière tendait à la création d'un comité de surveillance et d'un tribunal de l'informatique²⁰⁵. En 1974, la France

²⁰⁰ Traduction libre de l'auteur : « *If we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words* ». in. U.S. Congress Senate Committee on Government Operations, Legislative history of the Privacy Act of 1974, S.3418, Public Law 93-579, Source Book on Privacy, September 1976, p.4, En ligne: http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf (dernière consultation: 5 mars 2018)

²⁰¹ *Hessische Datenschutzgesetz vom 7 Oktober 1970 GVB1. II 300-10*, (loi sur la protection des données du Land de Hesse, du 7 octobre 1970), publié à Wiesbaden, 12 octobre 1970, Gesetz und Verordnungsblatt für das Land Hessen, Part I, n°41), suivi par le Land de Bavière (par une loi du 12 octobre 1970), et du Land de Baden-Württemberg (par une loi du 12 novembre 1970).

²⁰² *Gesetz zum schutz vor Missbrauch personenbezogener daten bei der datenverarbeitung*, vom 21 Januar 1977, in der Fassung der Bekanntmachung vom 1. Februar 1977 (BGBl. I Nr. 7 S. 201). In Kraft ab 1. Januar 1978. (loi visant à protéger les données personnelles contre l'utilisation abusive de ces dernières dans les traitements de données du 27 janvier 1977, dans la version publiée du 1^{er} février 1977 (BGBl. I n°7, p. 201), en vigueur à partir du 1^{er} janvier 1978), En ligne: https://www.bfdi.bund.de/bfdi_wiki/index.php/BDSG_1977 (dernière consultation: 5 mars 2018).

²⁰³ La loi suédoise a été envisagé à la suite des craintes de l'opinion publique las du recensement de 1969.

²⁰⁴ *Datalag*, 11mai 1973, Svensk författningssamling [SFS] 1973:289

²⁰⁵ Proposition de loi n° 1454 tendant à la création d'un comité de surveillance et d'un tribunal de l'informatique, Michel PONIATOWSKI, distribuée et renvoyée à la commission des lois constitutionnelles, de la législation et de l'Administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement, mentionnée dans le compte rendu intégral de la 69^{ème} séance en Assemblée Nationale, du 25 novembre 1970 (séance 2), En ligne: <http://archives.assemblee-nationale.fr/4/cri/1970-1971-ordinaire/069.pdf> (dernière consultation: 5 mars 2018). Cette proposition de loi ne sera jamais adopté. D'autres propositions de lois ont, pendant les années 70, été dans le même sens que cette constitution d'un tribunal de l'informatique. Et notamment, la proposition de loi n°144 déposée par M. Henri CAILLAVET tendant à créer un directoire et un tribunal de l'informatique (mentionnée dans le compte rendu intégral des séances du sénat, seconde session ordinaire de 1973 – 1974, séance du mardi 2 avril 1974, Débats Parlementaires, Journal officiel de la République Française du mercredi 3 avril 1974, En ligne: http://www.senat.fr/comptes-rendus-seances/5eme/pdf/1974/04/s19740402_0201_0246.pdf (dernière consultation: 5 mars 2018))

découvre le projet SAFARI - Système Automatisé pour les Fichiers Administratifs et Répertoire des Individus²⁰⁶. Certains journaux télévisés de l'époque résument alors le problème posé par SAFARI, et plus largement par l'informatique, de cette manière : « *nous vivons aujourd'hui le temps de l'ordinateur et nos libertés sont aujourd'hui réellement menacés*²⁰⁷ ». Une nouvelle proposition de loi tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens est alors déposée en 1974 à l'Assemblée Nationale par M. Pierre-Bernard Cousté²⁰⁸. Deux ans plus tard, en 1976, un projet de loi relatif à l'informatique et aux libertés est déposé par M. Jean Lecanuet, alors garde des sceaux²⁰⁹.

83. Dans le même temps, le gouvernement français voit en l'informatisation de la société un objectif d'intérêt général. C'est effectivement en 1976 que le Président Valéry Giscard d'Estaing confie à Simon Nora une « *mission d'exploration consistant, d'une part, à faire progresser la réflexion sur les moyens de conduire l'informatisation de la société, et d'autre part, à déterminer avec plus de précision le champ de l'étude et la nature du mandat à confier à une éventuelle Commission*²¹⁰ ». Quarante ans après sa publication le rapport Nora-Minc revêt un caractère quasi

²⁰⁶ Le 21 mars 1974 est publié un article dans les pages justice du journal Le Monde, intitulé *Safari ou la chasse aux Français*, En ligne: http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg (dernière consultation: 5 mars 2018). Les années 70 correspondent, en France, à une véritable mouvance tendant vers la modernisation et la simplification des tâches administratives via l'utilisation des technologies informatiques. Au sein des ministères, de nombreuses initiatives visant à créer des systèmes automatisés d'informations voient alors le jour à cette époque. On citera par exemple: le projet GAMIN tendant à la gestion automatisée de la médecine infantile et devant permettre la sélection automatique d'enfants devant faire l'objet d'une surveillance médico-sociale, le projet SAFARI. Ces deux projets se fondent sur l'identification par numéro unique permettant de centraliser les informations collectées (par exemple le numéro d'inscription au répertoire national d'identification des personnes physiques, le NIR (numéro de sécurité sociale).

²⁰⁷ Propos issus du journal télévisé de 20h00 d'Antenne 2 du 15 juillet 1976 relatif au projet de loi présenté en Conseil des Ministres concernant les libertés et l'informatique par M Lecanuet, propos disponibles en ligne sur le site de l'INA, En ligne: <http://www.ina.fr/video/CAB7600764601/informatique-et-liberte-rossi-video.html> (dernière consultation: 5 mars 2018)

²⁰⁸ Proposition de loi n°1004 tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens, présentée par M. Pierre-Bernard COUSTE, enregistré à la Présidence de l'Assemblée Nationale le 4 avril 1974, annexe au procès-verbal de la séance du 6 juin 1974, Assemblée Nationale, seconde session ordinaire de 1973-1974, En ligne: <https://www.senat.fr/leg/ppl73-1004.pdf> (dernière consultation: 5 mars 2018)

²⁰⁹ Projet de loi n° 2516 relatif à l'informatique et aux libertés, renvoyé à la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République à défaut de constitution d'une Commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement, Présenté au nom de M. Jacques CHIRAC, Premier Ministre, par M. Jean LECANUET, garde des sceaux, Enregistré à la Présidence de l'Assemblée Nationale le 9 août 1976, annexe au procès-verbal de la séance du 2 octobre 1976, Assemblée Nationale, Première session ordinaire de 1976-1977, En ligne: <https://www.senat.fr/leg/pjl76-2516.pdf> (dernière consultation: 5 mars 2018)

²¹⁰ Propos issus de la lettre de mission confiée à Simon Nora. NORA Simon et MINC Alain, *Rapport à Monsieur le Président de la République concernant l'informatisation de la société*, 1978, La documentation française, p. 3, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000252.pdf> (dernière consultation: 5 mars 2018)

prophétique quant à la réalisation d'une ère nouvelle fondée sur l'informatique: la télématique²¹¹. La France des années 70 ne connaissait alors que les prémices des nouvelles technologies. Pourtant, les mots d'Alain Minc et de Simon Nora sont frappants de réalisme. Ces auteurs prévoient l'apparition de nouveaux usages liés à la fusion de l'informatique et des télécommunications²¹², une mise en réseau du monde²¹³, les impacts économiques et la croissance permis par ces nouvelles technologies²¹⁴, les nouveaux jeux de pouvoirs ayant une incidence sur l'indépendance nationale et la souveraineté des États²¹⁵, les relations publiques-privées modifiées par le rôle croissant de l'informatique²¹⁶, l'informatisation de l'administration²¹⁷ ou encore la socialisation de l'information²¹⁸. Bien que le terme même de télématique, cher aux auteurs de ce rapport n'ait pas été retenu, l'ensemble de leurs conclusions semblent quant à elle très prégnantes. Elles s'inscrivent dans la volonté, sans cesse renouvelée, des institutions publiques et privées d'adapter leur organisation et leur structure à l'environnement informatique.

2. L'ambiguïté des législations informatique et libertés: entre protection de la personne fichée et protection d'un marché économique en devenir

84. D'aucuns évoqueront que les prémices de la protection des données à caractère personnel ont été posées à travers les textes législatifs européens précités. Ainsi, par exemple, dès les

²¹¹ Voir en ce sens: Présentation du rapport Nora-Minc sur l'informatisation de la société par Roger Gicquel, suivi d'un reportage consacré à la télématique et ses différentes implications par François de Closets, le 19 mai 1978, TF 1, archive de l'INA, En ligne: <http://www.ina.fr/video/CAA7800628501/informatique-rapport-nora-video.html> (dernière consultation: 5 mars 2018). On relèvera les propos de Roger Gicquel: « *J'ai ici un rapport, un rapport assez redoutable, rapport sur l'informatisation de la société. La télématique, ça s'appelle. Et c'est l'ère nouvelle qui est annoncée dans ce rapport très important et qui a été publié aujourd'hui par Messieurs Simon Nora et Alain Minc, rapport établi à la demande du Président de la République. La télé-matique, qu'est-ce que c'est ?... C'est un peu le triomphe de l'ordinateur. C'est l'informatique orchestrant toute notre vie : pour nous distraire, pour nous faire travailler, pour organiser la sécurité sociale, la Poste, la banque, ... Bref, la révolution de l'ordinateur qu'on croyait derrière nous et qui reste encore à accomplir. (...). Notre vie quotidienne, le marché de l'emploi, la concurrence internationale, les rapports entre les individus, l'organisation de la société. Tout en sera bouleversé. Ce sont des perspectives fascinantes, mais aussi inquiétante ô combien* ».

²¹² Ibid. p. 17 à 30. Ce que les auteurs nomment « *la télématique* ». A la page 11 du rapport précité on peut lire : « *cette imbrication croissante des ordinateurs et des télécommunications – que nous appellerons la « télématique » - ouvre un horizon radicalement neuf. Ce n'est certes pas d'hier que les moyens de communication structurent les communautés : routes, chemin de fer, électricité, autant d'étapes d'une organisation familiale, locale, nationale, multinationale* ».

²¹³ Ibid. et spécialement p. 21 à 30.

²¹⁴ Ibid. p. 31 à 48

²¹⁵ Ibid. p. 49 à 72

²¹⁶ Ibid. p. 73 à 100

²¹⁷ Ibid. p. 101 à 109

²¹⁸ Ibid. p. 119 à 125

premières pages de son ouvrage dédié au Droit de l'Internet²¹⁹, Céline Castets-Renard écrit que « *la protection des données personnelles fut la première préoccupation du législateur français pour canaliser le développement informatique*²²⁰ ». Plus loin, l'auteur écrit « *la France fut l'un des premiers pays à envisager de protéger les individus contre l'utilisation de leurs données à caractère personnel*²²¹ ». Bien que les différents cas d'usages envisagés²²² sont, comme il a été démontré précédemment, tous nés en réaction contre un fichage organisé par l'État sur ses citoyens; il ne faut pas pour autant conclure à l'organisation pleine et entière de la protection des données à caractère personnel. Ces différents exemples témoignent avant tout d'une méfiance forte de l'opinion publique vis-à-vis du traitement automatisé et informatisé de données organisé par l'État. Au delà de la simple activité informatique, c'est l'encadrement du traitement de données personnelles qui est ici envisagé. Sur ce point, l'élaboration des lois informatiques et libertés témoignent d'une ambiguïté réelle, propre à toute ambition de protection d'une activité économique en devenir.

85. A ce stade de l'étude, la bonne compréhension de la notion de « donnée » est cruciale. La lecture attentive des textes de lois précités montre que les différents législateurs européens ou américains opèrent tous par référence à la notion de donnée²²³ ou par référence à la notion d'information²²⁴. Ces termes ne doivent absolument pas être confondus avec les notions de données personnelles ou de données à caractère personnel qui prévalent aujourd'hui dans les différents cadres législatifs nationaux, européens ou encore internationaux²²⁵. Les législateurs nationaux des cas d'usages précités ont inséré ces notions par référence à l'opération technique de traitement automatisé. Les références à ces concepts insérées dans les différentes lois des années 1970 constituent alors l'objet technique du traitement automatisé, et ne conduisent pas à la subjectivisation de la notion de données. A lire les lois précitées, le souhait des législateurs correspondait dans les faits à une volonté de protection de la personne fichée à l'égard du traitement

²¹⁹ CASTETS-RENARD Céline, *Droit de l'Internet*, Montchrestien, Lextenso éditions, Collection Cours, 2010.

²²⁰ Ibid. p. 9

²²¹ Ibid. p. 13

²²² Land de Hesse, Suède, travail législatif français élaborant la future loi informatique et libertés de 1978, et même la Privacy Act américaine

²²³ C'est le cas pour le législateur du Land de Hesse, pour le législateur allemand et suédois.

²²⁴ C'est le cas pour le projet de loi déposé par M. Lecanuet en 1976 à l'Assemblée Nationale. Le Privacy Act opère quant à lui par référence aux deux notions d'informations et de données (« data »)

²²⁵ On notera que les États-Unis ne connaissent pas la notion de données personnelles.

automatisé des données, des informations qui les concernent²²⁶, envisagé par le secteur public et privé. Cette protection s'organisait alors, selon les lois étudiées, par référence à des principes et expressions générales de droit tel que : les intérêts légitimes des personnes concernées²²⁷ et l'absence « *d'atteinte à la vie privée²²⁸ et aux libertés individuelles ou publiques²²⁹* ». On retrouve d'ailleurs cette volonté de protéger la personne fichée à l'égard du traitement automatisé dans la loi française n°78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*²³⁰. La version initiale de cette loi indique clairement que « *toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés²³¹* ».

86. Aussi, à la lumière des objectifs poursuivis dans le cadre du rapport sur l'informatisation de la société rédigé par Simon Nora et Alain Minc, il faut nécessairement conclure à l'ambivalence des buts et objectifs des lois informatique et libertés. Ces lois n'ont certes pas organisé les prémices du droit à la protection des données personnelles c'est-à-dire d'un droit particulier attaché à ces données. Elles ont plutôt envisagé une protection centrée sur l'individu dont les informations seraient traitées automatiquement, par la prise en compte de la méfiance et de la défiance des citoyens de l'époque face à un fichage organisé par l'État. Le rappel, dès l'article 1^{er} de la loi de 1978 précitée d'une absence d'atteinte par l'informatique « *à l'identité humaine, aux droits de l'homme, à la vie privée, aux libertés individuelles ou publiques* » témoigne de cette large volonté

²²⁶ Ces propos ont d'ailleurs été rappelés par M. Michel Gentot, président de la Commission d'accès aux documents administratifs (CADA) de 1989 à 1995 puis de 1998 à 1999, membre (en janvier 1999), puis Président de la Commission Nationale de l'Informatique et des libertés (en février 1999) jusqu'au 7 janvier 2004, date à laquelle M. Alex Türk lui succédera. Michel Gentot écrivait fort justement : « *ces observations expliquent sans doute que le principe d'une protection (improprement dite « des données personnelles » alors qu'il s'agit d'une protection des personnes à l'égard du traitement automatique des données qui les concernent) soit, dans bien des États, consacrés au niveau constitutionnel, plus encore lorsque ces États ont connu des régimes autoritaires* ». GENTOT Michel, *La protection des données personnelles à la croisée des chemins*, in, Académie des Sciences Morales et Politiques (ASMP), Groupe de travail société d'information et vie privée coordonné par M. Pierre Tabatoni, *La protection de la vie privée dans la société d'information*, Tome 3, 1^{er} janvier 2002, En ligne: <http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr1.pdf> (dernière consultation: 5 mars 2018)

²²⁷ Loi du Land de Hesse précitée

²²⁸ Loi fédérale allemande et loi suédoise précitées

²²⁹ L'article 1^{er} du projet de loi déposé par M. Lecanuet précité était ainsi écrit : « *L'informatique doit se développer dans le respect de la vie privée, des libertés individuelles et des libertés publiques* ».

²³⁰ Loi n° 78-17 du 6 Janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, Journal Officiel du 7 Janvier 1978, p.227, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000886460 (dernière consultation: 5 mars 2018)

²³¹ Ibid. article 3.

de protection des citoyens français par le législateur. Ce même article dispose en tant que principe²³² que « *l'informatique doit être au service de chaque citoyen* ». Pour la doctrine, ce préambule témoigne de la prise en compte des craintes concernant l'utilisation de l'informatique. Cette conception est d'ailleurs parfaitement illustrée par les propos du Professeur Jean Frayssinet lorsqu'il commentait ce même préambule en 1989 : « *« L'informatique doit être au service de chaque citoyen » pose l'objectif (et le principe) fondamental ; la formule condense toute la problématique : de l'homme ou de l'ordinateur, lequel doit être subordonné à l'autre ?²³³* ». On comprend par ces mots une partie de l'ambiguïté des lois informatiques et libertés. Toutefois, si l'on poursuit l'analyse des principes issus de l'article 1er de la version initiale de la loi de 1978, on peut également lire que le développement de l'informatique « *doit s'opérer dans le cadre d'une coopération internationale²³⁴* ». Ainsi donc, les lois informatique et libertés portent en leur sein un double objectif qui semble être aux antipodes l'un de l'autre. D'une part, la protection des libertés individuelles des citoyens face à une subordination possible de ces derniers à l'informatique et aux procédés techniques par la reconnaissance de droits pour la personne fichée. D'autre part, la subordination de l'informatique et de la technique par l'homme à travers l'ambition de protection d'un marché économique en devenir.

87. Par la reconnaissance de ce double objectif, le législateur a malencontreusement donné une assise juridique à la « télématique » c'est-à-dire à la prolifération des moyens techniques et informatiques, et dans le même temps, a favorisé la diffusion de la surveillance.

²³² L'article 1er de la loi informatique et libertés de 1978 est contenu dans un chapitre 1er intitulé principes et définitions. Op. Cit.

²³³ FRAYSSINET Jean, « *L'utilité et les fonctions d'une formulation d'objectifs : l'exemple de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés* », Revue de la Recherche Juridique, n°4, 1989, p.904. Voir également pour une analyse plus récente de ce préambule: OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Op. cit., et spécialement les pages 29 et 30 où l'auteur écrit : « *Cette peur de l'informatique se comprend au regard du contexte socio-culturel entourant l'adoption de cette loi. Mais si l'on se positionne dans ce débat en adoptant une grille de lecture non pas politiste mais publiciste, en ayant à l'esprit que l'on évoque une police administrative spéciale, la perspective change : il ne viendrait à personne l'idée de considérer que la police administrative spéciale des armes à feu pose le problème de la subordination de l'homme au procédé technique même de l'arme à feu. C'est donc bien qu'il existe une tendance culturelle à ressentir une certaine forme de crainte pour les procédés informatiques, tendance se traduisant par la vivacité, toujours forte, de ce courant de la science-fiction tant en littérature qu'au cinéma* ». Bien que nous ne partageons pas ce rapprochement du droit des données personnelles en terme de police administrative spéciale, ce raisonnement par analogie entre la subordination de l'homme aux procédés techniques informatiques et la potentielle subordination de l'homme à l'arme à feu reste particulièrement intéressante.

²³⁴ L'article 1er de la loi précitée dispose en effet : « *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* ».

Paragraphe 2: Des intentionnalités et des perceptions du phénomène de surveillance diffuse : entre technophilie et technophobie

88. Comprendre l'apparition de la surveillance diffuse en tant que phénomène, c'est d'abord envisager d'analyser les perceptions, les représentations voire les intentionnalités tant positives que négatives liées à ce concept. C'est aussi situer ce phénomène, le restituer, comprendre son affiliation avec l'histoire des techniques. Cette dernière, et par voie de conséquences, le phénomène de surveillance diffuse sont partagés entre la mythification, voire, pour reprendre les termes de Stéphane Vial le « fétichisme²³⁵ » et la phobie qu'engendrent la technique. Ces deux éléments permettent de comprendre l'ensemble des ambiguïtés que peut soulever le traitement du concept de surveillance diffuse, et de le concevoir tel qu'il est vraiment.

89. Aborder la surveillance diffuse en tant que phénomène c'est d'abord opérer un retour à l'adage : « *toute conscience est conscience de quelque chose*²³⁶ ». Cet adage représente le fondement même de l'analyse phénoménologique puisque cette dernière est retour à la conscience des choses, aux intentionnalités. Ces dernières peuvent être positives (A) ou négatives (B). Il faut alors évoquer les représentations liées au concept de surveillance diffuse pour pouvoir, par la suite, s'en défaire et aborder la notion telle qu'elle est vraiment, c'est-à-dire revenir à son essence même.

A. Les intentionnalités positives du phénomène de surveillance diffuse: le paroxysme de la technophilie

²³⁵ Vial définit le fétichisme qu'entoure la notion de technique et de système technique comme une « *tendance à croire que la technique est une chose en soi, dotée d'une volonté abstraite qui dirige le cours des événements humains en poursuivant ses propres fins, comme un processus sans sujet.* » Op. Cit. p. 43. Nous nous éloignerons, dans notre premier paragraphe, quelque peu de cette définition pour en revenir à la conception classique du fétichisme c'est-à-dire le respect scrupuleux, l'admiration sans réserve pour quelqu'un ou quelque chose (définition du dictionnaire de français Larousse en ligne). La surveillance est effectivement présentée comme le seul élément possible à mettre en place pour éviter les menaces, les risques et potentiellement le terrorisme. C'est en cela qu'elle devient un fétiche.

²³⁶ Il est nécessaire de rappeler les propos du philosophe allemand, Eugen Fink : « *Le mouvement phénoménologique est, dès son origine, « anti-spéculatif », son inspiration propre est déterminée par un renoncement passionné à toute forme de violence, telle qu'en comporte une interprétation spéculative du monde. Ce qu'il lui importe, c'est de montrer les choses elles-mêmes, sans présuppositions préalables et sans constructions systématisantes, de dire ce qu'elles sont et comment elles sont, en elles-mêmes et en deçà de toute falsification. Elle veut donner le premier et le dernier mot aux « choses elles-mêmes ». Elle veut les préserver de la trame obnubilante des « interprétations » hâtives et ainsi rendre possible cette rencontre par laquelle l'homme vient aux choses dans une confiance humble et profonde à ce qu'elles sont en elles-mêmes, par laquelle il se livre à elles et s'éprouve ainsi libéré de la prison qu'il s'était jusque-là fabriqué lui-même et que, lorsqu'il est « philosophe », il nomme avec orgueil son « système ».* ». FINK Eugen, *Problèmes actuels de la phénoménologie*, p. 57, cité par AMSELEK Paul, *Méthode phénoménologique et théorie du droit*, Paris, LGDJ, 1964, p. 10.

90. L'approche positive de la surveillance diffuse se veut technophile : la technique et, plus globalement, la technologie peuvent emporter des effets positifs sur la société, et même régler les maux qui la frappent (1). Pour certains auteurs, tels que Evgueny Morozov ou Jacques Ellul, cette représentation positivée des technologies et de la technique engendre la mise en place d'un véritable « *solutionnisme technologique*²³⁷ », d'un « *bluff technologique*²³⁸ ». L'une des illustrations les plus éclairantes à ce sujet reste celle de la prise en charge et de la gestion du terrorisme par le politique (2).

1. La surveillance diffuse: une solution pour régler les maux de la société contemporaine

91. Analysant le « *bluff technologique* », Ellul écrit qu'il « *consistait essentiellement à réordonner toute chose, de façon exemplaire et proclamée, en fonction du progrès technique (...). On charge maintenant les techniques de centaines de réussites et d'exploits (dont on ne pose jamais ni les coûts, ni l'utilité, ni les dangers) et que la technique nous est dorénavant présentée expressément à la fois comme la seule solution à tous nos problèmes collectifs (le chômage, la misère du tiers-monde, la pollution, la menace de guerre) ou individuels (la santé, la vie familiale, et même le sens de la vie) (...). Dans ce discours l'on multiplie par cent les possibilités effectives des techniques et l'on voile radicalement les aspects négatifs*²³⁹ ». Plus récemment, pour Morozov, le solutionnisme technologique pourrait être illustré par l'évolution du slogan des entreprises de la Silicon Valley passant de « *l'innovation ou la mort*²⁴⁰ » à « *l'amélioration ou la mort*²⁴¹ ». Et d'ajouter, que « *dans l'ensemble, l'essentiel n'est pas tant de savoir précisément ce qui est amélioré, mais c'est plutôt le fait d'être en mesure de changer les choses, d'amener les êtres humains à adopter un comportement plus responsable et durable, et de parvenir à une efficacité optimale. (...). La technologie peut nous rendre meilleurs, et c'est ce qu'elle fera. Ou pour le dire à la manière des geeks: avec les bonnes applications, tous les bogues de l'humanité deviennent mineurs*²⁴² ».

²³⁷ MOROZOV Evgeny, *L'aberration du solutionnisme technologique - Pour tout comprendre cliquez ici*, Editions FYP, Collection Innovation, 2014

²³⁸ ELLUL Jacques, *Le bluff technologique*, préface de Jean-Luc Porquet, *Ellul l'éclairé*, Hachette, 1988 ; réédition Hachette Littératures, collection « Pluriel », 2004

²³⁹ Ibid, p. 26.

²⁴⁰ MOROZOV Evgeny, *Op. Cit.*, p. 12

²⁴¹ Ibid.

²⁴² Ibid.

92. En réalité, derrière les expressions de « solutionnisme technologique » ou de « bluff technologique » se cache un même dénominateur: la pensée relativement admise dans nos sociétés que la technologie, la technique et le progrès permettent de résoudre l'ensemble des problèmes que rencontre la société. Cette pensée touche l'individu, séduit le politique et est fortement suscitée par les entreprises du numérique. Conjointement, ces acteurs développent, consciemment ou non, un discours et des pratiques permettant de démontrer la puissance de résolution des technologies du numérique, et d'entretenir cette pensée.

93. Si le phénomène de surveillance a pris de l'ampleur ces dernières années²⁴³, c'est bel et bien du fait de l'usage croissant de l'informatique dans la vie quotidienne. Plus globalement l'usage des technologies de l'information et de la communication, l'implantation de technologies de sécurité, l'interconnexion et l'interopérabilité (encore appelée connectabilité) de ces différentes technologies, la généralisation des fichiers, et la création de toujours plus de bases de données personnelles ont permis à la surveillance de devenir elle-même automatisée, technicisée. Plus l'informatique et les technologies ont évolué, plus elles se sont combinées, plus elles ont interagi entre elles, plus elles ont fait naître de nouvelles formes de communication et de connexion, et donc de possibilités de surveillance. Aujourd'hui, chaque objet de notre vie est susceptible de devenir un outil communiquant, un objet connecté. Demain, ces objets deviendront invisibles (puces RFID, nanotechnologies), et évolueront dans leur manière d'être : d'une surveillance d'un individu par ses données (dataveillance), on passera à la surveillance d'un corps, pour enfin envisager la surveillance intra-corporelle. Qu'il s'agisse du réfrigérateur connecté permettant de surveiller notre consommation et notre alimentation; de l'instauration du numérique à l'école²⁴⁴, du règlement des impôts en ligne, de l'invocation récente d'une République du numérique; mais aussi, dans une certaine mesure, des pratiques des entreprises de la Silicon Valley²⁴⁵; le progrès technologique est présenté comme la solution pour vivre mieux, en sécurité, protéger des menaces, de se prémunir des

²⁴³ En ce sens, et du point de vue sécuritaire, voir: *Stasi Versus NSA, Quelle place prendraient les armoires d'archivage de la STASI et de la NSA - si la NSA décidait d'imprimer ses 5 zettaoctet de fichiers?* (0,0019 km² pour la Stasi, 17 millions de km² pour la NSA), En ligne: <https://apps.opendatacity.de/stasi-vs-nsa/francais.html> (dernière consultation: 5 mars 2018)

²⁴⁴ Voir en ce sens: LELIEVRE Claude, *Le numérique à l'école: une (vienne) affaire présidentielle ?*, 10 novembre 2014, Médiapart, En ligne: <https://blogs.mediapart.fr/claude-lelievre/blog/101114/le-numerique-lecole-une-vienne-affaire-presidentielle> (dernière consultation: 5 mars 2018)

²⁴⁵ On citera par exemple la récente ambition de Facebook de s'inscrire pleinement dans la lutte contre le terrorisme par l'intelligence artificielle. Voir: GAROSCIO Paolo, *Facebook: l'IA pour lutter contre le terrorisme*, 16 juin 2017, Clubic, En ligne: <http://www.clubic.com/internet/facebook/actualite-832002-facebook-ia-lutter-terrorisme.html> (dernière consultation: 5 mars 2018)

risques, et même, en France d'inverser la courbe du chômage²⁴⁶. Et ce sont ces raisons qui font de ces exemples des symptômes du bluff ou du solutionnisme technologique. La technologie, ses implications - allant de l'information et de la communication à la surveillance - les progrès sans cesse renouvelés de la technologie sont présentés comme un remède à chaque problématique particulière et sociétale.

94. Au-delà du potentiel de surveillance des technologies utilisées, c'est en fait une nouvelle pratique qui est engendrée par le progrès technologique, et validée par ce bluff, ce solutionnisme technologique: la surveillance. A chaque nouvelle problématique collective et individuelle liée à l'environnement, la finance, au domaine du sanitaire; ou de certaines problématiques individuelles (santé, alimentation, sécurité), correspond aujourd'hui, par effet miroir, une forme de surveillance: surveillance sismique, surveillance des centrales nucléaires, surveillance de l'environnement et de l'eau, surveillance et contrôle des maladies, surveillance d'Internet... Pour paraphraser ce que Jacques Ellul écrivait à propos du progrès technique²⁴⁷, il est possible d'affirmer aujourd'hui que chaque pratique de surveillance est destinée à résoudre un certain nombre de problèmes, ou plus exactement en face d'un danger, d'une difficulté, on trouve forcément la surveillance technicisée adéquate.

2. Illustration du solutionnisme technologique: la surveillance diffuse comme réponse au terrorisme

95. Le terrorisme a toujours été présent dans nos sociétés²⁴⁸. La lutte contre le terrorisme

²⁴⁶ Voir en ce sens: DE LA BROUSSE Julie, Paul Duan, ce petit génie qui a élaboré un algorithme anti-chômage, 25 février 2016, L'express, En ligne: https://www.lexpress.fr/emploi/paul-duan-ce-petit-genie-qui-a-elabore-un-algorithme-antichomage_1766940.html (dernière consultation: 5 mars 2018)

²⁴⁷ « Chaque progrès technique est destiné à résoudre un certain nombre de problèmes. Ou plus exactement: en face d'un danger, d'une difficulté précis, limités, on trouve forcément la réponse technique adéquate ». ELLUL Jacques, *Le bluff technologique*, Op. Cit., p. 112

²⁴⁸ Jacques Derrida déclare que, « si on se réfère aux définitions courantes ou explicitement légales du terrorisme, qu'y trouve-t-on ? La référence à un crime contre la vie humaine en violation des lois (...) y implique à la fois la distinction entre civil et militaire (...) et une finalité politique (...). Ces définitions n'excluent donc pas le « terrorisme d'État ». Tous les terroristes du monde prétendent répliquer, pour se défendre, à un terrorisme d'État antérieur qui, ne disant pas son nom, se couvre de toutes sortes de justifications plus ou moins crédibles ». in. Borradori Giovanna, *Entretiens avec deux grands intellectuels sur le « concept » du 11 septembre 2001 - qu'est ce que le terrorisme ?*, Le monde diplomatique, février 2004, p. 16, En ligne: <https://www.monde-diplomatique.fr/2004/02/DERRIDA/11005> (dernière consultation: 5 mars 2018). En guise de référence générale, on évoquera des exemples de terrorisme dit individuel (pratiqué par des anarchistes à la fin des années 1890), de terrorisme organisé (Al Qaeda ou encore DAESH), mais également des formes de terrorisme d'État, des terrorismes revendiquant l'indépendance ou le séparatisme (la fondation de l'IRA en 1919 par exemple). Et: COOLSAET Rick, *Au temps du terrorisme anarchiste*, Le Monde diplomatique, septembre 2004, p. 26, En ligne: <https://www.monde-diplomatique.fr/2004/09/COOLSAET/11443> (dernière consultation: 5 mars 2018)

s'organise, quant à elle, traditionnellement autour de la surveillance²⁴⁹. De fait, les affaires récentes liées aux révélations de Edward Snowden, s'inscrivent dans une continuité²⁵⁰, pour les Etats-unis, dans la collecte de renseignements à grande échelle contre le terrorisme, et, plus globalement, leur sécurité nationale. Néanmoins, la technicisation de la surveillance, son caractère massif tant en volume d'individus surveillés que d'informations collectées, les discours de légitimation de ces pratiques sont des caractéristiques de la surveillance qu'il faut analyser à la lumière du bluff ou du solutionnisme technologique.

96. Avec le 11 septembre 2001, et sous couvert de la guerre contre le terrorisme, des logiques discursives sont apparues : menaces, risques, dangers, prévention, sécurité, ennemis protéiformes sont devenus des notions et concepts manipulés au gré des discours politiques permettant l'effacement progressif des limites posés par l'État de droit. Comme le rappelle Mireille Delmas-Marty, « *au vu de ces évolutions récentes apparemment convergentes apparaît l'hypothèse d'un effet indirect des attentats du 11 septembre 2001 qui auraient en quelque sorte libéré les responsables politiques, symboliquement et juridiquement, de l'obligation de respecter les limites propres à l'État de droit ; et ainsi déclenché, par une série d'ondes de choc, des mouvements qui sont d'autant moins contrôlables qu'ils relèvent pour une large part des interdépendances liées aux phénomènes d'internationalisation du droit*²⁵¹ ». Parmi ces ondes de choc, les glissements sémantiques tels que l'évocation, voire « l'invocation quasi-diabolique », des notions de menaces, de risques, de peurs, mais également d'ennemis, ont eu des répercussions importantes sur le Droit, sur la notion même d'État de droit, sur notre perception du monde. Par exemple, si nous nous intéressons à la rhétorique

²⁴⁹ La Conférence internationale de Rome pour la défense sociale contre les anarchistes de 1898 permet, par exemple, la mise en place d'une coopération inter-étatique et policière contre un mouvement considéré comme terroriste. Cette coopération a engendré la surveillance et le recueil d'information sur ce groupe. Pour une référence générale, voir BAUSARDO Thomas, « Quel passé pour Prism et Snowden ? », *Vacarme* 2014/1 (n°66), Op. Cit. . L'auteur retrace brièvement une histoire de la surveillance et débute son article ainsi: « *ça le fait doucement rire, l'historien, de lire en marge de l'affaire Snowden, qu'entre les services de renseignement occidentaux le niveau de coopération en matière d'anti-terrorisme est des plus élevés. Parce que cela ne date pas d'hier, ni même des débuts du renseignement d'origine électromagnétique. Faut-il voir dans Prism, X-Keyscore, Muscular, Tempora, etc., des révélations véritables ou fondamentales ? Ou seulement des témoignages de la permanence des luttes anti-terroristes depuis la fin du XIXe siècle ? Comment concevoir le présent de ces luttes à la lumière des pratiques du passé ?* ». Nous partageons totalement le questionnement ironique de l'auteur. Un simple regard à l'histoire du renseignement en France et à l'international, montre que l'utilisation de la surveillance en matière de lutte contre le terrorisme n'a rien de nouveau.

²⁵⁰ Du programme Echelon au programme Prism, les enjeux restent effectivement les mêmes pour les Etats-Unis: sécurité nationale, lutte contre le terrorisme, hégémonie économique. Ainsi que le rappelle Thomas Bausardo, dans l'article précité, ces pratiques ne sont pas propres aux Etats-Unis. « *De tous temps, l'espionnage. (...) Tous les Etats, selon des stratégies, des intérêts et des moyens qui leur sont propres - espionnent. Ils l'ont toujours fait - et continueront de le faire. Le renseignement a toujours été une donnée fondamentale de l'art de gouverner* », in. BAUSARDO Thomas, Op. Cit., p. 144 - 145.

²⁵¹ DELMAS-MARTY Mireille, *Libertés et sûreté dans un monde dangereux*, Éditions du Seuil, Collection « La couleur des idées », 2010, p. 8

de la guerre contre l'ennemi prônée dans chacun des discours politiques et médiatiques qui ont suivi le 11 septembre 2001²⁵², on s'aperçoit que la vision humaniste du droit pénal²⁵³ s'est progressivement effacée au profit d'une vision positiviste²⁵⁴ dite de « défense sociale ». Aujourd'hui cette vision du droit pénal se déplace de l'idée de défense à l'application d'une logique de prévention totale. Cette « *déshumanisation du droit pénal*²⁵⁵ » couplée à « *une anthropologie guerrière*²⁵⁶ », rendue possible par ces discours médiatiques et politiques qui contribuent à insuffler une « *culture de la peur*²⁵⁷ », ont permis le passage de la notion de criminel personnifié à la notion d'ennemi désincarné. Ainsi, on a vu proliférer des concepts comme celui aux Etats-Unis « *d'ennemi combattant illégal*²⁵⁸ », mais également, en Europe avec le passage du concept « d'ennemi intérieur à l'ennemi transversal²⁵⁹ », « *d'ennemi de l'ordre public*²⁶⁰ » ; autant de notions relevant de la désincarnation du droit pénal et de « l'anthropologie guerrière » pour reprendre l'expression utilisée par Mireille Delmas-Marty.

97. Ces stratégies discursives et logiques d'argumentation guerrière ne s'arrêtent pas simplement

²⁵² Cela vaut également pour les discours politiques et médiatiques qui ont suivi les meurtres perpétrés à Charlie Hebdo le 7 janvier 2015. On notera, pour s'en convaincre, une phrase issue du livre de Marc Crépon, *La culture de la peur*, Paris, Galilée, 2008, p. 14. L'auteur évoque le développement « *d'une culture de la peur à laquelle aucun discours politique, aucune mise en scène médiatique de l'information ne semble résister* ».

²⁵³ Les tenants de la vision humaniste et classique du droit pénal sont Kant (école de la justice absolue), Beccaria (école classique) et Ortolan (école néo-classique). La doctrine néo-classique pourrait se résumer par l'adage suivant : « *punir ni plus qu'il n'est juste, ni plus qu'il n'est utile*. » La répression doit prendre en compte la double exigence de la justice morale et de l'utilité sociale. Pour ce faire, les néo-classiques insistent sur la nécessité d'une individualisation de la peine. L'individu, son passé, sa personnalité doivent être pris en compte *in concreto* par le juge afin d'apprécier la responsabilité pénale d'un individu.

²⁵⁴ Les tenants de l'école positiviste, en droit pénal, sont Lombroso, Ferri, Garofalo, tous trois disciples d'Auguste Comte. Ici, la criminalité est placée dans une compréhension nouvelle et est traduite par le phénomène criminel. Ce phénomène est éclairé par deux concepts : le déterminisme (le crime est le résultat de causes exogènes ou endogènes), ainsi que l'irresponsabilité morale du délinquant (l'homme étant déterminé, il est insensé pour les positivistes de raisonner en termes de responsabilité morale, de culpabilité ou encore de libre arbitre). L'individu est alors objet de la science pénale, non plus acteur individualisé doué de raison

²⁵⁵ DELMAS – MARTY Mireille, *Op. Cit.*, p.41 et suivantes

²⁵⁶ *Ibid.*, p.84

²⁵⁷ Voir le livre de Marc Crépon précité. La culture de la peur sera analysée par la suite de nos développements.

²⁵⁸ CANTEGREIL Julien, « *La doctrine américaine de « l'ennemi combattant illégal »* », in DELMAS – MARTY Mireille, HALPERIN Jean - Louis et GIUDICELLI – DELAGE Geneviève (dir.), *Les politiques sécuritaires à la lumière de la doctrine pénale du 19^{ème} au 21^{ème} siècle*, Revue de Sciences Criminelles (RSC), Dalloz, 2010 n°81, 15 mars 2010

²⁵⁹ RIGOUSTE Mathieu, « *L'ennemi intérieur, de la guerre coloniale au contrôle sécuritaire* », *Cultures & Conflits*, 67, automne 2007, 4 janvier 2010, En ligne: <http://conflits.revues.org/3128> (dernière consultation: 5 mars 2018); et du même auteur, *La généalogie coloniale et militaire de l'ordre sécuritaire dans la France contemporaine*, Collection La Découverte Poche/Essais n°348, Éditions Broché, juin 2011

²⁶⁰ JAKOBS Günther, *Aux limites de l'orientation par le droit : le droit pénal de l'ennemi*, in RSC, 2009, n°1, p7. Plus globalement, le dossier consacré au droit pénal de l'ennemi – droit pénal de l'inhumain paru à la revue de science criminelle dans son numéro 1/2009.

à des mots que nos responsables politiques auraient préférés utiliser à la place d'un autre, ni à de simples glissements sémantiques. Métamorphose de la justice pénale, mais aussi, plus insidieusement, du contrôle social par l'entretien d'une culture de la peur sont des conséquences nettes et palpables de ces stratégies. Plus loin encore, ces dernières ont permis la légalisation de la surveillance. A la suite des attentats du 11 septembre 2001, lorsque Georges Bush emploie pour la première fois l'expression de « guerre contre le terrorisme », ce n'est pas dans le simple but de frapper les esprits avec cette métaphore. En effet, à l'inverse de la Constitution française qui prévoit expressément l'état d'exception²⁶¹, permettant, dans le cas où l'État se trouve en situation de péril grave, de méconnaître les règles légales qui régissent normalement son activité afin d'assurer sa sauvegarde ; la Constitution américaine, elle, ne prévoit pas ce genre de mesures. Ainsi, seul l'état de guerre permet un transfert de pouvoirs au président des États-Unis. Six semaines après les attaques du 11 septembre 2001, le Congrès américain approuvait le USA Patriot Act²⁶² proposé par le président Bush. Cette loi a rendu possible, grâce à la métaphore « guerre contre le terrorisme », la surveillance de masse et technicisée, ainsi qu'un régime pénal d'exception (torture, assassinats ciblés).

98. Une autre forme de discours de légitimation se manifeste dans les mots et expressions utilisés pour évoquer certaines technologies de surveillance. L'un des exemples les plus révélateurs est le recours à la notion de vidéoprotection pour remplacer la notion de vidéosurveillance en France. Le texte de loi de référence en la matière est la loi d'orientation et de programmation

²⁶¹ L'article 16 de la Constitution française du 4 octobre 1958 déclare : « Lorsque les institutions de la République, l'indépendance de la Nation, l'intégrité de son territoire ou l'exécution de ses engagements internationaux sont menacés d'une manière grave et immédiate et que le fonctionnement régulier des pouvoirs publics constitutionnels est interrompu, le Président de la République prend les mesures exigées par ces circonstances, après consultation officielle du Premier ministre, des Présidents des Assemblées ainsi que du Conseil constitutionnel. Il en informe la Nation par un message. Ces mesures doivent être inspirées par la volonté d'assurer aux pouvoirs publics constitutionnels, dans les moindres délais, les moyens d'accomplir leur mission. Le Conseil constitutionnel est consulté à leur sujet. Le Parlement se réunit de plein droit. L'Assemblée nationale ne peut être dissoute pendant l'exercice des pouvoirs exceptionnels. Après trente jours d'exercice des pouvoirs exceptionnels, le Conseil constitutionnel peut être saisi par le Président de l'Assemblée nationale, le Président du Sénat, soixante députés ou soixante sénateurs, aux fins d'examiner si les conditions énoncées au premier alinéa demeurent réunies. Il se prononce dans les délais les plus brefs par un avis public. Il procède de plein droit à cet examen et se prononce dans les mêmes conditions au terme de soixante jours d'exercice des pouvoirs exceptionnels et à tout moment au-delà de cette durée ».

²⁶² Le USA Patriot Act est une loi américaine votée par le Congrès des États-Unis et signée par le Président Georges W. Bush le 26 octobre 2001. Le titre réel de cette loi est le suivant : *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*. Cette loi anti-terroriste permet donc d'unir et de renforcer les États-Unis d'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme. Cette loi permet d'améliorer l'efficacité des services de renseignements américains en cas de terrorisme suspecté, et donc permet légalement, pour la première fois, la surveillance. Il est utile de noter dès maintenant que les révélations d'Edward Snowden ont permis de réviser cette loi, dont la section 215, qui permettait aux services de renseignements américains de collecter et de stocker massivement des données portant sur les communications téléphoniques des citoyens américains.

relative à la sécurité du 21 janvier 1995²⁶³. Son article 10 évoque clairement la notion de vidéosurveillance. Or, avec l'explosion des usages de cette technologie, et les craintes soulevées par cette dernière²⁶⁴, il a fallu donner une vision positive de cette notion. C'est ainsi qu'en mars 2011, la LOPPSI 2²⁶⁵, venue réformer la loi du 21 janvier 1995, remplaça le terme vidéosurveillance par le terme vidéoprotection²⁶⁶. En 2009 déjà, un guide méthodologique de vidéoprotection avait été imaginé pour situer « *l'outil vidéo dans une démarche de sûreté et de sécurité*²⁶⁷ ». La préface de ce guide est à cet égard très instructive en termes de discours de légitimation. Brice Hortefaux déclare : « *en dix ans, la vidéoprotection a fait ses preuves. Elle constitue un outil efficace d'une politique de sécurité. Nos concitoyens le savent et y sont très largement favorables, ayant compris qu'il ne s'agit pas de surveiller mais de protéger. Nous sommes passés de la vidéosurveillance à la vidéoprotection*²⁶⁸ ». Ces propos méritent quelques éclaircissements. D'une part, à l'époque de la rédaction de ce guide, aucune étude sérieuse ne parvient à déterminer les réels apports de l'installation de la vidéosurveillance sur la voie publique en matière de prévention de la délinquance et de prévention du terrorisme²⁶⁹. D'autre part, les avis des citoyens français n'ont pas été recueillis

²⁶³ Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, spécialement son article 10, JORF n°0020 du 24 janvier 1995, page 1249, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000369046&categorieLien=id> (dernière consultation: 5 mars 2018)

²⁶⁴ On pense notamment au concept de société de surveillance, à la vision Orwellienne d'un monde organisé sous caméras de vidéosurveillance, et à l'ensemble des problématiques liés au respect de la vie privée.

²⁶⁵ Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n° 0062 du 15 mars 2011, page 4582, texte n°2, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000023707312 (dernière consultation: 5 mars 2018)

²⁶⁶ L'article 17 de la LOPPSI 2 énonce « *sous réserve des dispositions de la présente loi, dans tous les textes législatifs et réglementaires, le mot « vidéosurveillance » est remplacé par le mot « vidéoprotection »* ».

²⁶⁷ *Guide méthodologique de vidéoprotection – L'outil vidéo dans une démarche de sûreté et de sécurité*, La Documentation Française, Paris, 2009

²⁶⁸ Ibid p. 5

²⁶⁹ Un rapport de la Cour des comptes de 2011 consacre une section entière à la question de l'évaluation de l'efficacité de ce type de dispositif. Ce rapport souligne que: « *Le taux d'élucidation des faits de délinquance de proximité n'a pas davantage progressé dans les circonscriptions de sécurité publique (CSP) équipées de caméras de vidéosurveillance de la voie publique que dans celles qui ne le sont pas. Pour les faits de délinquance pris globalement, il s'est même davantage amélioré dans les CSP non vidéo-surveillées. Malgré un usage désormais plus répandu, la proportion des faits de délinquance élucidés grâce à la vidéosurveillance de la voie publique est relativement faible.* », in. Cour des Comptes, Rapport public thématique – *L'organisation et la gestion des forces de sécurité publique*, juillet 2011, p. 148, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/114000374/0000.pdf> (dernière consultation: 5 mars 2018). En 2013, un autre rapport d'information déclare que le « *rapporteur spécial déplore cet investissement d'un coût élevé dans des systèmes de surveillance potentiellement attentatoires aux libertés publiques et dont aucune étude sérieuse (ni en France, ni à l'étranger) n'a prouvé l'efficacité en termes de sécurité publique.* ». Ce rapport établit deux recommandations: la décision d'un « *moratoire sur les investissements relatifs à la vidéosurveillance, dans l'attente d'une étude scientifique indépendante sur les apports véritables de la vidéosurveillance en termes de sécurité* », ainsi que la nécessité de « *créer un indicateur de performance relatif aux dispositifs de vidéosurveillance (mesurant par exemple le nombre d'affaires élucidées grâce à ce type de dispositif)* ». in. PLACE Jean-Vincent, Rapport d'information fait au nom de la commission des finances sur les investissements dans la police et la gendarmerie, Enregistré à la Présidence du Sénat le 22 octobre 2013, En ligne: <http://www2.senat.fr/rap/r13-091/r13-0911.pdf> (p. 57 - 58) (dernière consultation: 5 mars 2018).

individuellement et collectivement dans le cadre d'un référendum, mais bien à l'occasion de sondages qui n'ont pas la même portée ni la même signification.

99. Par l'usage de mots, d'expressions, de stratégies discursives et logiques d'argumentation qui s'appuient sur la peur d'un ennemi invisible, la surveillance de masse technicisée et globalisée a été rendue possible, et son usage a été légalisé. Dans cette optique positive, tout se passe alors comme si la surveillance permettait de prévenir la réalisation hypothétique d'un scénario du pire, comme si elle était la seule solution aux maux de nos sociétés contemporaines.

B. Les intentionnalités technophobiques et négatives de la surveillance diffuse: vers un monde rationalisé

100. Les éléments précités, bien que constituant un terreau favorable à la surveillance, ne permettent pas de comprendre sa diffusion aussi importante dans la société. Réduire la progression du phénomène de surveillance aux simples usages technologiques, à l'accès et à la circulation de l'information et aux discours de légitimation des différents acteurs serait insuffisant. Pour autant, ces derniers permettent de comprendre que la surveillance et sa diffusion sont fortement liées à la notion de « technique », entendue dans une acception large. La majuscule est de rigueur car elle permet, à ce stade de l'étude, de comprendre ce terme comme englobant tout ce que nos sociétés industrielles ont « enveloppé » sous l'appellation progrès technologique et ce qu'il engendre (1). L'analyse de ce concept permettra alors de questionner la rationalité des actions prises par le législateur et les discours politiques en vue de légitimer la surveillance (2).

1. La surveillance diffuse comme facteur de rationalisation et de désenchantement du monde

101. Dès 1934, Simone Weil écrivait « *la période présente est de celles où tout ce qui semble normalement constituer une raison de vivre s'évanouit, où l'on doit, sous peine de sombrer dans le désarroi ou l'inconscience, tout remettre en question. (...). Le progrès technique semble avoir fait faillite, puisque au lieu du bien-être il n'a apporté aux masses que la misère physique et morale où nous les voyons se débattre ; au reste les innovations techniques ne sont plus admises nulle part, ou*

*peu s'en faut, sauf dans les industries de guerre*²⁷⁰ ». Ces lignes, écrites il y a quatre-vingt-quatre ans, sont encore étonnantes de réalisme et d'actualité. Les causes du malaise que décrit Simone Weil ne se trouvent pas réellement dans la montée du nationalisme et de l'autoritarisme²⁷¹ mais bien dans le progrès technique qui angoisse et prive d'avenir toute une génération²⁷². Plus que la désillusion²⁷³ des individus face à la technique, Simone Weil annonce, par cette description de la perte de sens de la vie, un monde désenchanté par le progrès technique.

102. La notion sociologique de « *désenchantement du monde*²⁷⁴ », dont la paternité revient à Max Weber, est très présente dans la littérature de la technique. Dans son ouvrage intitulé « *l'éthique protestante et l'esprit du capitalisme* », Weber évoque pour la première fois le désenchantement du monde et le définit comme « *l'abandon de la magie comme instrument du salut*²⁷⁵ ». Pour mieux comprendre les contours de cette notion, il faut se référer à un autre ouvrage de Max Weber : « *le savant et le politique* ». Dans ce dernier, l'auteur déclare à nouveau que le désenchantement du monde s'explique par un recul des croyances religieuses et magiques comme mode d'explication des phénomènes. Il écrit notamment : « *le destin de notre époque caractérisée par la rationalisation, par l'intellectualisation et surtout par le désenchantement du monde, a conduit les humains à*

²⁷⁰ WEIL Simone, *Réflexions sur les causes de la liberté et de l'oppression sociale*, Les Éditions Gallimard, Collection Idées, 1955, p. 7. Parmi ses œuvres, voir notamment : *L'enracinement : prélude à une déclaration des devoirs envers l'être humain*, Éditions Gallimard, Collection Folio Essais, 1990 ; *La pesanteur et la grâce*, Éditions Pocket, Collection Classique, 1993 ; *Note sur la suppression générale des partis politiques*, Éditions Climats, 2006

²⁷¹ Simone Weil l'écrit fort justement : « *Que le triomphe des mouvements autoritaires et nationalistes ruine un peu partout l'espoir que de braves gens avaient mis dans la démocratie et dans le pacifisme, ce n'est qu'une partie du mal dont nous souffrons ; il est bien plus profond et bien plus étendu. On peut se demander s'il existe un domaine de la vie publique ou privée où les sources mêmes de l'activité et de l'esérance ne soient pas empoisonnées par les conditions dans lesquelles nous vivons* ». Ibid. p.7.

²⁷² Simone Weil écrit : « *La génération même [les jeunes] pour qui l'attente fiévreuse de l'avenir est la vie tout entière végète, dans le monde entier, avec la conscience qu'elle n'a aucun avenir, qu'il n'y a point de place pour elle dans notre univers. Au reste ce mal, s'il est plus aigu pour les jeunes, est commun à toute l'humanité d'aujourd'hui. Nous vivons une époque privée d'avenir. L'attente de ce qui viendra n'est plus espérance, mais angoisse* ». Ibid. p.8.

²⁷³ Il faut bien opérer une distinction entre les termes « désillusion » et « désenchantement du monde ». Pour décrire ce désenchantement, Weber utilise le terme « entzauberung » (désenchanter) et non le mot « enttäuschung » qui signifie la simple désillusion. Au-delà de cette simple sémantique de traduction, il faut s'attacher à donner une bonne interprétation de ce que signifie ces deux termes, et spécialement le concept de désenchantement du monde. Alors que la désillusion relève de la conscience propre d'un individu sur son vécu, et particulièrement sur la conscience d'un décalage entre la réalité et les représentations idéalisées qu'il se fait de la réalité, le désenchantement du monde va plus loin que la simple déception entre la réalité et des attentes idéalisées. Ce concept relève d'un phénomène de plus grande ampleur et touche un ensemble, un groupe social large.

²⁷⁴ Max Weber a envisagé cette notion, pour la première fois, dans son livre intitulé *L'éthique protestante et l'esprit du capitalisme* paru en 1905. Il a ensuite développé ce concept dans un ouvrage intitulé *Le savant et le politique*, qui contient deux conférences données en 1919, l'une sur « *le métier et la vocation du savant* », l'autre sur « *le métier et la vocation d'homme politique* ». WEBER Max, *L'éthique protestante et l'esprit du capitalisme*, Traduction inédite et présentation par Isabelle Kalinowski, Éditions Flammarion, Collection Champs, 2000. WEBER Max, *Le savant et le politique*, Préface, traduction et notes de Catherine Colliot-Thélène, Éditions La Découverte, Collection Poche, Paris 2003.

²⁷⁵ WEBER Max, *L'éthique protestante et l'esprit du capitalisme*, Op. Cit., p. 190.

*bannir les valeurs suprêmes les plus sublimes de la vie publique*²⁷⁶ ». Plus concrètement, ce concept signifie que l'irrationnel, voire le surnaturel, comme la magie et les religions, s'estompent peu à peu comme moyens d'explications du monde. La Science et la technique remplacent progressivement ces derniers. Dès lors que la Science et la technique permettent d'analyser, d'opérer par gestion des risques, analyse des menaces qui pèsent sur le monde, les individus ne cherchent plus à le comprendre ou à analyser le sens caché de certains événements. La Science comme la technique ne permettent absolument plus de donner un sens à la vie en prescrivant des lignes de conduites ou de morales, ce que font les religions et les croyances ; elles intellectualisent et rationalisent le monde qui entoure les hommes²⁷⁷.

103. Appliqués au phénomène de surveillance, les mots de Simone Weil et de Max Weber ont un retentissement particulier. La surveillance, telle qu'on la connaît aujourd'hui, c'est-à-dire technicisée, s'appuyant sur les dernières innovations technologiques et tendant à recouvrir tous les aspects de l'existence des individus, est bel et bien un phénomène né de la technique. La société contemporaine ne tend plus à la simple recherche d'un bien-être qui serait rendu possible par la technique. Aujourd'hui les individus, les États et les entreprises recherchent la sécurité en toute chose : sécurité individuelle, sécurité globale, sécurité nationale, sécurité internationale, sécurité économique et financière, ou encore sécurité sanitaire. Les innovations, la technique et la surveillance sont admises partout, elles sont rendues acceptables dans la sphère publique et s'immiscent insidieusement dans l'antré privée du domicile. Elles servent, non plus simplement une industrie de guerre²⁷⁸, comme le décrivait Simone Weil, mais un ensemble d'acteurs variés allant des industriels aux États, en passant par les individus. Et, la surveillance, par la collecte de données croissante qu'elle suppose, sert également cet effort sécuritaire. Cette recherche permanente de la sécurité en toute chose correspond bien au mouvement de rationalisation du monde décrit par Weber. Par la surveillance,

²⁷⁶ WEBER Max, *Le savant et le politique*, traduit par J. Freund, Collection Le Monde en 10-18, Paris : Union Générale d'Éditions, 1963, p. 120.

²⁷⁷ Sur ces deux notions, Weber ajoute: « *l'intellectualisation et la rationalisation croissantes ne signifient donc nullement une connaissance générale croissante des conditions dans lesquelles nous vivons. Elles signifient bien plutôt que nous savons ou que nous croyons qu'à chaque instant nous pourrions, pourvu seulement que nous le voulions, nous prouver qu'il n'existe en principe aucune puissance mystérieuse et imprévisible qui interfère dans le cours de la vie; bref que nous pouvons maîtriser toute chose par la prévision. Mais cela revient à désenchanter le monde* ». Ibid. p. 90.

²⁷⁸ La majeure partie des innovations récentes ont eu, en premier lieu, une vocation militaire, pour trouver ensuite une application dans la société civile. Tel est le cas, par exemple, pour Internet qui a été rendu possible grâce à un projet de recherche et développement du Département de la Défense Américaine (DARPA), pour la géolocalisation par satellite (liée également à la DARPA), ou plus récemment pour l'intérêt grandissant concernant les drones, les nanotechnologies et les nanomatériaux.

nous croyons être en sécurité, ou plutôt nous sommes arrivés dans une ère de recherche permanente de prévisibilité qui nous pousse à croire en des discours prônant la sécurité.

104. Aussi, la description du désenchantement du monde opérée par Weber, en ce qui concerne la technique et le progrès, peut trouver application dans le domaine de la surveillance. Pour décrire cette notion, Weber évoque deux concepts opératoires : l'intellectualisation et la rationalisation du monde. Cette dernière est caractérisée par le fait que l'individu²⁷⁹ agit de manière rationnelle, c'est-à-dire qu'il donnera un sens à son action. Weber privilégie une approche de l'action sociale déterminée par la rationalité en finalité²⁸⁰. L'individu choisit, dans ce cadre, les moyens les plus efficaces afin d'atteindre un objectif rationnel, tout en anticipant les conséquences de cette action par un bilan entre les coûts et les avantages recherchés. Les promoteurs de la mise en œuvre d'une surveillance étatique²⁸¹ s'inscrivent dans cette logique d'action rationnelle en finalité. Pour preuve, il

²⁷⁹ Afin d'appréhender les actions sociales et leur sens, variant en fonction du degré de conscience qu'ont les individus, Weber utilise la notion d'idéal-type. Cette notion est une construction théorique qui permet d'avoir une représentation de la réalité, une image, un modèle afin de pouvoir élaborer des hypothèses et de les comparer à cette réalité. Cette construction intellectuelle permet alors de comprendre les relations entre des phénomènes concrets, leur causalité et leur signification. L'action sociale est elle-aussi défini par Weber: « *Nous entendons par « activité » un comportement humain (peu importe qu'il s'agisse d'un acte extérieur ou intime, d'une omission ou d'une tolérance) quand et pour autant que l'agent ou les agents lui communiquent un sens subjectif. Et par activité « sociale », l'activité qui, d'après son sens visé par l'agent ou les agents, se rapporte au comportement d'autrui, par rapport auquel s'oriente son déroulement.(...) L'action ou l'activité sociale doit être comprise par le sens que lui attachent les acteurs* » in., WEBER Max, *Économie et société – 1. Les catégories de la sociologie*, Traduit de l'allemand par J. Freund (et al.), Éditeur Pocket, Collection Pocket Agora, 1995

²⁸⁰ Weber pose le principe suivant: *a priori*, le comportement des individus est rationnel. L'analyse de l'écart entre ce comportement, supposé rationnel, et le comportement réel des individus dans la société qui permet de vérifier le principe, ou alors l'exception à l'hypothèse de départ (c'est-à-dire la rationalité de l'action).

²⁸¹ En-deçà de cette logique de rationalité se profile la notion de management où la vertu fait place à l'efficacité, et où le couple efficacité-efficience permet la primauté des moyens mis en œuvre sur les finalités réelles. A travers un vocable managérial, la loi organique relative aux lois de finances a, par exemple, insufflé, une réelle culture de la performance et du pilotage stratégique pour une gestion, souhaitée efficace, des dépenses publiques. On pense notamment à la Révision Générale des Politiques Publiques (RGPP), puis à la Modernisation de l'Action Publique (MAP). Le secteur privé est également touché par la logique de rationalité. On se référera à certains écrits de l'économiste, Joseph Schumpeter. Dans son œuvre intitulé *Capitalisme, socialisme et démocratie*, publié en 1942 il démontre que les entreprises ne pourront que se tourner vers des actions rationnelles en finalité, et ce, afin de s'inscrire dans un processus perpétuel de « *destruction créatrice* ». L'auteur déclare : « *L'ouverture de nouveaux marchés nationaux ou extérieurs et le développement des organisations productives, depuis l'atelier artisanal et la manufacture jusqu'aux entreprises amalgamées telles que l'U.S. Steel, constituent d'autres exemples du même processus de mutation industrielle - si l'on me passe cette expression biologique – qui révolutionne incessamment de l'intérieur la structure économique, en détruisant continuellement ses éléments vieillis et en créant continuellement des éléments neufs. Ce processus de Destruction Créatrice constitue la donnée fondamentale du capitalisme : c'est en elle que consiste, en dernière analyse, le capitalisme et toute entreprise capitaliste doit, bon gré mal gré, s'y adapter* » (in.. SCHUMPETER Joseph, *Capitalisme, socialisme et démocratie*, Traduction française de Gaël Fain, 1942, Paris, éd. Payot, p. 93). La notion de destruction créatrice décrite par Schumpeter doit être analysée à la lumière des stratégies d'innovations permanentes, tant sur le plan des investissements et des méthodes financières, des processus de production et de marketing, mais également sur le plan des produits eux-mêmes. Ce cycle d'évolution continue conditionne la vie de l'entreprise dans le but d'assurer sa compétitivité, son efficacité, sa rentabilité. Ce constat est le même pour les individus. Comme le rappelle Max Weber : « *L'homme est tributaire du profit qui devient la fin de sa vie : ce n'est plus le profit qui est subordonné à l'homme, comme un moyen destiné à satisfaire ses besoins matériels. Tout bonnement impensable d'un point de vue naïf, ce renversement de l'ordre que l'on pourrait dire « naturel » est manifestement un leitmotiv du capitalisme : ceux qui n'ont pas été touchés par son souffle ne peuvent le saisir.* » (in. WEBER Max, *L'éthique protestante et l'esprit du capitalisme*, Op. Cit., 2000, p.92)

est possible de s'appuyer sur la loi française relative au renseignement²⁸² ou encore sur le USA Patriot Act. Ces deux lois ont été mises en place à la suite d'attentats terroriste : l'un contre les États-Unis le 11 septembre 2001, l'autre contre la France le 7 janvier 2015. Ces deux comportements, actions des législateurs américains et français, ou plutôt ces réactions face au terrorisme, ont pour objectif d'augmenter les moyens techniques et juridiques, attribués à la prévention des menaces, à la sécurité nationale. Par la mise en place d'une surveillance de masse et l'attribution d'un cadre juridique pour l'exercice des activités de renseignement de l'État²⁸³, les législateurs américains et français ont souhaité renforcer la protection de leurs concitoyens respectifs. Cet objectif est d'ailleurs clairement évoqué dans l'exposé des motifs de la loi française relative au renseignement « *le renseignement permet de connaître et de prévenir les risques et les menaces pesant sur notre pays et sa population, ainsi que de mieux appréhender les grands enjeux auxquels ils sont confrontés. Par là-même, il participe de la garantie des droits des citoyens, qui dépend notamment de l'ordre public pour être pleinement assurée*²⁸⁴ ». La mise en place de la surveillance, par le renforcement des activités de renseignement étatique, semble donc *a priori* correspondre à une action rationnelle en finalité décrite par Weber.

2. La légitimation de la surveillance diffuse: action rationnelle ou réaction d'opportunisme ?

105. Pour atteindre l'objectif rationnel de sécurité et de protection, les législateurs américains et français ont édicté des lois sur la sécurité, la surveillance et le renseignement, qui ont été vues comme les moyens les plus efficaces pour atteindre ce but. Un bilan entre les coûts et les avantages recherchés a été imaginé par le gouvernement français afin d'anticiper les possibles conséquences de la loi sur le renseignement. Un premier indice de cette anticipation est palpable dans le cadre de l'exposé des motifs de la loi sur le renseignement : « *dans le contexte actuel, international aussi bien qu'intérieur, le renforcement de la politique du renseignement, dans le strict respect des*

²⁸² Loi n° 2015 – 912 du 24 juillet 2015 relative au renseignement, JORF n°0171 du 26 juillet 2015 page 12735, texte n°2, En ligne: <http://www.legifrance.gouv.fr/eli/loi/2015/7/24/PRMX1504410L/jo/texte> (dernière consultation: 5 mars 2018)

²⁸³ Le USA Patriot Act et la loi française sur le renseignement poursuivent le même objectif : augmenter les moyens techniques et juridiques attribués à la prévention des menaces à la sécurité nationale, à l'ordre public par l'organisation et la gouvernance de l'activité de renseignements.

²⁸⁴ Loi n° 2015-912 du 24 juillet 2015 relative au renseignement - Exposé des motifs, En ligne: https://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=AC82D0703DA2374DEF16BEA404A88989.tpdila23v_3?idDocument=JORFDOLE000030375694&type=expose&typeLoi=&legislature=14 (dernière consultation: 5 mars 2018)

*libertés individuelles, est nécessaire*²⁸⁵ ». Cette balance entre les coûts potentiels - le respect des libertés individuelles - et les avantages - le renforcement des activités de renseignement, et, par voie de conséquence, la sécurité - était déjà envisagé dans un rapport d'information présenté en 2013 sur le cadre juridique applicable aux services de renseignement²⁸⁶, mais également en 2014 dans le cadre du rapport d'activité de la délégation parlementaire au renseignement²⁸⁷. Ce dernier présente même les bénéfices majeurs d'un cadre juridique unifié de l'activité de renseignement : « *la France demeure en effet la seule démocratie occidentale à ne pas bénéficier d'un cadre juridique, laissant de ce fait nos services dans la plus parfaite indigence juridique (...). Un cadre unifié présentera trois bénéfices majeurs : consacrer les libertés individuelles (...), légitimer l'activité des services (...), protéger les agents de ces administrations régaliennes (...)*²⁸⁸ ». Si l'on peut aisément comprendre que le phénomène de surveillance puisse participer à ce que Weber décrit comme le désenchantement du monde par l'intellectualisation et la rationalisation des activités humaines, il est néanmoins nécessaire de nuancer le propos quant aux actions prises de manière isolée permettant le renforcement et la légitimation de la surveillance.

106. La loi française sur le renseignement²⁸⁹ est présentée par le gouvernement comme un aboutissement pour la politique publique du renseignement. A la lecture du dossier législatif de ce

²⁸⁵ Ibid.

²⁸⁶ URVOAS Jean-Jacques et VERCHERE Patrice, *Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, enregistrée à la présidence de l'Assemblée nationale le 14 mai 2013, En ligne: <http://www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf> (dernière consultation: 5 mars 2018). La page 13 de ce rapport est particulièrement éclairante sur cette balance entre les coûts et les avantages recherchés : « *alors qu'il compte parmi les plus anciennes des nations démocratiques, notre pays est également le dernier à ne pas avoir établi un cadre normatif adapté. (...). Vos rapporteurs ont donc souhaité réaliser un état des lieux de ces derniers, préalable à la formulation de préconisations visant à améliorer l'action de notre appareil de renseignement dans un cadre plus conforme aux standards d'une démocratie aboutie* ».

²⁸⁷ URVOAS Jean-Jacques, Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, En ligne: <http://www.assemblee-nationale.fr/14/pdf/rap-off/i2482.pdf>. (dernière consultation: 5 mars 2018)

²⁸⁸ Ibid. p. 65-66

²⁸⁹ Afin de démythifier ce texte de loi, le gouvernement a envisagé une réelle campagne « marketing » en présentant le « *vrai/faux du gouvernement sur le #PJL Renseignement* » (cf.: <http://www.gouvernement.fr/le-vraifaux-du-gouvernement-sur-le-pjlrenseignement> (dernière consultation: 5 mars 2018)). Aussi, fait assez exceptionnel, cette loi a été présentée à l'Assemblée Nationale directement par le Premier ministre, Manuel Valls. A cette occasion, il a tenu à démontrer l'importance de l'activité de renseignement: « *dans une démocratie, le renseignement est une activité exclusivement tournée vers la protection des citoyens et de leurs libertés* » (JORF, Assemblée Nationale XIVe législature, session ordinaire de 2014-2015, *Compte rendu intégral 1ère séance du Lundi 13 avril 2015*, p. 3977, En ligne: <http://www.assemblee-nationale.fr/14/pdf/cri/2014-2015/20150212.pdf> (dernière consultation: 5 mars 2018)). Et d'ajouter que : « *S'il fallait résumer ce projet de loi en quelques mots, on pourrait le faire ainsi : désormais, toute opération de surveillance régalienne menée en n'importe quel point du territoire national dans le cadre d'une mission de renseignement fera l'objet d'une autorisation hiérarchique extérieure au service, d'un contrôle approfondi par une autorité indépendante et d'un droit au recours juridictionnel effectif pouvant enjoindre au Gouvernement d'y mettre fin. Il s'agit là d'un progrès juridique et démocratique majeur* ». (in :Ibid, p. 3979).

texte, le juriste se retrouve face à une confusion des genres assez nettes. En vue de légaliser la surveillance, objectif non avoué²⁹⁰ mais réel de cette loi, le politique et le législateur ont mêlé l'émotionnel et l'opportunisme dans la lutte contre le terrorisme. D'une part, s'il est vrai que le projet de loi sur le renseignement était en préparation depuis plus d'une année²⁹¹, on notera tout de même que la décision du 19 mars 2015, prise en conseil des ministres, de l'inscrire à l'ordre du jour de l'Assemblée Nationale, soit seulement deux mois après les attentats des 7 et 9 janvier 2015, a pu contribuer à faire peser une suspicion d'opportunisme sur le pouvoir exécutif, renforcée par le choix de la procédure accélérée²⁹². D'autre part, ce contexte a sans doute été préjudiciable à l'exigence de

²⁹⁰ La campagne marketing du gouvernement vise à lutter activement contre l'idée d'une mise en place d'une surveillance massive des données sur internet (point 2), d'un dispositif massif d'interception des conversations privées (point 3), mais également contre l'idée d'un champ des finalités justifiant le recours aux techniques de renseignement trop large (point 6) en se justifiant par la même précision avec laquelle il est venu décrire la notion de sécurité nationale. Selon le gouvernement, « l'énumération des finalités permet de dire précisément dans quels domaines les mesures de surveillance sont possibles, et dans quels domaines elles sont interdites. (...). C'est donc un moyen de renforcer le contrôle. La France se distingue de ses voisins, qui emploient des notions beaucoup plus larges. Le projet de loi est même plus précis que la Convention européenne des droits de l'Homme, qui prévoit que les motifs pouvant justifier une ingérence dans la vie privée sont « la sécurité nationale, la sûreté publique, le bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui ». Or, à la lecture de la loi n° 2015 – 912 du 24 juillet 2015 relative au renseignement, le juriste connaîtra quelques difficultés à parvenir à un avis aussi tranché. La pertinence de cette loi, ainsi que de la campagne de publicité du gouvernement y afférente, pourront également être mise en doute au regard de la notion d'interception de sécurité dite « administrative » issue de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications (JORF n°162 du 13 juillet 1991 p. 9167, En ligne: http://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000173519 (dernière consultation: 5 mars 2018)).

²⁹¹ Selon le Premier Ministre: « si cette loi tient compte du contexte le plus récent, elle n'est en rien une réponse préparée dans l'urgence. Elle a été mûrement réfléchi, (...). La décision de légiférer avait été prise en conseil de défense par le Président de la République dès juillet 2014 ». In. JORF, Assemblée Nationale XIVe législature, session ordinaire de 2014-2015, 1ère séance du Lundi 13 avril 2015, compte rendu intégral, p. 3978, En ligne: <http://www.assemblee-nationale.fr/14/pdf/cri/2014-2015/20150212.pdf> (dernière consultation: 5 mars 2018)

²⁹² Ce choix a d'ailleurs été vivement critiqué par plusieurs députés à l'Assemblée Nationale. Les griefs se sont concentrés sur le temps de parole réduit (deux minutes). Ce rythme imposé par le choix de la procédure accélérée, ne permettait pas, selon certains députés « un examen réellement apaisé et approfondi » que méritait « un tel projet par respect pour le peuple », que les députés représentent (in., JORF, Assemblée Nationale XIVe législature, session ordinaire de 2014-2015, 1ère séance du Lundi 13 avril 2015, compte rendu intégral, p. 3993, En ligne: <http://www.assemblee-nationale.fr/14/pdf/cri/2014-2015/20150212.pdf> (dernière consultation: 5 mars 2018)). Cette opinion a d'ailleurs été partagée par M. Pierre Lellouche qui déplorait « le choix du gouvernement d'imposer la procédure accélérée pour l'examen de ce texte. (...). De même, je n'ai que deux minutes pour vous parler de l'article 1er (...), qui est un texte compliqué, composé de plusieurs chapitres et à l'architecture complexe. Je n'aurai pas le temps de dire ce que je voulais dire, ce qui est extrêmement frustrant. Mettez-vous à la place de l'opposition : ce n'est pas une façon correcte de travailler » (in., JORF, Assemblée Nationale XIVe législature, session ordinaire de 2014-2015, 2ème séance du Lundi 13 avril 2015, compte rendu intégral, p. 4019, En ligne : <http://www.assemblee-nationale.fr/14/pdf/cri/2014-2015/20150213.pdf> (dernière consultation: 5 mars 2018)). Les attaques liées à la procédure accélérée se sont ensuite fixées sur la complexité du texte de loi et des questions fondamentales qu'il sous-tend en matière de balance entre sécurité et libertés fondamentales. On peut ainsi lire : « La complexité de cette question et la nature même des activités de renseignement méritent un débat de fond, un débat à la hauteur de l'enjeu. C'est la raison pour laquelle nous déplorons le recours à la procédure accélérée. Pourquoi y recourir sur ce texte très technique ? (...) D'autant plus qu'une question fondamentale est posée : celle de la protection des libertés publiques de nos concitoyens. Tout l'enjeu consiste à concilier la nécessité d'assurer la sécurité et le devoir de préserver les droits et libertés » (in., JORF, Assemblée Nationale XIVe législature, session ordinaire de 2014-2015, 1ère séance du Lundi 13 avril 2015, compte rendu intégral, p. 3993). Ou encore : « Nous sommes en guerre contre des ennemis qui ont juré de nous détruire, des ennemis qui kidnappent, violent, tuent. C'est une lutte à mort, une lutte pour la survie de chacun de nos concitoyens, de notre nation, de nos grandes démocraties. C'est tout simplement une lutte pour la sauvegarde de notre civilisation. (...) Oui, j'estime que ce texte ne va pas suffisamment loin. Je le dis avec gravité, il faut d'urgence renoncer à certaines libertés pour sauvegarder la liberté » (in., Ibid., p. 4002).

rigueur et de clarté juridique tant sur la forme de cette loi que sur le fond²⁹³. Ces éléments tendent alors à infirmer la rationalité de l'action menée par le législateur français pour donner un cadre juridique aux activités de renseignement. Cette action se rapproche plutôt de la catégorie que Weber décrit comme action affectuelle, déterminée par la soudaineté incontrôlable de l'affect, d'une pulsion, et ici, d'une forme d'opportunisme politique.

107. La lecture des déclarations de M. Pierre Lellouche en séance publique à l'Assemblée Nationale le 13 avril 2015 confirme ce propos. Ce membre de l'opposition déclare ainsi que : « *rien n'est plus dangereux dans une démocratie que les lois de circonstance – surtout lorsqu'il s'agit de lois d'exception –, prises sous le coup de l'émotion. Seulement trois mois après le grave traumatisme subi par notre pays, et alors que nos soldats patrouillent encore dans les rues des grandes villes, voilà que nous discutons d'un texte majeur qui a un impact, qu'on le veuille ou non, sur les libertés publiques*²⁹⁴ ». Cette action, ou plutôt cette réaction du législateur français a permis le renforcement de la surveillance, entendue ici comme phénomène. Grâce à ces réactions d'opportunisme, la vertu a fait place à l'efficacité et l'on permet la primauté des moyens sur les réelles finalités nécessitant alors une adaptation inévitable des individus. Or, comme le rappelle Max Weber, hormis les hommes de science, les individus n'ont qu'une connaissance très limitée des objets techniques qu'ils utilisent, il leur suffit de pouvoir « compter » sur eux. En effet, « *il ne s'agit plus pour nous, comme pour le sauvage qui croit à l'existence de ces puissances, de faire appel à des moyens magiques en vue de maîtriser les esprits ou de les implorer mais de recourir à la technique et à la prévision. Telle est la signification essentielle de l'intellectualisation*²⁹⁵ ».

Section 2: Approche pragmatique et démythifiée de la diffusion de la surveillance: un phénomène global et banalisé

108. L'approche technophile de la surveillance diffuse a permis de mettre en exergue les discours de légitimation sécuritaire, de prévention des risques et des menaces. L'approche technophobe a, quant à elle, mis en évidence le potentiel de nuisance sur nos sociétés du progrès, et par là, de la

²⁹³ On relèvera l'imprécision du législateur quant au domaine même du renseignement, ainsi que l'incertitude qui entoure les pratiques et les finalités du renseignement.

²⁹⁴ JORF Assemblée Nationale XIV^e législature, session ordinaire de 2014-2015, Séances du Lundi 13 avril 2015, compte rendu intégral, 2^eme séance du lundi 13 avril 2015, p. 4019, En ligne: <http://www.assemblee-nationale.fr/14/pdf/cr/2014-2015/20150213.pdf> (dernière consultation: 5 mars 2018)

²⁹⁵ WEBER Max, *Le savant et le politique*, Op. Cit., 1963, p. 90.

surveillance. Rationalisation et désenchantement du monde sont au coeur de cet analyse. Bien que l'on puisse ou non partager ces analyses, il n'en reste pas moins que ces deux courants de pensées ont permis le passage de la surveillance du simple fait social à un phénomène recouvrant de plus en plus une traduction juridique. Les premières législations informatiques et libertés lui ont donné une assise juridique. Sa filiation au phénomène technique a facilité sa propagation dans les sociétés contemporaines.

109. D'un point de vue pragmatique pourtant, ces seuls éléments ne permettent pas de comprendre la globalisation de la surveillance (paragraphe 1), ni même sa banalisation croissante (paragraphe 2).

Paragraphe 1: De la globalisation de la surveillance dictée par un impératif ancien: l'information une source de pouvoir ...

110. Depuis les années 60-70, la mise en place d'une société caractérisée par la communication, le savoir, la connaissance, et par des technologies permettant de véhiculer ces informations ne cesse de se développer. Le succès de la notion de société d'information est en partie liée à sa conception: la troisième révolution industrielle. En parallèle, depuis une quinzaine d'années, de nombreuses voix s'élèvent sur la scène internationale et nationale²⁹⁶ afin de mettre en garde contre son « *envers diabolique*²⁹⁷ » : la société de surveillance. Pourtant cette nouvelle société n'est ni plus ni moins que le prolongement de la société de l'information (A). Certes, la surveillance s'est globalisée, mais elle prospère grâce au même carburant : l'information et les nouvelles technologies. Notre époque est caractérisée par ce nouvel impératif: l'information c'est le pouvoir. Dès 1996, Joseph Nye, professeur de relations internationales écrivait: « *la connaissance plus que jamais, c'est le pouvoir. Le pays qui conduira le mieux la révolution de l'information sera plus puissant que tout autre. Dans un avenir prévisible, ce pays c'est les Etats-Unis. (...). En vérité le 21ème siècle, et non le 20ème, se révélera un jour comme ayant été la période de la suprématie américaine. L'information est la nouvelle monnaie sur la scène internationale, et les Etats-Unis sont mieux positionnés que*

²⁹⁶ De manière non exhaustive, on citera la thématique de la 28ème Conférence internationale des commissaires à la protection des données personnelles et à la vie privée du 2 et 3 novembre 2006 intitulée : une société de surveillance ? (Communiqué de la conférence En ligne: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/06-11-03_London_Communique_EN.pdf (dernière consultation: 5 mars 2018)), ou encore le 27ème Rapport d'activité de la CNIL de 2006 (En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000422.pdf> (dernière consultation: 5 mars 2018)) qui s'ouvre avec cette mise en garde : « *alerte à la société de surveillance* ».

²⁹⁷ FOREST David, Op. Cit.

*n'importe quel autre pays...*²⁹⁸ ». C'est donc bien la notion même d'information qu'il faut comprendre et saisir pleinement pour appréhender le passage de la société de l'information à la banalisation de la surveillance diffuse. Le principe de libre circulation de l'information et la doctrine américaine du free flow of information sont alors des éléments juridiques structurant de la société de l'information mais également de la surveillance (B).

A. L'édification de la société de l'information comme prélude à la surveillance diffuse

111. « *Rome ne s'est pas faite en un jour* », et la surveillance diffuse n'a pas surgit de nulle part, tel un pop-up²⁹⁹ non sollicité. Outre son agrégation³⁰⁰ à la technique, la surveillance diffuse a également une filiation forte avec la notion de réseaux et d'informations, le concept de communication et les théories y afférentes (1). Dans la conception de la société de l'information, ces différents termes sont fondamentaux et permettent de comprendre en quoi l'information représente un enjeu de pouvoir et de domination à l'international (2). Cette affirmation reste toujours d'actualité dans le cadre du siècle de la surveillance diffuse.

1. Les théories de l'information et de la communication: fondement de la construction de la future société de l'information

112. La société de l'information n'est pas un concept récent. Dès les années 50, Norbert Wiener prédit l'avènement de cette société fondée sur la circulation de l'information, condition d'un nouvel exercice de la démocratie³⁰¹. Rappeler l'héritage de Wiener, et son concept de cybernétique³⁰² peut

²⁹⁸ NYE Joseph, OWENS William, « America's Information edge », in *Foreign Affairs*, Mars 1996, pp. 20-36, p. 20 et p. 35, En ligne: <http://www.unz.org/Pub/ForeignAffairs-1996mar> (dernière consultation: 5 mars 2018) (traduction libre de l'auteur des lignes suivantes : « *Knowledge more than ever before, is power. The one country that can best lead the information revolution will be more powerful than any other. For the foreseeable future, that country is the United States. (...). In truth, the 21st century, not the twentieth, will turn out to be the period of America's greatest preeminence. Information is the new coin of the international realm, and the United States is better positioned than any other country (...).* »

²⁹⁹ Un pop-up est une fenêtre qui surgit et s'affiche de manière intrusive et non sollicitée devant la page web consultée par l'utilisateur d'un navigateur.

³⁰⁰ Plus qu'une affiliation, la surveillance diffuse s'est agrégée au phénomène technique, c'est-à-dire que la technique et la surveillance se sont assemblées en un tout devenu aujourd'hui homogène.

³⁰¹ Pour confirmer ces propos, voir : WIENER Norbert, *Cybernétique et société : L'usage humain des êtres humains*, Collection Points Sciences, Points, 2014

³⁰² Cette notion dérive du mot grec *kubernêtikê*, qui signifie l'art de gouverner. Platon, dans son oeuvre *Le Politique*, utilise cette notion comme une métaphore. En effet, ce terme employé pour désigner le pilote d'un navire, est utilisé par Platon pour décrire l'art véritable de gouverner, ou sciences du gouvernement des hommes.

paraître superflu tant cette notion semble être assimilée dans la culture du 21^{ème} siècle, sans pour autant jamais la nommer clairement. Envisagée par son auteur comme une science dédiée à la recherche des lois générales de communication et à leurs applications techniques, la cybernétique renvoie aujourd'hui aux expressions générales de cyberspace³⁰³, de nouvelles technologies de l'information et de la communication, de numérique, et à des domaines recouvrant l'informatique, la biologie, les sciences du comportement, l'intelligence artificielle. En quelque sorte, l'ensemble des mutations structurelles, technologiques, culturelles, sociétales et humaines de la société actuelle a été permis grâce à cette notion, comme participant de la construction d'une vision nouvelle du monde. Souligner le rôle prépondérant de ce concept dans l'avènement de la société de l'information et, par voie de conséquence, dans l'apparition de la globalisation de la surveillance diffuse, permet de comprendre la relation entre ces deux conceptions sociales et les notions de communication et d'information.

113. C'est d'abord dans les sciences sociales, et spécialement dans les théories de la communication qu'il faut tenter d'appréhender ces notions. Si le 19^{ème} siècle a permis l'invention des systèmes techniques permettant à la communication de voir le jour, les théories économiques du libre échange, du laissez faire et de « la main invisible » chères à Adam Smith ont quant à elles permis de prendre la mesure économique de la circulation de l'information. Ainsi que le rappellent Armand et Michèle Mattelart, « *d'abord centrée sur la question des réseaux physiques et projetée au coeur même de l'idéologie du progrès, la notion de communication a englobé à la fin du siècle la gestion des multitudes humaines. La pensée de la société comme organisme, comme ensemble d'organes s'acquittant de fonctions déterminées, inspire les premières conceptions d'une « science de la communication »*³⁰⁴ ». Ainsi, la communication se caractérise par deux éléments fondateurs : les réseaux physiques - aspects technologiques, la technique, le progrès - qui permettent une nouvelle organisation sociale fondée sur la communication - « *la gestion des multitudes humaines* », ou pour reprendre les termes de Saint-Simon une organisation sociale passant du « gouvernement

³⁰³ En 1994, Pierre Lévy, dans son ouvrage intitulé : *L'intelligence collective – Pour une anthropologie du cyberspace*, reprend la première définition de ce terme donné par William Gibson, et l'enrichit. Ainsi le cyberspace y est envisagé comme suit : « *Cyberspace : mot d'origine américaine, employé pour la première fois par l'écrivain de science-fiction William Gibson en 1984 dans le roman Neuromancien. Le cyberspace y désigne l'univers des réseaux numériques comme lieu de rencontres et d'aventures, enjeu de conflits mondiaux, nouvelle frontière économique et culturelle. Il existe dans le monde un foisonnement de courants littéraires, musicaux, artistiques, voire politiques se réclamant de la « cyberculture ».* Le cyberspace désigne moins les nouveaux supports de l'information que les modes originaux de création, de navigation dans la connaissance et de relation sociale qu'ils permettent », in. LEVY Pierre, *L'intelligence collective – Pour une anthropologie du cyberspace*, Collection Sciences et Société, Editions La Découverte, 1994, p. 119.

³⁰⁴ MATTELART Armand et Michèle, *Histoire des théories de la communication*, 3^{ème} édition, Collection Repères, Editions La découverte, Paris, 2004, p.5.

des hommes à l'administration des choses³⁰⁵ »

114. Retraçant l'histoire des théories de la communication, Armand et Michèle Mattelart dressent un parallèle intéressant entre le concept de communication et la division du travail théorisée par Adam Smith³⁰⁶, ainsi qu'avec les nouveaux moyens de communication que la révolution industrielle a fait apparaître dans les sociétés occidentales. Selon ces auteurs, la division du travail, en légitimant la mécanisation des opérations du travail et de l'intelligence³⁰⁷, a créé de nouvelles voies de communication (fluviales, maritimes et terrestres) permettant à une économie des flux et des échanges de se développer dans une société en réseau, devenue une « *totalité organique*³⁰⁸ ». Et ainsi d'ajouter, « *de l'homogène à l'hétérogène, du simple au complexe, de la concentration à la différenciation, la société industrielle incarne la « société organique ». (...) Dans ce tout-système, la communication est une composante de base des deux « appareils d'organes », le distributeur et le régulateur. A l'image du système vasculaire, le premier (routes, canaux et chemins de fer) assure l'acheminement de la substance nutritive. Le second assure l'équivalent de la fonction du système nerveux. Il rend possible la gestion des relations complexes d'un centre dominant avec sa périphérie. C'est le rôle des informations (presse, pétitions, enquêtes) et de l'ensemble des moyens de communication par lesquels le centre peut « propager son influence » (postes, télégraphe, agence de presse)*³⁰⁹ ».

115. Cette citation est essentielle pour appréhender les répercussions de la notion de communication et ses théories sur son prolongement : la société de l'information. A travers ces lignes, il est, en effet, aisé de comprendre la relation entre la communication et l'information, ainsi

³⁰⁵ Claude Henry de Rouvroy, comte de Saint-Simon, philosophe et économiste français (1760-1825). Saint-Simon et ses disciples ont fortement participé à théoriser la société industrielle et ses conséquences sociales.

³⁰⁶ On peut ainsi lire: « *la « division du travail » représente un premier pas théorique. il faut remonter à la fin du XVIII ème pour en trouver chez Adam Smith la première formulation scientifique. La communication contribue à l'organisation du travail collectif au sein de la fabrique et dans la structuration des espaces économiques. Dans la cosmopolis commerciale du laissez-faire, la division du travail et les moyens de communication (voies fluviales, maritimes et terrestres) riment avec opulence et croissance* ». Et de conclure: « *l'Angleterre a déjà fait sa « révolution de la circulation »; celle-ci commence à s'intégrer naturellement au nouveau paysage de la révolution industrielle en cours* ». MATTELART Armand et Michèle, *Histoire des théories de la communication*, 3ème édition, Collection Repères, Editions La découverte, Paris, 2004, p.5.

³⁰⁷ Les réflexions de Charles Babbage (1792-1871), mathématicien, cryptanalyste et inventeur britannique, concernant la machine analytique, sont notamment mentionnées par Armand et Michèle Mattelart (Op. Cit. p.6) comme étant représentatives de l'élaboration d'une « *division du travail mental* » et participant à l'élaboration des projets de « *mécanisation des opérations de l'intelligence* ».

³⁰⁸ Ibid.

³⁰⁹ Ibid. p. 7

que de deviner les contours de ce que sous-tend la notion de société de l'information. La communication permet la circulation, le flux de marchandises, de services, de biens, d'hommes, de capitaux et d'informations. Elle est à la fois moyens et finalités. Dans cette nouvelle organisation sociale, l'information joue le rôle de pont, de liens entre ces moyens et cette finalité et devient alors un véritable enjeu de pouvoir.

2. L'information : un enjeu de pouvoir et de domination à l'international

116. D'un point de vue juridique, les notions de communication et d'information n'ont pas réellement de contour sémantique. Le glossaire des synthèses de la législation de l'Union européenne décrit par exemple le terme « société de l'information » comme faisant « *référence à une société dont une grande partie des activités se concentre sur la création, la distribution, l'utilisation et la réutilisation de l'information. Ces activités sont réalisées grâce à ce que l'on appelle les « technologies de l'information et de la communication » (TIC)³¹⁰ »*. Il faut d'emblée conclure à la faiblesse de cette définition qui n'aborde pas la notion d'information, tout en en faisant la caractéristique principale de la société actuelle. En effet, s'inscrivant dans la continuité de la société de l'information, la surveillance reprend cette caractéristique fondamentale.

117. Selon Wiener, l'information « *est le nom pour désigner le contenu de ce qui est échangé avec le monde extérieur à mesure que nous nous y adaptons et que nous lui appliquons les résultats de notre adaptation. Le processus consistant à recevoir et à utiliser l'information est les processus que nous suivons pour nous adapter aux contingences du milieu ambiant et vivre dans ce milieu. (...). Vivre, c'est vivre avec une information adéquate. Ainsi, la communication et la régulation concernent l'essence de la vie intérieure de l'Homme, même si elles concernent sa vie en société³¹¹ »*. A travers ces lignes, l'auteur opère une liaison assez prophétique et descriptive de la

³¹⁰ La définition se poursuit par quelques mises en garde: « *Le recours à ces TIC, l'essor de l'internet ainsi que l'ouverture des marchés des télécommunications ont révolutionné le quotidien des citoyens européens au cours des vingt-cinq dernières années. Elles offrent des nouvelles opportunités comme le télétravail, l'éducation et la santé en ligne pour n'en citer que quelques-unes. La société de l'information comporte, cependant, quelques inconvénients. Des mesures doivent être prises pour faire face à de nouvelles formes de criminalité, comme la cybercriminalité, ainsi que pour répondre aux problèmes de protection des données et de violation de la propriété intellectuelle. Il convient également de remédier à ce que l'on désigne comme la « fracture numérique »: la différence entre ceux qui sont équipés pour participer à la société de l'information et ceux qui ne le sont pas. L'agenda numérique, l'une des priorités phares de la stratégie Europe 2020 pour générer une croissance intelligente, durable et inclusive, vise à aider les citoyens et les entreprises de l'Union européenne à tirer le meilleur parti possible de la révolution numérique »*. Glossaire des synthèses de la législation de l'Union Européenne, *Société de l'information*, http://eur-lex.europa.eu/summary/glossary/information_society.html?locale=fr (dernière consultation: 5 mars 2018)

³¹¹ WIENER Norbert, *Cybernétique et société : L'usage humain des êtres humains*, Collection Points Sciences, Points, 2014, p. 89- 90

société contemporaine dominée par la surveillance diffuse. La société actuelle est dominée par l'ambition d'une mise en donnée (personnelle ou non) du monde, des individus, de leurs activités et des faits sociaux, en vue de réduire ces éléments à des chiffres, des mesures, des éléments statistiques et quantifiables³¹². Aujourd'hui, pour bien vivre et de manière efficiente, il faut être informé, et obtenir la bonne information pour un but défini. En cela, l'information ne doit pas être réduite à la seule liberté d'information, au droit à l'information, à la liberté d'expression, ou encore à la liberté de la presse. Elle doit bien plutôt être considérée comme un contenu, un moyen, un but, une action, mais également une activité économique (dans le sens du marché économique). L'information est, en effet, envisagée comme l'action d'informer, de porter à la connaissance, de tenir au courant, d'indiquer, de renseigner, de donner des précisions à quelqu'un à propos d'événements, de jugements ou de faits, par différents moyens (sons, images, discours, textes, ...). Elle est également, dans son sens informatique³¹³, l'élément de connaissance susceptible d'être représenté à l'aide de conventions pour être collecté, traité, diffusé ou communiqué. Elle devient de fait une activité économique, un marché, puisque sa mise en mémoire, sa communication, sa diffusion et son traitement sont nécessaires à l'activité informatique, puis plus largement à la surveillance. Elle est comme le rappelait Wiener tout ce qui peut être échangé avec le monde extérieur³¹⁴ et constitue dès lors une enjeu de pouvoir, de domination économique et politique.

118. L'apparition dans les années 80 du droit de l'informatique et des réseaux devenant progressivement le droit des nouvelles technologies de l'information et de la communication, témoigne de la prise en compte de cet enjeu. Sous l'angle européen, on évoquera l'ensemble des

³¹² Ainsi que Mattelart le décrit, « *l'idée d'une société régie par l'information est pour ainsi dire inscrite dans le code génétique du projet de société inspiré par la mystique du nombre. Elle date donc de bien avant l'entrée de la notion d'information dans la langue et la culture de la modernité. Ce projet qui prend forme au cours du XVII^e et du XVIII^e siècle intronise la mathématique comme modèle du raisonnement et de l'action utile. La pensée du chiffrable et du mesurable devient le prototype de tout discours vrai en même temps qu'elle instaure l'horizon de la quête de la perfectibilité des sociétés humaines* ». MATTELART Armand, *Histoire de la société de l'information*, 4^e édition, Collection Repères, Editions La découverte, 2009, p. 5. L'auteur poursuit sa pensée d'une société fondée sur « *la culture du nombre* » et déclare que le « *moment fort de la matérialisation de la langue des calculs, la Révolution française en fait l'aune de l'égalité citoyenne et des valeurs de l'universalisme* ».

³¹³ L'Académie française envisage la notion d'informatique comme suit: nom féminin et adjectif (XX^e ème siècle). Dérivé d'information sur le modèle de mathématique, électronique. Dans un sens premier: science du traitement rationnel et automatique de l'information; l'ensemble des applications de cette science. Ce sens n'est pas sans rappeler la description d'Armand Mattelart de la société fondée sur la culture du nombre, participant à la rationalisation des activités humaines. Dans un second sens, (adjectif), il faut entendre par là tout ce qui se rapporte à l'informatique: *système informatique*, ensemble des moyens qui permettent de conserver, de traiter et de transmettre l'information; *programme informatique*; *réseau informatique*, ensemble de systèmes informatiques communiquant entre eux par voies locales, privées ou publiques. *Traitement informatique des données, matériel informatique, fichier informatique, les divers langages informatiques*. (Eléments de définitions issus du dictionnaire de l'Académie française)

³¹⁴ Allant de l'économie à la finance, aux assurances et à la comptabilité, à la culture alimentée par les produits et services des industries culturelles, et à la connaissance.

dynamiques à l'oeuvre, dans les années 2000, en matière de commerce électronique et de propriété intellectuelle. La directive 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 intérieur³¹⁵, et la directive du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (DADVSI³¹⁶) en sont des exemples parfaits. Les logiques à l'oeuvre dans la création de ces directives sont sensiblement les mêmes que lors de la création des premières législations informatiques et libertés. Les considérants de la directive DADVSI, par exemple, démontrent l'ambition des institutions européennes de créer un cadre juridique suffisamment souple et général afin de favoriser le développement de la société de l'information³¹⁷ dans une logique globale de marché économique³¹⁸. La notion récente de marché unique numérique reconnu par le Conseil Européen dès 2013³¹⁹ tend à confirmer ce propos tant par le choix des mots de cette expression que par les buts poursuivis par la Commission Juncker³²⁰.

³¹⁵ 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 »), Journal officiel n° L 178 du 17 juillet 2000, p. 0001 – 0016, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2000:178:TOC> (dernière consultation: 5 mars 2018)

³¹⁶ 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*, Journal officiel n° L167 du 22 juin 2001, p. 0010 – 0019, En ligne: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2001.167.01.0010.01.FRA&toc=OJ:L:2001:167:TOC (dernière consultation: 5 mars 2018)

³¹⁷ Le considérant n°2 de la directive de 2001 précise que : « *Le Conseil européen de Corfou des 24 et 25 juin 1994 a souligné la nécessité de créer un cadre juridique général et souple au niveau de la Communauté pour favoriser le développement de la société de l'information en Europe. Cela suppose notamment l'existence d'un marché intérieur pour les nouveaux produits et services. (...) Le droit d'auteur et les droits voisins jouent un rôle important dans ce contexte, car ils protègent et stimulent la mise au point et la commercialisation de nouveaux produits et services, ainsi que la création et l'exploitation de leur contenu créatif* ».

³¹⁸ Cette logique économique est forcément très induite par la « directive commerce électronique » précitée et se ressent très fortement dans la dynamique de protection des droits d'auteur et droits voisins, Cf. considérant 6: « *(6) En l'absence d'harmonisation à l'échelle communautaire, les processus législatifs au niveau national, dans lesquels plusieurs États membres se sont déjà engagés pour répondre aux défis technologiques, pourraient entraîner des disparités sensibles en matière de protection et, partant, des restrictions à la libre circulation des services et des marchandises qui comportent des éléments relevant de la propriété intellectuelle ou se fondent sur de tels éléments, ce qui provoquerait une nouvelle fragmentation du marché intérieur et des incohérences d'ordre législatif* ».

³¹⁹ Dès octobre 2013, les dirigeants de l'Union européenne appellent à la création d' « *une économie numérique forte est vital pour la croissance et la compétitivité européenne dans un monde globalisé* ». Secrétariat Général du Conseil européen, EUCO 169/13, CO EUR 13, CONCL 7, *Conclusions du Conseil Européen des 24 et 25 octobre 2013*, Bruxelles, 25 octobre 2013, p. 1, En ligne: <http://data.consilium.europa.eu/doc/document/ST-169-2013-INIT/en/pdf> (dernière consultation: 5 mars 2018)

³²⁰ Le marché unique numérique vise la consolidation d'un marché économique fondée sur l'information, en ce compris les données personnelles, la connaissance, et la création d'entreprises permettant la circulation de biens, de savoirs, de marchandises, et, en filigrane, la garantie des droits et libertés fondamentales. Les objectifs définis: « *conclure rapidement les négociations sur des règles européennes communes en matière de protection des données; donner plus d'ambition à la réforme des règles en matière de télécommunications qui est en cours; de modifier, simplifier et clarifier les règles régissant les droits d'auteur afin de tenir compte des nouvelles technologies; simplifier les règles de protection des consommateurs pour les achats en ligne; faciliter la création d'entreprise afin de favoriser l'innovation; renforcer l'apprentissage et les compétences dans le domaine du numérique; permettre l'accès aux mêmes services et contenus en ligne dans tous les pays de l'Union européenne* » (https://ec.europa.eu/priorities/digital-single-market_fr (dernière consultation: 5 mars 2018)).

119. Cette logique globale de marché économique touche également la notion de donnée personnelle. Les premières législations informatiques et libertés du continent européen, et spécialement la loi française de 1978, permettent à l'information de devenir un élément de la personnalité des individus. La loi n° 78-17 du 6 Janvier 1978 évoquent la notion « d'informations nominatives³²¹ », ou encore que la notion de donnée à caractère personnel, dans la modification de la loi informatique et liberté de 2004, est définie comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres*³²² », mais également comme l'entend l'article 2 de la directive 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 données³²³: « *toute information concernant une personne physique identifiée ou identifiable* ». La donnée personnelle, telle que conçue dans les premières législations informatiques et libertés, doit donc être envisagée comme une information bénéficiant d'une protection spécifique au titre du droit au respect de la vie privée de la personne fichée, d'un attribut de la personnalité. Dans cette optique, le droit des données personnelles pouvait être considéré comme une entrave au marché de l'informatique et de l'information. Tel n'est plus le cas aujourd'hui³²⁴.

B. La doctrine du free flow of information et la libre circulation de l'information: des mécanismes juridiques au service de la globalisation de la surveillance

120. Bien que les notions d'information et de communication ne soient pas définies en tant que telles par le droit, elles engendrent des conséquences et des forces juridiques bien présentes. La reconnaissance de la libre circulation de l'information, ainsi que la doctrine du free flow of information (2) représentent l'aboutissement de la reconnaissance de la valeur marchande de l'information, au coeur de la construction de la société de l'information, et structurant la diffusion

³²¹ Article 4 et 5 de la loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 janvier 1978, page 0027

³²² Article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers, et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2001, JORF 7 Août 2004

³²³ 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*, Journal officiel n° L 281 du 23 novembre 1995, p. 0031 - 0050, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046> (dernière consultation: 5 mars 2018)

³²⁴ Voir en ce sens: Partie 2, Titre 1, Chapitre 1 et 2

de la surveillance. Ces doctrines ont été fortement influencées par le rôle d'institutions particulières tels que l'UNESCO prônant la circulation libre et équilibrée de l'information (1).

1. Le rôle de l'UNESCO dans la reconnaissance d'une circulation libre et équilibrée de l'information

121. L'UNESCO a largement contribué à théoriser les logiques ultra-libérales sous entendues par le nouvel ordre mondial de l'information et de la communication³²⁵ et la société de l'information³²⁶. L'ambition d'une « *circulation libre et équilibrée* » de l'information³²⁷, prémices d'une libre circulation de l'information, apparaît en effet très tôt dans la doctrine de cette institution internationale. A l'origine envisagée comme une consécration de la liberté d'opinion et d'expression de l'article 19 de la Déclaration Universelle des Droits de l'Homme³²⁸, la circulation libre et équilibrée de l'information devient très vite synonyme de reconnaissance d'un marché économique

³²⁵ En 1977, l'UNESCO décide de la création d'une commission internationale d'étude sur les problèmes de communication dirigée par Sean Mac Bride. Ayant pour mandat d'établir « *une synthèse des problèmes de la communication et de leur solution possible* », cette commission contribuera à l'apparition de la société de l'information, à travers une autre dénomination: le nouvel ordre mondial de l'information et de la communication. Voir: UNESCO, *Allocution de M. Amadou - Mahtar M'bow, Directeur général de l'UNESCO à l'ouverture de la Commission Internationale d'étude sur les problèmes de communication*, Paris, 14 décembre 1977, DG/77/15, p 2, En ligne: <http://unesdoc.unesco.org/images/0002/000290/029029fb.pdf> (dernière consultation: 5 mars 2018). Au titre des pistes de réflexion de cette commission, l'une des demandes du Directeur général attire l'attention: « *les principales directions de travail et réflexion (...) à savoir: (...); (c) analyser les problèmes de la communication, sous leurs différents aspects, dans la perspective de l'établissement d'un nouvel ordre économique international et des initiatives à prendre pour favoriser l'instauration de ce que l'on pourrait appeler « un nouvel ordre mondial de l'information ».*

³²⁶ Dans le cadre d'un rapport remis à l'UNESCO, Herbert Schiller évoque particulièrement l'enjeu du contrôle de l'information, et la domination des Etats-Unis sur ce marché économique. La conclusion de ce rapport décalre: « *ce qui est en jeu n'est rien de moins que la continuité de la rentabilité du système mondial d'affaires des Etats-Unis. Les mécanismes complexes de composition et de transmission de messages, ainsi que la machinerie de persuasion et de contrôle des consciences, sont ce qui permet au système mondial de fonctionner. (...). Quand la pression pour un nouvel ordre mondial de l'information arrive à ce niveau, ce n'est plus une question d'information. C'est une question de transformation sociale. Il reste encore à déterminer si c'est dans cette direction que le défi est lancé* » in. SCHILLER Herbert, *La communication suit le capital*, UNESCO - Commission internationale d'étude des problèmes de la communication, n°47, 1978, p. 14, En ligne: <http://unesdoc.unesco.org/images/0003/000342/034210fb.pdf> (dernière consultation: 5 mars 2018). Voir également: SCHILLER Herbert, *Communication and cultural domination*, White Plains, New York, International Arts and Sciences Press, 1976.

³²⁷ Ce concept apparaît dans la *Résolution de la Conférence générale de l'UNESCO, 19 C/Résolution 4.126*, in Records of the General Conference, Nineteenth Session, Nairobi, du 26 octobre au 30 novembre 1976, Volume 1 Résolutions, p. 21 : « *Promotion of a free and balanced flow of information and of international exchanges* », En ligne: <http://unesdoc.unesco.org/images/0011/001140/114038E.pdf> (dernière consultation: 5 mars 2018)

³²⁸ Dans l'allocution précitée, le directeur déclare en effet: « *Nous ne pouvons ignorer (...) le grand débat qui s'est instauré, ces dernières années, avec une ampleur nouvelle, autour du thème de la « circulation libre et équilibrée de l'information ».* J'ai eu l'occasion d'affirmer, à plusieurs reprises, l'importance qui me paraît s'attacher à donner son plein effet à l'article 19 de la Déclaration Universelle des Droits de l'Homme qui stipule - je cite - que: « *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 rechercher, de recevoir et de répandre, sans considération de frontière, les informations et les idées par quelque moyen d'expression que ce soit* ». Parmi les droits et les libertés politiques qui constituent l'un des biens les plus précieux dont peuvent jouir les hommes, la liberté de l'information apparaît certes comme fondamentale, et donc sa garantie est essentielle ». UNESCO, *Allocution de M. Amadou-Mahtar M'bow Op. Cit.*, p. 4

pour les Etats-Unis³²⁹. Il suffit de citer un rapport de 1978 rendu au nom de la Commission internationale d'étude des problèmes de la communication intitulé: observations sur la relation entre le nouvel ordre international de l'information et le nouvel ordre économique international³³⁰. L'auteur déclare: « *dès lors que, rangeant l'information dans la catégorie (innombrable) des biens économiques, on voit dans le nouvel ordre de l'information un sous-système du nouvel ordre économique*³³¹ ». Et d'ajouter plus loin « *s'il s'agissait, dans le cas du marché de l'information, de tempérer des fluctuations excessives des prix ou de mieux gérer des ressources non renouvelables (...) de telles interventions entraîneraient inévitablement une réduction du volume de l'information. (...) La liberté de l'information implique: la liberté pour toute personne et toute institution de produire et consommer des informations; l'exclusion de toute entrave au libre accès et à la libre circulation de l'information*³³² ». Ces deux éléments (marché VS liberté) représentent l'ensemble de la problématique du nouvel ordre mondial de l'information et de la communication³³³. Cette dernière se retrouve également dans le cadre plus récent de la société de l'information. Au titre d'une étude sur les implications éthiques des nouvelles technologies publiée en 2007, l'UNESCO déclare en effet: « *la question fondamentale n'est pas l'information elle-même, mais les libertés qu'elle permet. L'objectif de la Société de l'information est donc de promouvoir la réalisation des*

³²⁹ Les Etats-Unis se retireront de l'UNESCO en 1984 du fait de l'absence de reconnaissance de ce marché par l'UNESCO.

³³⁰ PRONK Jan, *Observations sur la relation entre le nouvel ordre international de l'information et le nouvel ordre économique international*, UNESCO - Commission internationale d'étude des problèmes de la communication, n°35, 1978, En ligne: <http://unesdoc.unesco.org/images/0003/000346/034647fb.pdf> (dernière consultation: 5 mars 2018)

³³¹ Ibid. p. 14

³³² Ibid. p. 17 - 18

³³³ Ils en constituent également son principal échec. L'échec de l'UNESCO dans sa mission principale de coordination et de coopération internationale dans le cadre du NOMIC s'explique également par son acte constitutif qui décrit les buts et fonctions de l'organisation. L'article 1er de la Convention créant une Organisation des Nations Unies pour l'éducation, la science et la culture dispose : « *l'organisation se propose de contribuer au maintien de la paix et de la sécurité en resserrant, par l'éducation, la science et la culture, la collaboration entre nations, afin d'assurer le respect universel de la justice, de la loi, des droits de l'homme et des libertés fondamentales pour tous, sans distinction de race, de sexe, de langue ou de religion, que la Charte des Nations Unies reconnaît à tous les peuples* ». in. Convention créant une Organisation des Nations Unies pour l'éducation, la science et la culture (acte constitutif de l'UNESCO), Adoptée à Londres le 16 novembre 1945 et modifiée par la Conférence générale lors de ses 2e, 3e, 4e, 5e, 6e, 7e, 8e, 9e, 10e, 12e, 15e, 17e, 19e, 20e, 21e, 24e, 25e, 26e, 27e, 28e, 29e et 31e sessions, in. UNESCO, Textes fondamentaux, Editions 2004 comprenant les textes et amendements adoptés par la Conférence générale lors de sa 32^e session (Paris, 2003), UNESCO, Paris, 2004, p. 8. En ligne: <http://unesdoc.unesco.org/images/0013/001337/133729f.pdf#page=7> (dernière consultation: 5 mars 2018). Cette organisation a pour vocation essentielle de défendre les préceptes de liberté et de justice issus de la Charte des Nations Unies. Charte des Nations Unies (et Statut de la Cour Internationale de Justice), signée à San Francisco le 26 juin 1945 suite à la Conférence des Nations Unies pour l'Organisation Internationale, entrée en vigueur le 24 octobre 1945, En ligne: <http://www.un.org/fr/sections/un-charter/introductory-note/index.html> (dernière consultation: 5 mars 2018)

objectifs de l'info-éthique par la conception, le déploiement et l'utilisation éthiques de la technologie³³⁴ ».

122. Bien qu'il soit possible de comprendre que l'UNESCO ne prenne pas en compte la dimension marchande de l'information, et ce même dans la société de l'information des années 2000, son occultation totale du débat est assez surprenante. D'autant que, très tôt, des experts évoquent la toute puissance de l'information et de la communication. Au niveau international d'abord, un rapport rendu par Mustapha Masmoudi pour la Commission internationale d'étude des problèmes de la communication, déclare que « ***l'établissement d'un nouvel ordre mondial de l'information doit être considéré comme le corollaire essentiel du nouvel ordre économique international³³⁵*** ». Au niveau national ensuite, et à titre d'exemple, le rapport Nora - Minc, précité, déclarait dès l'année 1978: « *cette imbrication croissante des ordinateurs et des télécommunications - que nous appellerons la « télématique » - ouvre un horizon radicalement neuf. Ce n'est certes pas d'hier que les moyens de communication structurent les communautés: routes, chemins de fer, électricité, autant d'étapes d'une organisation familiale, locale, nationale, multinationale. La « télématique », à la différence de l'électricité ne véhiculera pas un courant inerte, mais de l'information, c'est-à-dire du pouvoir. La ligne téléphonique ou le canal de télévision constituent les prémisses de cette mutation. Ils se fondent aujourd'hui dans des transmetteurs polyvalents, commencent à relier des ordinateurs et des bases de données, disposeront bientôt, grâce aux satellites, d'un outil impérial. La télématique constituera non pas un réseau de plus mais un réseau d'une autre nature, faisant jouer entre eux images, sons et mémoires: elle transformera notre modèle culturel³³⁶ ».*

123. Ces lignes démontrent bien que la communication technicisée a pris corps dans la société.

³³⁴ RUNDLE MARY, CONLEY Chris, *Etude sur les implications éthiques des nouvelles technologies*, Programme Information pour tous, Secteur de la communication et de l'information, Unesco, Paris, 2007, p. 108, En ligne: <http://unesdoc.unesco.org/images/0014/001499/149992f.pdf> (dernière consultation: 5 mars 2018)

³³⁵ Traduction libre de l'auteur des propos suivants: « *The establishment of a new world information order must be considered as the essential corollary of the new international economic order* ». in. MASMOUDI Mustapha, *The new world information order*, Commission Internationale d'étude des problèmes de la communication, n° 31, Juillet 1978, p. 22, En ligne: <http://unesdoc.unesco.org/images/0003/000340/034010EB.pdf> (dernière consultation: 5 mars 2018). Mustapha Masmoudi, ancien Secrétaire d'Etat à l'information Tunisien, sous le gouvernement Hédi Nouira, Représentant permanent de la Tunisie auprès de l'UNESCO.

³³⁶ NORA Simon et MINC Alain, *Rapport à Monsieur le Président de la République concernant l'informatisation de la société*, 1978, La documentation française, p. 11 - 12, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000252.pdf> (dernière consultation: 5 mars 2018)

L'information en est son carburant essentiel, un enjeu de pouvoir et d'économie³³⁷. Ces éléments démontrent également l'ambition de la poursuite d'un double objectif, de construction d'un marché économique et de respect des libertés, poursuivi dans le cadre du nouvel ordre mondial de l'information et de la communication, repris par la société de l'information, et parachevé dans le cadre de la surveillance diffuse.

2. La liberté de circulation de l'information : une liberté économique structurante de la surveillance

124. La doctrine du *free flow of information*, ou libre flux de l'information, a émergé dans les pays occidentaux, et spécialement aux Etats-Unis pendant la guerre froide. D'abord envisagé comme un corollaire à la liberté de la presse comme permettant la circulation des idées, le concept de *free flow of information* est vite considéré aux Etats-Unis comme une possibilité nouvelle d'assurer le libre échange dans sa vision économique, c'est-à-dire de poursuivre après la guerre froide la libéralisation économique³³⁸. Cette doctrine inspire encore aujourd'hui des institutions internationales telles que l'Organisation Mondiale du Commerce (OMC), l'Organisation des Nations Unies (ONU) et l'Union Internationale des Télécommunications (UIT). Dans sa vision américaine, la libre circulation de l'information doit être comprise comme une véritable politique partagée, et globale de libéralisation économique, facilitant le développement et la construction d'une infrastructure des télécommunications.

125. En matière de protection de la vie privée et des données personnelles, cette doctrine a un impact fort puisque le concept de *free flow of information* a pour but essentiel de faciliter la circulation des informations. Des sanctions, en cas de violation de la vie privée, sont prévues, mais il faut d'ores et déjà préciser qu'aux Etats-Unis l'autorégulation des entreprises et les sanctions privées sont préférées à toutes sanctions purement étatique. Ces dernières étant assimilées à des

³³⁷ Voir en ce sens: PORAT Marc Uri, *The Information economy: definition and measurement*, Nine Volumes, Washington DC, Department of Commerce Government Printing Office, 1977. Ou pour une analyse plus récente: LAGET Marc, *Le numérique, simple mue du libéralisme ou avènement d'une économie soutenable*, Netcom, 22 - 3/4, 2008, En ligne: <https://netcom.revues.org/1618> (dernière consultation: 5 mars 2018)

³³⁸ Les Etats-Unis importeront d'ailleurs ce concept dans le cadre d'organisations internationales telles que l'UNESCO et les Nations Unies, en particulier lors de la Conférence de Genève de 1948. Pour une étude intéressante du concept de *free flow of information*, voir GOHAN-KLAS Tomasz, *The concept of the « Free and balanced flow of information » in the interpretation of central and east European countries*, UNESCO, Paris, 25 Septembre 1978, et spécialement les pages 4 et 5 de ce rapport, En ligne: <http://unesdoc.unesco.org/images/0003/000333/033313eb.pdf> (dernière consultation: 5 mars 2018). Voir aussi: MATTELART Armand, *Histoire de la société de l'information*, 4ème édition, Collection Repères, Editions La découverte, 2009, p. 36, p. 63 et suivantes

entraves au marché économique. En 1997, les Etats-Unis réagissent avec inquiétude à l'adoption de la directive européenne 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. Ces inquiétudes sont essentiellement résumées dans le cadre d'un document émanant de la Maison Blanche intitulé « *a framework for global electronic commerce*³³⁹ ». A la lecture de ce document, la Maison Blanche rappelle qu'au titre du premier amendement de la Constitution américaine la liberté de circulation de l'information est protégée, et que, pour prospérer, le commerce issu de la *global information infrastructure* doit prendre en compte un équilibre entre les droits des individus, spécialement la vie privée, avec les intérêts (économiques) associés à la libre circulation de l'information³⁴⁰. Pour le gouvernement américain, la directive de 1995 risque de « *conduire à des politiques disparates, susceptibles d'entraîner l'interruption des flux transfrontières*³⁴¹ » d'informations et de données. Aussi, il est alors nécessaire pour les Etats-Unis de poursuivre les discussions avec les partenaires européens afin de leur faire comprendre l'attachement américain à des solutions d'autorégulation des entreprises, ainsi que du marché économique. Ces mêmes points furent soulevés par les Etats-Unis, spécialement par les GAFAs, lors de l'élaboration du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016³⁴². Ces inquiétudes paraissent surprenantes au regard de la lecture attentive de la directive précitée. Bien que l'Union Européenne mette en oeuvre des mécanismes de sanctions administratives et légales, ainsi que des gardes fous à toute violation de la vie privée à l'égard du traitement des données à caractère personnel, elle les considère comme des marchandises. En effet, l'article 1er de la directive de 95 évoque les mêmes

³³⁹ THE WHITE HOUSE, *A framework for global electronic commerce*, 1^{er} Juillet 1997, En ligne: <https://clinton4.nara.gov/WH/New/Commerce/read.html> (dernière consultation: 5 mars 2018)

³⁴⁰ Traduction libre de l'auteur des lignes suivantes: « *At the same time, fundamental and cherished principles like the First Amendment, which is an important hallmark of American democracy, protect the free flow of information. Commerce on the GII will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information* ». Ibid.

³⁴¹ Traduction libre de l'auteur des lignes suivantes: « *Privacy concerns are being raised in many countries around the world, and some countries have enacted laws, implemented industry self-regulation, or instituted administrative solutions designed to safeguard their citizens' privacy. Disparate policies could emerge that might disrupt transborder data flows. For example, the European Union (EU) has adopted a Directive that prohibits the transfer of personal data to countries that, in its view, do not extend adequate privacy protection to EU citizens. To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United States will engage its key trading partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled* ». Ibid.

³⁴² Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, JOUE L 119 du 4 Mai 2016, P;1 - 88, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR> (dernière consultation: 5 mars 2018). L'article 1er du règlement en son paragraphe 3 dispose clairement que « *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* ».

préoccupations quant à la liberté de circulation des données à caractère personnel entre Etats membres. Ainsi, « *les Etats membres assurent (...) la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel. Les Etats membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etats membres pour des raisons relatives à la protection assurée*³⁴³ » en vertu de la protection de la vie privée. On retrouve cette même inspiration dans le Règlement précité.

126. La confrontation des visions américaines et européennes de la libre circulation de l'information est au coeur d'un enjeu de domination du marché économique de l'information et de la communication, et sont toujours d'actualité dans le cadre de la globalisation³⁴⁴ de la surveillance. La collecte d'information, qu'elle soit personnelle, économique, environnementale, étatique, culturelle, ou technique constitue l'essence même de nos sociétés. Elle trouve son apogée dans le concept de surveillance. Les deux logiques en présence se partagent entre une volonté d'hégémonie économique de la part des Etats-Unis³⁴⁵ et une volonté de protection contre « *la marchandisation de l'information personnelle* » qui pourrait primer sur les droits de l'Homme, et spécialement le droit à la protection de la vie privée³⁴⁶. Au niveau international, le principe de libre-circulation de l'information est donc par essence à la fois représentatif d'une liberté économique et d'une liberté fondamentale d'expression; et à la fois, structurante de la diffusion de la surveillance de part son ambition économique.

³⁴³ Article Premier 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*, Journal officiel n° L 281 du 23 novembre 1995, p. 0031 - 0050

³⁴⁴ Comme le souligne Lewis Mumford, dans son ouvrage *Technique et Civilisation*, la globalisation pourrait désigner la création, à l'échelle d'une civilisation, d'une forme d'unité politique. Il écrit: « *Platon définit l'optimum de population d'une cité par le nombre des citoyens qui peuvent entendre la voix d'un seul orateur. Aujourd'hui, ces limites ne désignent pas une cité, mais une civilisation. Partout où les instruments néotechniques sont disponibles et où l'on parle un langage commun, il y a maintenant les éléments d'une unité politique qui se rapproche presque de celle des plus petites cités de l'Attique jadis. Les possibilités en bien ou en mal sont immenses* ». MUMFORD Lewis, *Technique et civilisation*; traduit de l'américain par Denise Moutonnier, Éditions du Seuil, Les collections Esprit – La cité prochaine, Paris, 1950, p. 219

³⁴⁵ Voir en ce sens: BRZEZINSKI Zbigniew, *La révolution technétronique*, traduit de l'américain par Jean Viennet, Collection Liberté de l'esprit, Calmann-Lévy, Paris, 1971. Le titre anglais de l'ouvrage est : *Between two Ages: America's Role in the Technetronic Age*. La société américaine est décrite, dans cet ouvrage, comme la première société globale, principale instigatrice de la révolution technétronique, et principale force à l'oeuvre pour un changement global du monde, à travers la fabrique d'une conscience planétaire

³⁴⁶ En ce sens, voir GENTOT Michel, *La protection des données personnelles à la croisée des chemins*, Groupe d'études société d'information et vie privée, 2000, En ligne: <https://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr1.pdf> (dernière consultation: 5 mars 2018), Ou encore CNIL, 21 ème Rapport d'activité, 2000, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/014000460.pdf> (dernière consultation: 5 mars 2018)

Paragraphe 2: ... A la banalisation de la surveillance diffuse

127. Dans cette « société monde³⁴⁷ » que l'information a participé à créer, la surveillance s'est diffusée. Plus qu'une potentielle société de surveillance³⁴⁸, nombre d'auteurs ont alerté l'opinion publique dès les années 2000, et plus particulièrement en 2007, sur la « *grande surveillance*³⁴⁹ » ou encore sur la « *globalisation de la surveillance*³⁵⁰ ». Si ces expressions permettent de traduire une conception de société, la réalité d'une société de surveillance en tant que conception sociale doit être mise en doute. Cette conception est la traduction d'un imaginaire aux conséquences certes palpables, mais en aucune façon une vision sociale ayant fait l'objet d'un consensus.

128. La surveillance s'est diffusée par l'existence de la société de l'information qui a érigé en principe la liberté de circulation des informations et la vision marchande de ces dernières. Elle ne peut, pour autant, être un projet de société, telle que l'ont été la société de l'information et la société de la connaissance. Il est nécessaire de garder ces éléments en tête pour comprendre le refus d'utiliser le concept de société de surveillance, ainsi que pour bien comprendre la banalisation à l'oeuvre actuellement de la surveillance diffuse. Si l'idée même de la surveillance s'est banalisée, c'est d'abord et avant tout par l'enchevêtrement des dispositifs technologiques qui s'inscrivent dans des ambitions économiques et politiques différentes, et répondent, par là même, à des usages variés (A). De ce constat découle une nouvelle analyse: si la surveillance diffuse s'appuie sur une multiplicité de dispositifs socio-techniques, il semble alors qu'il faille s'intéresser aux formes de surveillance chères aux analyses sociologiques produites ces dernières années. Cette étude révélera l'insuffisance de ces analyses à produire une représentation claire et objective de la surveillance

³⁴⁷ On emprunte cette conception à Norbert Wiener. Ce dernier écrit: « *De nos jours avec l'avion, la radio, la parole de nos gouvernants s'étend jusqu'aux confins du globe et un grand nombre de raisons qui s'opposaient autrefois à la constitution d'un Etat mondial n'ont plus de valeur. On peut même affirmer que les problèmes de communications modernes qui nous obligent à régler juridiquement les revendications internationales des différents réseaux aériens et systèmes de radiodiffusion, rendent inévitable l'Etat mondial* ». WIENER Norbert, *Cybernétique et société : L'usage humain des êtres humains*, Collection Points Sciences, Points, 2014, p. 232

³⁴⁸ On notera ici que le 85ème congrès de la ligue des droits de l'Homme de 2009 est consacré à la « société de surveillance ». Ligue des Droits de l'Homme, Résolution adoptée lors du 85ème congrès de la LDH - Société de surveillance, vie privée et libertés, En ligne: http://www.ldh-france.org/IMG/pdf/Resolution_Societe_de_surveillance_-_85eme_congres_def.pdf (dernière consultation: 5 mars 2018). Il est également nécessaire d'évoquer la 27ème rapport d'activités de la CNIL de 2006 qui lance dès ses premières pages une « alerte à la société de surveillance »: CNIL, 27ème Rapport d'activités, 2006, La documentation française, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000422.pdf> (dernière consultation: 5 mars 2018)

³⁴⁹ VADROT Claude-Marie, *La Grande Surveillance - Caméras, ADN, portables, Internet...*, Collection L'Histoire immédiate, Editions du Seuil, 2007

³⁵⁰ MATTELART Armand, *La globalisation de la surveillance - Aux origines de l'ordre sécuritaire*, Editions la découverte, 2007

diffuse. Cette dernière semble aujourd'hui revêtir une forme double: une surveillance banale, du quotidien, et une surveillance imposée (B).

A. La surveillance diffuse : un enchevêtrement de dispositifs socio-techniques présents dans l'espace privé et public conduisant à une banalisation de la surveillance

129. Au-delà de la liberté de circulation de l'information, la société de l'information a permis de développer au niveau mondial des infrastructures, ainsi qu'un usage de dispositifs technologiques sans précédent. Ces deux éléments sont à la base même de l'élaboration et de la diffusion de la surveillance. Cette dernière fonctionne essentiellement sur les infrastructures créées par la société de l'information, et les innovations issues des premières technologies envisagées dans ce cadre (1). De cette pluralité technologique, l'usage technologique s'est banalisé, et a permis, à son tour, de banaliser l'idée même de la surveillance en tant qu'activité, moyen de parvenir à un but, finalité contre certains risques et menaces (2).

1. La pluralité technologique comme élément structurant de la surveillance

130. Bien que l'on connaisse des possibilités offertes par le marché économique du numérique et de sa pierre angulaire, l'information, entendue comme source de pouvoir, on comprend moins pourquoi et comment s'est agencée la prolifération technologique. A l'image d'une « synapse informationnelle³⁵¹ », l'enjeu est ici de comprendre la zone de contact fonctionnelle entre secteur public et privé ayant permis d'aboutir à la surveillance diffuse. Evoquer la pluralité technologique ne revient alors pas à dresser une simple liste de l'ensemble des technologies nouvelles, ou non, mises en place dans notre société. La pluralité technologique servant la surveillance diffuse correspond bien plutôt à une forme de continuité. Ainsi que l'explique Eric Sadin, la situation actuelle correspond à un « *entrecroisement récent de causes multiples (qui) produit une sorte de « bouillon de culture » composé d' « ingrédients idéaux », favorables à la formation d'un continuum ininterrompu de dispositifs de surveillance³⁵²* ». La première continuité identifiée dans le cadre de cette analyse réside dans la poursuite des objectifs de la société de l'information et de la

³⁵¹ Ainsi que le rappelle le rapport Théry, dès son introduction, « *la révolution de l'an 2000 sera celle de l'information pour tous. Comparable en ampleur à celle des chemins de fer ou de l'électrification, elle sera plus profonde dans ses effets car les réseaux de télécommunications constituent désormais le système nerveux de nos sociétés* ». In. THERY Gérard, BONAFE Alain, *Rapport au premier ministre - Les autoroutes de l'information*, Collection des rapports officiels, La documentation française, Janvier 1994, p. 7

³⁵² SADIN Eric, *Surveillance Globale - enquête sur les nouvelles formes de contrôle*, Flammarion, Climats, 2009, p. 18

communication. Cette dernière a permis à Internet de faire partie des usages quotidiens des individus pour accéder à la connaissance, aux échanges, et participer aux flux permanents d'informations. A la succession de ces événements s'est mêlée une prolifération technologique créant à son tour de nouveaux usages, de nouveaux flux.

131. La synapse informationnelle se cristallise essentiellement dans le thème des autoroutes de l'information, qui engendrera Internet. Dans les années 90, ce thème a suscité l'engouement sur la scène internationale, et spécialement dans les pays de l'OCDE. Ainsi, par exemple, Edouard Balladur écrivait en 1994: « *de même que les technologies de l'informatique et des télécommunications ont, en leur temps, convergé pour produire ce qu'on a appelé la télématique, de même le monde des télécommunications et celui de l'audiovisuel sont-ils désormais appelés à s'interpénétrer. Le rôle des autoroutes de l'information sera ainsi de transporter simultanément voix, données et images jusqu'à l'utilisateur final*³⁵³ ». Le concept d'autoroutes de l'information est officiellement élevé au rang de politiques publiques par Al-Gore, sénateur proche de Bill Clinton, puis vice-président des Etats Unis. Grâce à cette métaphore située dans la lignée des hommes politiques de la famille Gore³⁵⁴, Al-Gore (Junior) est parvenu à légitimer auprès du grand public l'intérêt pour les Etats-Unis de développer une infrastructure nationale dans le domaine de l'information et de la communication³⁵⁵. Cette légitimation progressive a d'abord été envisagée du fait de la loi³⁵⁶, puis réellement par la mise sur agenda politique des objectifs et actions à mener

³⁵³ Lettre de mission de Monsieur le Premier Ministre Edouard Balladur, à Monsieur Gérard Théry, du 28 février 1994, Paris, In. THERY Gérard, BONAFE Alain, *Rapport au premier ministre - Les autoroutes de l'information*, Collection des rapports officiels, La documentation française, Janvier 1994, p. 3

³⁵⁴ La thématique des autoroutes est un sujet cher à la famille Gore. Albert Gore Senior a joué un rôle important dans la création et la promulgation de la loi créant aux Etats-Unis le grand réseau autoroutier inter-états (Federal-Aid Highway Act de 1956, Public Law 627, 29 Juin 1956, En ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-70/pdf/STATUTE-70-Pg374.pdf> (dernière consultation: 5 mars 2018)).

³⁵⁵ Autrement appelé la National Information Infrastructure, qui deviendra deux ans plus tard (1994) la Global Information Infrastructure c'est-à-dire l'infrastructure mondiale de l'information.

³⁵⁶ C'est en effet au travers de la High Performance Computing Act de 1991 proposée par Al Gore que l'on trouve mention de la national information infrastructure au travers de l'exposé des motifs de la loi: « *A 1991 report entitled « Grand Challenges: High-Performance Computing and Communications » by the Office of Science and Technology Policy, outlining a research and development strategy for high-performance computing, provides a framework for a multiagency high-performance computing program. Such a program would provide American researchers and educators with the computer and information resources they need, and demonstrate how advanced computers, high-capacity and high-speed networks, and electronic data bases can improve the national information infrastructure for use by all Americans* ». *High-Performance Computing Act of 1991*, 15 USC 5501, Public Law 102-194, 9 décembre 1991, En ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-105/pdf/STATUTE-105-Pg1594.pdf> (dernière consultation: 5 mars 2018)

pour construire cette infrastructure³⁵⁷. Dans le même temps, l'Europe publie son livre blanc concernant la croissance, la compétitivité et l'emploi³⁵⁸. Les enjeux exposés dans le cadre de ce livre blanc concernant les autoroutes de l'information sont clairs. Ces dernières, ou plus globalement les réseaux, sont considérés par l'Europe comme « *les artères nourricières du grand marché*³⁵⁹ » qui permettront d'injecter du « *sang neuf*³⁶⁰ » à la situation économique de l'Union européenne³⁶¹.

132. A l'image des politiques américaines, l'Europe et les gouvernements nationaux³⁶² développent des stratégies d'actions à mettre en place afin d'assurer la connexion du plus grand nombre. Le rôle de l'Etat semble alors s'éloigner de sa fonction de prescripteur, pour y préférer un rôle de préconisation. En effet, ces politiques des autoroutes de l'information sont assimilables à des principes dégagés par les Etats, fixant des buts à atteindre, et envisageant les principales entraves à l'édification de ce marché en devenir. L'exemple de la Commission européenne est particulièrement éclairant sur ce point. Dans le cadre du livre blanc précité, la Commission insiste sur la construction des autoroutes de l'information d'un point de vue économique, et influence les choix stratégiques à développer sur les questions de financements et de partenariats publics-privés, sur les enjeux de concurrence, de libéralisation du marché, d'effacement progressif du protectionnisme. Par le biais de la mise sur agenda politique des autoroutes de l'information, l'Etat devient un véritable relais

³⁵⁷ La High Performance Act de 1991 a pour objectif de préserver la position de leader des Etats-Unis dans le domaine des technologies de l'information et de la communication en établissant à l'origine un vaste réseau national à haut débit pour la recherche et l'éducation. Pour ce faire, un programme public national est mis en place afin d'établir les buts et les priorités de ce réseau.

³⁵⁸ Commission des Communautés Européennes, *Livre Blanc Croissance, compétitivité, emploi - Les défis et les pistes pour entrer dans le XXI ème siècle*, Bulletin des Communautés européennes, Supplément 6/93, Luxembourg: Office des publications officielles des Communautés européennes, 1993, En ligne: <http://bookshop.europa.eu/fr/croissance-comp-titivit-emploi-les-d-fis-et-les-pistes-pour-entrer-dans-le-xxie-si-cle.-livre-blanc-bulletin-des-communaut-s-europ-ennes-suppl-ment-6-93-pbCMNF93061/> (dernière consultation: 5 mars 2018)

³⁵⁹ Ibid. p. 77 - 78

³⁶⁰ Ibid.

³⁶¹ La Commission européenne dégage quatre éléments fondamentaux, conditions préalables à la réalisation en Europe d'une politique des autoroutes de l'information. Cette dernière doit prendre en compte « *l'état des finances de la Communauté* » et ne doit pas entraîner de « *besoins nouveaux en matière de financement public* ». Pour ce faire, la Commission propose d'élaborer « *de nouvelles formes de partenariat entre financement privé et financement public, sur la base d'une « ingénierie » financière englobant toutes les sources et formes de financement* ». La Commission envisage également deux problématiques essentielles, sortes d'entraves à la construction de ces autoroutes dans le marché unique: « *l'absence de marchés ouverts et concurrentiels interdits, à différents degrés, de valoriser au mieux les réseaux existants et de les compléter dans l'intérêt des consommateurs et des opérateurs; les lenteurs inhérentes aux procédures de préparation, de planification, d'autorisation, et d'évaluation entravent considérablement la réalisation de projets importants* ». Ibid.

³⁶² A la suite de la publication de ce livre blanc, les gouvernements nationaux, tels que la France, l'Angleterre et l'Allemagne, ont tous pris la mesure des autoroutes de l'information à travers des rapports et des plans d'actions à élaborer pour assurer l'effectivité de cette thématique.

d'influence, assurant une fonction d'impulsion, de mobilisation (débat social), de coordination, et permettant à la fois de développer l'offre et la demande en la matière. Par la préconisation de l'assouplissement des cadres réglementaires dans le domaine des autoroutes de l'information et par la volonté d'une libéralisation du marché, l'Etat retrouve une partie de son rôle de prescripteur dans sa mission de réglementation et de régulation des infrastructures et des services de la future société de l'information. Relais d'influence, l'Etat l'est également par son soutien financier aux activités de recherche et développement³⁶³ en pleine expansion à la fin des années 90, début des années 2000.

133. Si la surveillance diffuse a pu se propager c'est donc essentiellement du fait d'une convergence d'intérêts des leaders du numérique (secteur privé) et du secteur public en termes de reconnaissance des besoins et des évolutions techniques et technologiques, et par imitation politique entre pays en vue de la construction des autoroutes de l'information³⁶⁴. Volonté d'harmonisation des réglementations, réglementations et objectifs communs internationaux., émulation entre secteur privé et secteur public, participation des citoyens³⁶⁵, déréglementation des télécommunications³⁶⁶ et

³⁶³ Voir: MACHLUP Fritz, *The Production and distribution of knowledge in the United States*, Princeton University Press, 1962; et du même auteur: *Knowledge: Its Creation, Distribution and Economic Significance*, Volume III, Princeton University Press 1984; *Economie des connaissances et de l'information*, p. 126 in. Réseaux, volume 11, n°58, 1993, *l'information scientifique et technique*, pp.109 - 129, En ligne: http://www.persee.fr/docAsPDF/reso_0751-7971_1993_num_11_58_2308.pdf (dernière consultation: 5 mars 2018); ORAT Marc-Uri, *The Information Economy: Definition and Measurement*, 9 volumes, Government Printing Office, Washington D.C., 1977; CASTELLS Manuel, *La société en réseaux - l'ère de l'information*, traduit de l'anglais par Philippe Delamare, Fayard, 1998. Manuel Castells écrit, par exemple, que lorsque la recherche « s'est formée en système, sur la base de conglomération (...), son développement et ses applications, et finalement son contenu, ont été modelés de façon décisive par le contexte historique dans lequel elle s'est épanouie. D'ailleurs, dans les années 1980, le capitalisme (et plus précisément les grandes sociétés et les gouvernements du G-7) a entamé un important processus de restructuration économique et organisationnelle, au coeur duquel la nouvelle technologie de l'information a joué un rôle fondamental, rôle qui l'a façonnée elle-même de manière déterminante » (p 76-77).

³⁶⁴ Voir TARDE Gabriel, *Les lois de l'imitation – Étude sociologique*, 7ème édition, Paris, Librairie Félix Alcan, 1921

³⁶⁵ Dès 1993, Al Gore présente l'agenda politique pour l'action sur l'infrastructure de l'information nationale, et exhorte citoyens et secteur privé à être acteurs des autoroutes de l'information: « *Tous les Américains ont un intérêt à la construction d'une infrastructure nationale de l'information avancée* ». Information Infrastructure Task Force, *The National Information Infrastructure: Agenda for Action*, Department of Commerce, Washington DC., 15 Septembre 1993, p. 5, En ligne: <http://files.eric.ed.gov/fulltext/ED364215.pdf> (dernière consultation: 5 mars 2018)

³⁶⁶ Après la publication du Livre vert de la Commission européenne sur le rôle des télécommunications dans la construction européenne en 1987, deux directives complémentaires sont publiées le même jour, l'une relative à la concurrence dans les marchés des services de télécommunication, l'autre relative à l'établissement du marché intérieur des services de télécommunications par la mise en oeuvre de la fourniture d'un réseau ouvert de télécommunications. Directive 90/388/CEE de la Commission, du 28 juin 1990, *relative à la concurrence dans les marchés des services de télécommunication*, Journal officiel n° L 192 du 24/07/1990 p. 0010 - 0016, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31990L0388> (dernière consultation: 5 mars 2018) et Directive 90/387/CEE du Conseil, du 28 juin 1990, *relative à l'établissement du marché intérieur des services de télécommunication par la mise en oeuvre de la fourniture d'un réseau ouvert de télécommunications*, Journal officiel n° L 192 du 24/07/1990 p. 0001 - 0009, <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31990L0387&from=FR> (dernière consultation: 5 mars 2018). En application de ces textes, la France à travers loi du 29 décembre 1990 relative à la réglementation des télécommunications limitera le monopole de France Télécom. Loi n°90-1170 du 29 décembre 1990 sur *la réglementation des télécommunications*, JORF n° 303 du 30 décembre 1990, p. 16439, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000533747&categorieLien=id> (dernière consultation: 5 mars 2018)

éclatement des monopoles³⁶⁷ dans ce domaine sont autant d'éléments préparatoires et structurants de la surveillance diffuse. Plus globalement, la surveillance s'est construite par un ajout permanent de (sur) couches et d'usages technologiques différents. Derrière le singulier du recours à l'expression de surveillance diffuse, derrière l'image préconçue d'un Big Brother totalitaire, d'une surveillance tentaculaire exercée dans un but précis par un acteur déterminé, il faut prendre la mesure de la pluralité de dispositifs socio-techniques et de leurs imbrications pour des finalités diverses. Les technologies mises en place dans les sociétés contemporaines ne correspondent pas toutes à une finalité de surveillance. Et, si tel est le cas, ces technologies sont souvent sans recoupement apparent. Rappelons ici que la surveillance diffuse n'obéit à aucun dessein prédéfini. Elle est à la fois poursuite logique d'un projet de société, d'une révolution sociale; et est ensuite un concept permettant de rendre compte de l'ensemble des stratégies de développement et de déploiement technologique non coordonnées permettant la collecte, l'enregistrement et le traitement de nombreuses données personnelles ou non. Elle est aussi la conséquence ultime du paradigme technologique qui a permis aujourd'hui la mise en données du monde, l'explosion de l'économie de la Data, et plus insidieusement la réduction de l'individu à ses traces, ses données, ses informations.

2. La banalisation de la surveillance diffuse

134. L'usage de l'expression surveillance diffuse permet de retranscrire la banalisation de la surveillance. Un point sémantique concernant ce terme permet à la fois de confirmer les propos précédents, mais également d'attirer l'attention sur les évolutions possibles de ce phénomène.

135. L'un des premiers sens de cet adjectif, selon le Larousse, renvoie à quelque chose de courant, d'ordinaire, qui ne s'écarte pas du cours normal des choses, ou encore dans un sens péjoratif, ce terme s'entend de quelque chose ou de quelqu'un qui manque d'originalité. Cette définition première, en ce qu'elle désigne la poursuite du cours normal des choses, pointe l'idée de continuité. En cela, cette notion confirme le fait de voir en la surveillance et en sa diffusion une poursuite, un développement et une apogée de la société de l'information et de la connaissance. Cette continuité se constate alors tant dans la fabrication du concept, que dans l'activité même de

³⁶⁷ On citera également l'exemple, aux Etats-Unis, de la fin du monopole de l'entreprise américaine AT&T en 1984, et la signature par Bill Clinton en 1996 de la loi sur les télécommunications (*Telecommunications Act of 1996*, Intergovernmental relations, 47 USC 609 note, Public Law 104-104 - 8 février 1996, En ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-110/pdf/STATUTE-110-Pg56.pdf> (dernière consultation: 5 mars 2018)).

surveillance: que cette dernière soit généralisée ou ciblée sur des populations à risque, des individus dangereux. Il faut ainsi noter que la surveillance des citoyens au nom de la sécurité, au nom de l'ordre public, a un passif ancien que ce soit dans les régimes dits autoritaires, ou dans les régimes dits démocratiques. A titre d'illustrations, le fichage des populations se développe sous Louis XIV, et spécialement grâce à Guillaudé³⁶⁸. On pourrait également citer le livret ouvrier qui permettait de surveiller les déplacements des classes populaires sous Napoléon au début du 19^{ème} siècle, ou encore le fichage des vagabonds des années 1900. La France de Vichy, a permis quant à elle de développer des pratiques de surveillance ciblée, par un recensement systématique, sur la population juive. Aujourd'hui, on pourrait mettre en exergue l'élaboration du fichier Titres Electroniques Sécurisés autorisé par le Décret du 28 octobre 2016³⁶⁹. Ainsi, la surveillance, entendu ici comme activité de police, est assez banale dans le cadre global de l'Histoire française. On comprend bien l'idée de continuité du point de vue de l'activité de surveillance, mais également du point de vue du phénomène contemporain de surveillance diffuse, en ce qu'elle représente la collecte et le traitement de toujours plus d'informations et de données.

136. Avec le développement de la société de l'information, la surveillance diffuse s'est également banalisée du fait des effets connexes et moyens mis en oeuvre. La société de l'information, la révolution numérique, et l'ambition d'un marché du numérique ont multiplié les usages possibles des technologies, leurs développements dans la sphère publique mais également privée. Chaque semaine apparaît une nouvelle divulgation dans la presse à propos des réseaux sociaux, des applications téléphoniques, des objets connectés, des caméras vidéos, des puces RFID³⁷⁰, de la biométrie, du développement de capteurs, des analyses génétiques... Chaque mois, une nouvelle

³⁶⁸ Guillaudé, officier de la maréchaussée, a inventé sous Louis XIV une machine (une roue fixée dans le mur qui faisait tourner des fichiers d'identifications pour diminuer l'espace de stockage) permettant de classer le registre de toute la population parisienne. Chaque habitant étant à l'époque fiché (nom, âge, origine, qualités, date d'arrivée dans les lieux d'habitation est enregistré dans des feuillets tenus par et pour la police, et une sorte de certificat d'identité est remis à l'habitant). La machine de Guillaudé porte le nom de « serre - papiers de Guillaudé ».

³⁶⁹ Ce fichier est constitué afin de réunir les données personnelles, notamment biométriques, de tous les détenteurs de carte d'identité et de passeport. Cette base de données a pour but de remplacer le précédent fichier TES, élaboré pour les passeports, et le fichier national de gestion (carte d'identité) en combinant ces deux fichiers. L'objectif affiché pour le gouvernement est de lutter contre la fraude (contrefaçons et vols de pièce d'identité), mais également de permettre une identification plus rapide des individus à partir de leurs données personnelles et biométriques dans le cadre des procédures judiciaires. Décret n° 2016 - 1460 du 28 octobre 2016 *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*, JORF n° 0254 du 30 octobre 2016, texte n°18, disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345&dateTexte=&categorieLien=id> (dernière consultation: 5 mars 2018)

³⁷⁰ A titre d'illustration, on notera l'ambition récente d'une société belge qui a permis à des salariés volontaires de se faire implanter une puce électronique sous la peau, et ce afin de remplacer l'identification et l'accès aux locaux par badges. (Pour plus d'informations, voir l'article de l'express à ce sujet: http://www.lexpress.fr/actualite/en-belgique-des-salaries-se-font-implanter-une-puce-electronique-sous-la-peau_1876738.html (dernière consultation: 5 mars 2018))

révélation sur des cyberattaques visant des Etats ou des entreprises, la vulnérabilité des systèmes d'informations, l'existence de backdoor présent dans nos smartphone, de piratage, de vol de données, de cyberdélinquance. L'élaboration du marché du numérique s'est accompagnée de transformations sociales et d'effets insidieux. D'une part, l'avènement du numérique dans nos sociétés a permis une large propagation des capteurs d'enregistrements de sons, d'images et de textes; d'objets intelligents et connectés avec des capacités de stockage importantes. Ces derniers sont souvent dotés d'une fonction de géolocalisation permettant soit de retrouver ces objets, soit leur propriétaire. La baisse du coût de production de ces objets a permis une baisse de prix rendant de plus en plus accessible les technologies à tout un chacun. A l'image de la démocratisation d'Internet, qui permet aux individus de rechercher et/ou de publier des informations, des textes, des images, des sons à propos de quelqu'un ou quelque chose de manière totalement anonyme, avec une audience potentiellement importante, la tendance est aujourd'hui de posséder télévision, frigo, montre, bracelet ou encore brosse à dents connectés. Ces objets émettent des informations (données personnelles, techniques...) sur leurs propriétaires qu'ils consentent à laisser à disposition en toute bonne foi. La multiplication de ces objets, et des plateformes potentielles (réseaux sociaux entre autres) n'est pas pour autant anodine. Bien que le consentement soit donné, il est nécessaire d'émettre quelques doutes: quid de la réutilisation des données? Quid également de l'exploitation abusive de ces données? L'effet principal de cette numérisation sociale est l'attractivité économique, sociale et politique que représentent ces données pour les entreprises, les Etats et les individus. Que l'on évoque ce problème sous l'angle de l'interconnexion et de l'interopérabilité des systèmes de communications et de bases de données qui permettent la collecte et le traitement de toujours plus d'informations, que l'on évoque le phénomène du Big data, ou encore les possibilités offertes par le Data mining, le volume de données se développe, et avec lui la désirabilité pour ces données. La possibilité de manipulation de ces informations évoluent également: traçabilité des opérations réalisées par le numérique, traçabilité des personnes, ou encore usage d'algorithme prédictif et préconisateur sont autant de nouvelles possibilités d'induire une banalisation de la surveillance dans la conscience collective, une culture véritable de la surveillance. Et, c'est bien l'un des problèmes de la surveillance diffuse.

137. Au-delà de sa généralisation³⁷¹, de sa mondialisation, de son caractère de plus en plus acceptable, la surveillance s'est massifiée. A l'image de bien de consommation devenue aujourd'hui

³⁷¹ Dans le sens premier de ce terme, c'est-à-dire de donner un caractère général à quelque chose, lui donner une portée, une extension plus grande

dans leur usage banal et quotidien³⁷², la surveillance diffuse s'est ancrée dans le quotidien, et a fortement imposé sa nécessité en même temps que sa banalité. A la fois généralisée de part le développement croissant des équipements présents dans l'espace public et privé, elle est devenue vitale pour l'activité économique, politique et pour l'ensemble d'une population en besoin de sécurité. Les propos du type « rien à cacher car rien à se reprocher », ou encore l'absence d'étonnement face à une surveillance généralisée suite à l'affaire Prism³⁷³, connaissant les possibilités d'écoute et d'interception de la NSA, montrent à quel point la surveillance s'est pleinement diffusée dans nos sociétés, quitte à en devenir naturel, banal dans la représentation que les individus s'en font, culturellement intégrée comme nécessaire, comme un moindre mal. Naturelle, la surveillance diffuse l'est aussi devenue puisqu'elle est un parfait aboutissement d'un processus évolutif lancée par le NOMIC³⁷⁴ et poursuivi par la société de l'information. Nouvel or noir³⁷⁵ de notre société et plus que jamais source de pouvoir, l'information protéiforme en représente le rouage essentiel. Pour autant, la banalité de la surveillance et sa diffusion dans notre société ne doit pas occulter les problématiques qu'elle pose tant en termes de transformations sociétales et de changements sociaux, qu'en termes juridiques, notamment en terme de protection des données personnelles, et du droit au respect de la vie privée.

B. Les formes de la surveillance à l'épreuve de la surveillance diffuse

138. Deux citations donneront le ton de cette analyse, l'une écrite par le philosophe Eric Sadin, l'autre par Mathieu Potte-Bonneville, philosophe et spécialiste de l'oeuvre de Michel Foucault. Ces deux auteurs écrivent en 2010, à l'occasion d'un dossier intitulé « *du contrôle à la sousveillance*³⁷⁶ » paru à la revue *Multitudes* que, d'une part « *c'est une illusion de croire à l'unicité du terme de « surveillance », la surveillance en tant que telle n'existe pas, elle est le résultat d'une*

³⁷² On pense ici à l'automobile, ou à la télévision. Voir: CHOQUET Olivier, *L'automobile, un bien banalisé*. In. *Economie et statistique* n° 154, Avril 1983. *Les 39 heures / les salaires en 1982 / L'automobile, un bien banalisé*. P. 47 - 55; En ligne: http://www.persee.fr/doc/estat_0336-1454_1983_num_154_1_4741 (dernière consultation: 5 mars 2018), GAILLARD Isabelle, *De l'étrange lucarne à la télévision - Histoire d'une banalisation (1949 - 1984)*, Vingtième siècle. *Revue d'histoire* 2006/3 n°91, p. 9-23, En ligne: <http://www.cairn.info/revue-vingtieme-siecle-revue-d-histoire-2006-3-page-9.htm> (dernière consultation: 5 mars 2018)

³⁷³ Op. Cit.

³⁷⁴ Op. cit.

³⁷⁵ Op. Cit.

³⁷⁶ *Multitudes* 2010 / 1, n° 40, « Du contrôle à la sousveillance », pp. 51 à 138, En ligne: <https://www.cairn.info/revue-multitudes-2010-1.htm> (dernière consultation: 5 mars 2018)

*pluralité de technologies éparses et de finalités très variées qui la plupart ne se recoupent pas*³⁷⁷ ». D'autre part, et concluant sur les analyses de Michel Foucault, Mathieu Potte-Bonneville écrit: « *elles engagent à dé-totaliser une thématique qu'il est parfois tentant d'énoncer au singulier - la surveillance, le contrôle. Non seulement, en effet, un même dispositif peut voir son sens modifié s'intégrer à des rationalités politiques différentes, et se trouve défini par la variété de ses usages, davantage que par ses caractéristiques intrinsèques; mais ces rationalités multiples peuvent coexister, se chevaucher, voire s'intégrer fonctionnellement tout en offrant des prises diverses à la critique. Non pas, donc : sous la variété des outils, l'unité d'une surveillance bio-politique, mais: à travers chaque surveillance, le disparate des bio-politiques*³⁷⁸ ». En deçà de l'emploi du singulier dans le cadre de l'expression surveillance diffuse se cache un sens polysémique tant en terme d'usage, de finalité, que de fonction technologique. Son contenu multiple (1) doit être questionné pour cerner les formes contemporaines que prend la surveillance diffuse (2). Pour ce faire, on se référera à la notion sociologique de dispositif cher à Michel Foucault afin de l'appliquer à l'une des technologies représentatives de la surveillance: Internet. Ces éléments permettront un constat: la surveillance diffuse revêt aujourd'hui une double nature - une surveillance de plus en plus banalisée et acceptée du quotidien et, en face, une surveillance imposée.

1. La polysémie de la surveillance diffuse

139. Selon Foucault, il faut entendre par dispositif « *un ensemble résolument hétérogène comportant des discours, des institutions, des aménagements architecturaux, des décisions réglementaires, des lois, des mesures administratives, des énoncés scientifiques, des propositions philosophiques, morales, philanthropiques ; bref, du dit aussi bien que du non-dit voilà les éléments du dispositif. Le dispositif lui-même, c'est le réseau qu'on établit entre ces éléments*³⁷⁹ ». Dans la pensée de cet auteur, la surveillance est représentée par un dispositif (pan)optique qui « *aménage*

³⁷⁷ QUESSADA Dominique, SADIN Eric, « Big Brother n'existe pas, il est partout. Discussion à partir du livre d'Éric Sadin, autour de la surveillance comme prisme d'observation des mutations de l'environnement contemporain », *Multitudes* 2010/1 (n° 40), p. 78-87, p. 78

³⁷⁸ POTTE-BONNEVILLE Mathieu, « Surveillance, contrôle, gouvernement : l'ADN du contemporain. De l'actualité de la pensée de Michel Foucault au travers de l'exemple polémique des « tests génétiques » », *Multitudes* 2010/1 (n° 40), p. 68-76, p. 75

³⁷⁹ FOUCAULT Michel, « le jeu de Michel Foucault » (entretien avec D. Colas, A. Grosrichard, G. Le Gaufey, J. Livy, G. Miller, J. Miller, J. - A. Miller, C. Millot, G. Wajeman), *Ornicar?*, *Bulletin périodique du champ freudien*, n°10, juillet 1977, pp. 62-93, in. DEFERT Daniel et EWALD François (sous la direction de), *Michel Foucault, Dits et écrits 1954 - 1988, II. 1976 - 1988*, Editions Quarto Gallimard, 2001, texte n°206, p. 299 - 300

*des unités spatiales qui permettent de voir sans arrêt et de reconnaître aussitôt*³⁸⁰ ». De nos jours la surveillance diffuse s'organise principalement grâce au réseau Internet. Avec les révélations de Snowden, Internet, en tant qu'objet technologique et dispositif socio-technique, focalise l'ensemble des attentions politiques, économiques et démocratique représentative des inquiétudes soulevées par la surveillance. Un ensemble de discours, d'institutions, d'énoncés moraux et scientifiques est mis en place à ce propos. Les conditions d'accès à ce réseau font l'objet depuis plus de quinze ans de rencontres et de sommets internationaux afin d'appréhender sa gouvernance³⁸¹, sa neutralité, ou encore son accès universel. On peut ainsi lire aux détours de plusieurs rapports d'information français enregistrés à la Présidence du Sénat des termes évoquent Internet comme un enjeu géopolitique, géostratégique et géo-économique³⁸². Plus que l'affaire Prism, on peut également lire dans ces rapports qu'Internet est devenu un « *support d'un monde d'hypersurveillance et de vulnérabilité*³⁸³ ». Alors qu'à l'origine ce réseau se voulait être un instrument de télécommunications permettant la liberté d'expression et de culture, il est devenu, en France et à l'international, sous couvert de guerre contre le terrorisme et d'enjeu de sécurité globale, un outil de surveillance et/ou de censure à cette même liberté. Un ensemble de lois servant tantôt le premier

³⁸⁰ Notons la description du panoptique de Foucault: « *on en connaît le principe; à la périphérie un bâtiment en anneau; au centre, une tour ; celle-ci est percée de larges fenêtres qui ouvrent sur la face intérieure de l'anneau ; le bâtiment périphérique est divisé en cellules, dont chacune traverse toute l'épaisseur du bâtiment ; elles ont deux fenêtres, l'une vers l'intérieur, correspondant aux fenêtres de la tour ; l'autre, donnant à l'extérieur, permet à la lumière de traverser la cellule de part en part. Il suffit alors de placer un surveillant dans la tour centrale, et dans chaque cellule d'enfermer un fou, un malade, un condamné, un ouvrier ou un écolier. Par l'effet du contre-jour, on peut saisir de la tour, se découpant exactement sur la lumière, les petites silhouettes captives dans les cellules de la périphérie. Autant de cages, autant de petits théâtres, où chaque acteur est seul, parfaitement individualisé et constamment visible. Le dispositif panoptique aménage des unités spatiales qui permettent de voir sans arrêt et de reconnaître aussitôt* ». Et de conclure, « *le Panopticon ne doit pas être compris comme un édifice onirique : c'est le diagramme d'un mécanisme de pouvoir ramené à sa forme idéale ; son fonctionnement, abstrait de tout obstacle, résistance ou frottement, peut bien être représenté comme un pur système architectural et optique : c'est en fait une figure de technologie politique qu'on peut et qu'on doit détacher de tout usage spécifique* ». in. FOUCAULT Michel, *Surveiller et punir - Naissance de la prison*, Op. Cit., p.358 et s.

³⁸¹ La gouvernance d'Internet a été défini lors du Sommet mondial de la Société de l'information (2003-2005), comme étant « *l'élaboration et l'application par les États, le secteur privé et la société civile de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet* » (<http://www.itu.int/wsis/index-fr.html> (dernière consultation: 5 mars 2018)).

³⁸² MORIN-DESAILLY Catherine, *Rapport d'information n°443 fait au nom de la commission des affaires européennes sur l'Union européenne, colonie du monde numérique ?*, Sénat, Session ordinaire 2012-2013, enregistré à la Présidence du Sénat le 20 mars 2013, En ligne: <https://www.senat.fr/rap/r12-443/r12-4431.pdf> (dernière consultation: 5 mars 2018), MORIN-DESAILLY Catherine, *Rapport d'information n°696 fait au nom de la mission commune d'information « nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet* », Sénat, Session extraordinaire de 2013-2014, enregistré à la Présidence du Sénat le 8 juillet 2014, En ligne: <https://www.senat.fr/rap/r13-696-1/r13-696-11.pdf> (dernière consultation: 5 mars 2018). Dans ce dernier rapport, qui reprend pour partie les conclusions du premier, on peut lire que la gouvernance d'Internet est « *un nouveau terrain d'affrontement mondial* » (chapitre 1), ou encore qu'il est « *un instrument de puissance qui échappe à l'Europe* » (p. 52 et s.), que « *le séisme Snowden transforme la gouvernance de l'internet en enjeu géopolitique* » (p. 132 et s.).

³⁸³ MORIN-DESAILLY Catherine, *Rapport d'information n°696* précédemment cité, p. 72 et s.

objectif³⁸⁴, tantôt le second est mis en place³⁸⁵. Les développements récents en France d'une volonté de surveillance renforcée aux fins de contrôle des données échangées via des réseaux de communication électronique ont transformé progressivement cet outil de communication en un véritable support de surveillance. Depuis la loi n°2013-1168 du 18 Décembre 2013³⁸⁶, mais également avec deux lois de 2015, l'une relative au renseignement³⁸⁷, l'autre relative aux mesures de surveillance des communications électroniques internationales³⁸⁸, des mesures encadrant la conservation et l'utilisation des données de connexion, autorisant la création de système automatisé permettant de détecter des connexions susceptibles de révéler une menace terroriste³⁸⁹ ont en effet détourné Internet de son but premier de communication, d'accès à la connaissance et à la culture. En deçà de l'usage d'Internet à des fins de sécurité (inter)nationale il faut également s'attarder sur les possibilités de tracking commercial, et de profilage à l'oeuvre depuis la naissance d'Internet. Et

³⁸⁴ Article 11 de la Déclaration des Droits de l'Homme et du citoyen, article 19 de la Déclaration Universelle des Droits de l'Homme

³⁸⁵ Concernant les restrictions à la liberté d'expression, on pourrait notamment citer: la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, son titre évoque plus précisément *la liberté de communication en ligne* (titre 1 de la loi, et spécialement son article 6), mais également la première loi Hadopi (Loi n° 2009-669 du 12 juin 2009 *favorisant la diffusion et la protection de la création sur internet*, JORF n°0135 du 13 Juin 2009, p. 9666, texte n°2, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id> (dernière consultation: 5 mars 2018)) qui permettait la coupure d'Internet comme sanction du téléchargement illégal (abandonnée par décret en 2013). Dans une autre mesure, puisque justifiée par des contenus provoquant des actes de terrorisme en faisant l'apologie, ou encore des contenus pédo-pornographique, on citera deux décrets publiés en 2015, en application la 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, texte n°5, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id> (dernière consultation: 5 mars 2018), et de la Loi n°2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure*, JORF n° 0062 du 15 mars 2011, page 4582, texte n°2 (https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000023707312 (dernière consultation: 5 mars 2018)) : le décret n°2015-125 du 5 février 2015 *relatif au blocage de 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*, JORF n°0031 du 6 février 2015 page 1811, texte n° 71, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030195477&categorieLien=id> (dernière consultation: 5 mars 2018), ainsi que le 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*, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030313562> (dernière consultation: 5 mars 2018). La CNIL propose une intéressante infographie résumant quelque peu les procédures de blocage de sites internet pour des contenus faisant l'apologie du terrorisme, provoquant à acte terroriste, ou à caractère pédo-pornographique (<https://www.cnil.fr/fr/infographie-la-procedure-de-blocage-des-sites-internet> (dernière consultation: 5 mars 2018))

³⁸⁶ Loi n°2013-1168 du 18 Décembre 2013 *relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, JORF n°0294 du 19 décembre 2013 page 20570, texte n° 1, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id> (dernière consultation: 5 mars 2018)

³⁸⁷ Loi n°2015-912 du 24 juillet 2015 *relative au renseignement*, JORF n°0171 du 26 juillet 2015, page 12735, texte n°2, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id> (dernière consultation: 5 mars 2018)

³⁸⁸ Loi n°2015-1556 du 30 novembre 2015 *relative aux mesures de surveillance des communications électroniques internationales*, JORF n°0278 du 1 décembre 2015, page 22185, texte n°1, En ligne: <https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte> (dernière consultation: 5 mars 2018)

³⁸⁹ Article L. 851-3 du Code de la Sécurité Intérieure, et L. 854- du Code de la Sécurité Intérieure imposant le système des boîtes noires (algorithme) visant pour l'un les connexions situées en France, et l'autre imposant le système des boîtes noires visant l'interception de communications émises ou reçues à l'étranger.

ce ne sont pas les possibilités nouvelles offertes par le Big data, le data mining, ou encore l'internet des objets, qui permettront d'estomper cette dimension d'internet. Au contraire, ces nouvelles possibilités facilitent encore davantage le stockage et le traitement de données, et permettront une collecte exponentielle de données, notamment personnelles. Ces données peuvent ainsi être exploitées aussi bien par les géants du net dans un but commercial, marketing que par les services de renseignement, comme l'affaire Snowden l'a amplement révélé.

140. Ainsi, pour reprendre les mots de Mathieu Potte-Bonneville, il faut « *dé-totaliser une thématique qu'il est parfois tentant d'énoncer au singulier*³⁹⁰ ». La surveillance diffuse s'est construite à l'image d'une cathédrale, par brique technologique successive, par usage technologique différents pour un même dispositif. Que ce soit dans l'analyse que Potte-Bonneville délivre concernant la biométrie, ou dans l'analyse du dispositif qu'est Internet, il faut garder en tête la suite de la définition de ce terme donnée par Foucault: « *ce que je voudrais repérer dans le dispositif, c'est justement la nature du lien entre ces éléments hétérogènes. Ainsi, tel discours peut apparaître tantôt comme programme d'une institution, tantôt au contraire comme un élément qui permet de justifier et de masquer une pratique qui, elle, reste muette, ou fonctionner comme réinterprétation seconde de cette pratique, lui donner accès à un champ nouveau de rationalité. Bref, entre ces éléments, discursifs ou non, il y a comme un jeu, des changements de position, des modification de fonctions, qui peuvent, eux aussi, être très différents. Troisièmement, par dispositif, j'entends une sorte - disons - de formation, qui, à un moment donné, a eu pour fonction majeure de répondre à une urgence. Le dispositif a donc une fonction stratégique dominante. (...). J'ai dit que le dispositif était de nature essentiellement stratégique, ce qui suppose qu'il s'agit là d'une certaine manipulation de rapports de force, d'une intervention rationnelle et concertée dans ces rapports de forces, soit pour les développer dans telle direction, soit pour les bloquer, ou pour les stabiliser, les utiliser. Le dispositif est donc toujours inscrit dans un jeu de pouvoir, mais toujours lié aussi à une ou à des bornes de savoir, qui en naissent mais, tout autant, le conditionnent. C'est ça le dispositif: des stratégies de rapport de force supportant des types de savoirs et supportés par eux*³⁹¹ ». Internet reflète à merveille l'ensemble des points soulevés par l'auteur En effet, en tant que dispositif

³⁹⁰ Op. Cit. p. 75.

³⁹¹ FOUCAULT Michel, « le jeu de Michel Foucault » (entretien avec D. Colas, A. Grosrichard, G. Le Gaufey, J. Livy, G. Miller, J. Miller, J. - A. Miller, C. Millot, G. Wajeman), *Ornicar?*, *Bulletin périodique du champ freudien*, n°10, juillet 1977, pp. 62-93, in. DEFERT Daniel et EWALD François (sous la direction de), *Michel Foucault, Dits et écrits 1954 - 1988, II. 1976 - 1988*, Editions Quarto Gallimard, 2001, texte n°206, p. 299 - 300

Internet s'intègre dans des rationalités politiques et économiques différentes³⁹², se trouve défini par la variété de ses usages³⁹³, et où la collecte et le traitement de données semblent servir conjointement la lutte contre le terrorisme³⁹⁴, et le marketing agressif des GAFAM et autres sites Internet. Enfin, et comme le rappelle Potte-Bonneville en conclusion de l'article précité: « *dès lors qu'un dispositif, fût-il moderne et bio-technologique, tire sa signification des technologies politiques où il s'intègre; dès lors, que ces technologies tendent moins à se substituer l'une à l'autre dans l'histoire (...) qu'à se ré-agencer en formant, à travers leurs emboîtements inédits, des configurations imprévues, on veillera à vérifier que l'inouï n'est pas, d'abord, une nouvelle façon de combiner l'ancien*³⁹⁵ ».

2. La double nature de la surveillance diffuse

141. L'analyse de la notion de dispositif permet le constat suivant: la surveillance diffuse revêt aujourd'hui deux formes principales. L'une est imposée pour des objectifs de sécurité, protection et prévention des menaces, l'autre est de plus en plus acceptée, ou du moins de plus en plus insidieuse, au quotidien pour des bénéfices marketing. En cela, elle ne s'écarte que peu de l'analyse du panoptique de Foucault, et spécialement de sa conclusion lorsqu'il écrivait que « *le Panopticon ne doit pas être compris comme un édifice onirique : c'est le diagramme d'un mécanisme de pouvoir ramené à sa forme idéale ; son fonctionnement, abstrait de tout obstacle, résistance ou frottement, peut bien être représenté comme un pur système architectural et optique : c'est en fait une figure de technologie politique qu'on peut et qu'on doit détacher de tout usage spécifique*³⁹⁶ ».

142. Le problème posé par les références des analyses contemporaines au Panoptique analysé par Foucault, c'est qu'elles ignorent à tout point de vue cette conclusion de Foucault. Elles conduisent à l'évocation de notions inopérantes. Pour exemple, le recours quasi-systématique à la figure d'un Big brother, ou encore au concept de société de surveillance méconnaissent au plus haut point le caractère démocratique des sociétés dans lesquelles la surveillance diffuse s'établit. La singularité

³⁹² Lutte contre le terrorisme VS marketing agressif

³⁹³ Sécurité, culture, connaissance

³⁹⁴ Discours affiché

³⁹⁵ Op. Cit. p. 75 - 76

³⁹⁶ Op. Cit.

de la surveillance, du contrôle social³⁹⁷, et du recours au Panoptique analysé par Foucault conduit à vouloir faire entrer le phénomène de surveillance diffuse dans des cases préfabriquées. Or, il faut à tout prix garder en tête les conclusions de Foucault, et élargir son analyse pour vérifier sa correspondance avec les mécanismes actuels. Les textes de Michel Foucault fournissent une grille d'analyse, qu'il est nécessaire d'enrichir. Ainsi que le rappelle Ariel Kyrrou en 2010: « *Surveillance? Contrôle? L'analyse de ces deux mots, de leur sens et de leur non sens les plus contemporains aboutit à deux paradoxes. Le premier paradoxe, c'est « l'auto-disqualification » de ces termes à la faveur de leur décryptage. (...). Le second paradoxe est une conséquence directe de cette perte de substance des notions de surveillance et de contrôle selon leur acception classique. Il se traduit par une remise en cause de nos références les mieux établies. Le désir d'actualiser l'étude des mécanismes de pouvoir pousse d'abord à revenir aux sources, à s'abreuver (de nouveau) à la fontaine des deux monstres sacrés de nos multitudes: Foucault et Deleuze. Sauf que leurs lumières, aussi nécessaires soient-elles pour éclairer les prémices d'une réflexion, paraissent vite insuffisantes à tracer un chemin dans la nuit de nos temps numérisés. Comble du désarroi philosophique: la référence qui vient naturellement sous toutes nos plumes (...) est un film hollywoodien : *Minority Report*³⁹⁸ ». Cette référence à Philipp K. Dick opérée par Kyrrou trouve un retentissement dans les écrits d'autres auteurs, et spécialement, Frédéric Neyrat. Ce dernier décrit les systèmes sociaux contemporains comme des sociétés de clairvoyance, terme qu'il emprunte à l'univers de *Minority Report*. Ces sociétés de clairvoyance s'évertuent, selon Neyrat, à « élaborer une sorte de contre-investissement préventif de l'avenir susceptible de réorienter les techniques de contrôle et de surveillance existantes ou en construction. (...). Car s'il est bien question, comme pour tous les genres de « sociétés » de machines et de technologies, et si celles-ci modèlent indubitablement les modalités d'exercice du pouvoir, ces dernières reposent en définitive sur un nouveau rapport à la temporalité dont les termes de surveillance et de contrôle ne parviennent pas à rendre compte³⁹⁹ ». Ainsi que le démontrent Kyrrou et Neyrat, il est nécessaire de replacer la surveillance diffuse dans son contexte temporel. Prétendre que la surveillance diffuse doit se résumer en l'exercice d'un contrôle généralisé, menant, selon François de Bernard, à une « tyrannie*

³⁹⁷ Cette notion sera développée par la suite de l'analyse

³⁹⁸ KYROU Ariel, « L'hypnose de l'à-venir. ou des fables de science-fiction comme moyen de déjouer les pièges de la sousveillance », *Multitudes* 2010/1 (n°40), p. 114 à 125, p. 114-115.

³⁹⁹ NEYRAT Frédéric, « Avant propos sur les sociétés de clairvoyance. « Le progrès consiste à être poussé en avant par la police » (Chesterton), *Multitudes* 2010/1 (n°40), p. 104-111, p. 104

virtuelle⁴⁰⁰ », c'est méconnaître la réalité contemporaine. Cet auteur utilise en 2015 l'image d'une « *société de surveillance générale - qui est nôtre, qui nous contrôle, mais que nous ne contrôlons pas - (...). Surveiller parce que cela serait devenu la vocation principale de l'Etat contemporain, au nom d'une « démocratie » qui s'apparente au Panoptique de Bentham⁴⁰¹ » ». La réduction systématique du phénomène de surveillance diffuse à cette image ne rend pas compte de l'évolution de la surveillance contemporaine. Le recours dans le cadre de cette analyse au concept de surveillance diffuse entendu comme un phénomène de société se justifie par la volonté de ne pas réduire les événements contemporains à une seule et unique notion singulière: la surveillance.*

143. Sa forme actuelle, son ampleur, et la singularité de ses effets font de la surveillance diffuse un objet d'étude complexe. Cette complexité provient de la multiplicité technologique mise en oeuvre dans l'espace public et privé permettant la collecte et le traitement de données; mais également des rationalités différentes qu'elle emporte (économie, politique, sécurité, liberté). La diffusion des dispositifs socio-techniques sur l'espace public - tels que la vidéoprotection, le recours à la biométrie - ont permis la banalisation de l'usage des technologies de surveillance, la rendant ainsi automatique. Cette automatisation, cette automaticité de la surveillance n'est pas sans rappeler les propos de Jacques Ellul, qui dès 1988, s'appuyant sur les travaux de Claude Riveline et son article intitulé « Manifeste pour la désinformatisation de la société⁴⁰² » écrivait: « *autrefois, devant un « mystère de la nature », on réfléchissait. Aujourd'hui, on traduit ses interrogations en systèmes logiques propres à être digérés par la machine. Mais celle-ci est très sélective. Ce qui masque l'appauvrissement, c'est la quantité de faits élémentaires que la machine peut absorber et sa vitesse de traitement: mais « l'intelligence est la préoccupation efficace de l'essentiel ». Or, pourquoi chercher l'essentiel quant on peut tout traiter à la fois !... L'apparition d'un nouvel outil ou d'une nouvelle application est saluée comme une victoire, même si les vertus en sont contradictoires. Ce qui produit cet enthousiasme pour l'ordinateur, ce n'est pas son utilité, effective, mais le fait qu'il donne à n'importe qui l'illusion d'être intelligent⁴⁰³ » ». La surveillance s'appuie sur les systèmes logiques décrit par Riveline et Ellul, et tente d'atteindre une prévision des risques, des menaces, mais également des potentialités d'achat. En ce sens, l'un des premiers traits caractéristiques de la*

⁴⁰⁰ BERNARD François (de), *L'homme post-numérique - Face à la société de surveillance générale*, Editions Yves Michel, 2015, p. 14

⁴⁰¹ Ibid. p. 49.

⁴⁰² RIVELINE Claude, *Manifeste pour la désinformatisation de la société*, Pandore n°17, Février 1982

⁴⁰³ ELLUL Jacques, *Le bluff technologique*, préface de Jean-Luc Porquet, Ellul l'éclaireur, Hachette, 1988 ; réédition Hachette Littératures, collection « Pluriel », 2004, p. 577-578

surveillance diffuse est sa propension au brassage d'informations, sa dimension informationnelle: la collecte, l'enregistrement et le traitement de données personnelles ou non. Cette dernière est organisée en vue de tracer les personnes, d'établir une sorte de traçabilité des individus, mais également et surtout de les réduire à leurs traces. Ces deux assertions n'emportent pas les mêmes conséquences. Dans la première hypothèse - tracer les personnes - la surveillance permet le suivi des individus, l'analyse des comportements normaux ou anormaux⁴⁰⁴, en vue de vérifier la conformité des actions individuelles à la loi⁴⁰⁵. Dans la seconde hypothèse - la réduction de l'individu à sa trace numérique - , la surveillance permet ainsi que le rappelle Eric Sadin, en prenant appui sur l'exemple des téléphones portables et du système GPS, de créer « *de toutes nouvelles conditions de cartographie des personnes et des choses sur une surface de visibilité devenue globale*⁴⁰⁶ ». Ces deux hypothèses correspondent en réalité aux deux temps de pénétration de la surveillance diffuse dans nos sociétés. Ces éléments d'analyse amènent à deux constats. D'une part, les formes de surveillance contemporaine ne permettent pas de rendre compte de la réalité de la surveillance diffuse. D'autre part, cette dernière repose sur la coexistence d'une double nature: une surveillance imposée permettant le suivi des personnes pour vérifier la conformité de leurs actions à la loi, à l'ordre public; une surveillance de plus en plus banalisée, du quotidien, permettant la réduction de l'individu à sa trace numérique.

144. Ce double constat rappelle les conclusions précédentes évoquant l'image du monstre doux de Raffaëlle Simone et l'enrichit de son versant économique, capitaliste. L'analyse de Ariel Kyrou, lorsqu'il évoque « *l'auto-disqualification*⁴⁰⁷ » des termes de surveillance et de contrôle illustrent parfaitement ce propos. Il écrit ainsi: « *le premier paradoxe, c'est « l'auto-disqualification » de ces termes à la faveur de leur décryptage. La surveillance ne surplombe plus le surveillé. Elle s'exerce à hauteur d'individu, chacun prenant tour à tour le statut de surveillé et de surveillant en une danse confuse à ras des champs de pissenlits numériques. D'où ce terme « sousveillance », inventé pour signifier cette plombée nouvelle de la veille de tous sur tous, notamment sur soi-même. Le contrôle,*

⁴⁰⁴ Voir en ce sens les analyses produites par l'ensemble de l'équipe du projet Comportements Anormaux : analyse, Détection, Alerte, financé par l'Agence Nationale de la Recherche en 2006, au titre de son programme concernant les concepts systèmes et outils pour la sécurité globale (ANR_06_SECU_0002). Pour consulter la fiche projet: <http://www.agence-nationale-recherche.fr/?Projet=ANR-06-SECU-0002> (dernière consultation: 5 mars 2018). In. LAVENUE Jean-Jacques, VILLALBA Bruno (éds), *Vidéosurveillance et détection automatique des comportements anormaux - Enjeux techniques et politiques*, Presses Universitaires du Septentrion, 2011.

⁴⁰⁵ La surveillance vise alors ici le recueil d'indices (*a priori*) en vue d'une enquête potentielle, ou aide à la constitution d'éléments de preuves (*a posteriori*).

⁴⁰⁶ SADIN Eric, Op. Cit, p. 15.

⁴⁰⁷ Op. Cit

quant à lui, se désincarne. A l'instar du pouvoir, il n'a plus de tête. Le Léviathan capitaliste et sécuritaire est un « Alien ». Il incube en nous. Il se cache dans notre ventre avant de dévorer notre cerveau. Désormais, ses sbires pratiquent moins la vérification d'identité que le suivi de nos traces digitales et le calcul de nos probabilités d'actions. Ils ne frappent plus l'individu a posteriori, mais a priori, en toute discrétion et sans la moindre violence apparente. Mieux, les anges noirs de la sousveillance voguent au coeur même de notre intérieur, allègrement profilé par les bases de données⁴⁰⁸ ».

⁴⁰⁸ Op. Cit. p. 114

Chapitre 2: Des acteurs multiples au service de l'institutionnalisation de la surveillance diffuse: l'élaboration d'une culture de la surveillance

145. « Hier les enjeux de l'informatique étaient circonscrits : ils étaient commerciaux, industriels ou militaires. Désormais, parce qu'elle s'éparpille en une infinité de petites machines et qu'elle disparaît derrière un réseau aux ramifications illimitées, l'informatique prend dans ses rets la société entière⁴⁰⁹ ». Le phénomène de surveillance diffuse a été permis grâce à l'élaboration progressive de la société de l'information et de la connaissance. Cette élaboration progressive est depuis longtemps analysée par les sciences sociales comme « l'émergence du paradigme techno-informatique⁴¹⁰ ». L'utilisation même du terme de paradigme dans cet expression présuppose une pluralité d'acteurs au service de l'institutionnalisation de la surveillance diffuse. La surveillance diffuse est le fait d'un jeu entre institutions particulières qui ont progressivement permis à la surveillance de se banaliser. En réalité, il est même possible d'affirmer que nous sommes tous devenus acteurs de surveillance diffuse. De la banalisation des usages technologiques, de la banalité de l'évocation de l'intrusivité⁴¹¹ possible de ces dispositifs et de la surveillance, tout se passe en effet comme si toute la société tendait vers une véritable culture de la surveillance.

146. La surveillance diffuse est alors produite par l'alliance des intérêts des leaders du numérique, de leurs alliés institutionnels et politiques (section 1). Par divers moyens, ces acteurs ont organisé la surveillance diffuse de telle sorte à modifier le comportement des individus. Ces derniers, souvent fascinés par la surveillance et devenus Narcisse⁴¹², sont entièrement au service de la surveillance diffuse, et s'intègrent pleinement dans une culture de la surveillance (section 2).

⁴⁰⁹ Rapport Nora - Minc précité p. 30

⁴¹⁰ Nous reprenons les termes d'Armand Mattelart. MATTELART Armand, *Histoire de la société de l'information*, 4ème édition, Collection Repères, Editions La découverte, 2009, p. 30 à 46

⁴¹¹ Sur cette notion d'intrusivité voir TURK Alex, *La vie privée en péril. Des citoyens sous contrôle*, Paris, Odile Jacob, 2011, p. 21 - 22.

⁴¹² Pour un bref rappel mythologique, Narcisse tomba amoureux de son reflet dans un lac, et finit par mourir de ne pouvoir se saisir de ce reflet. Nous employons cette notion à un double égard. Dans un premier temps, la réactivation de l'étude de ce mythe ces dernières années a amené un regard nouveau, voire une analyse plus subtile. On pense ici à la réactivation de ce mythe par Lucien Jerphagnon à travers ses oeuvres, et prises de positions. Ses conclusions concernant l'autosuffisance (érotique) de Narcisse comme pêché principal entraînant son châtement (il se complait dans sa beauté et se noie) semble totalement adaptable à l'homme contemporain. D'autre part, l'analyse psychiatrique et spécialement les analyses de Freud semblent totalement opérantes à nos sociétés. Le dictionnaire de la Psychiatrie définit en effet le narcissisme comme suit: « *Amour de soi-même se marquant par un investissement libidinal du moi, pris en tant qu'objet, par la pulsion sexuelle. C'est en 1914, dans « pour introduire le narcissisme », que Freud donne du terme une définition structurale: le narcissisme ne correspond plus à un stade de l'évolution sexuelle qui viendrait s'insérer entre l'autoérotisme et l'amour objectal, mais représente plutôt une stase de la libido qui resterait fixée sur le moi tout au long de sa constitution* », in. POSTEL Jacques, *Dictionnaire de la psychiatrie*, Collection In Extensio, Larousse, 2011

Section 1: La surveillance diffuse et la convergence des intérêts des leaders du numérique et de leurs alliés institutionnels et politiques

147. Notre époque constitue un moment charnière. La surveillance diffuse semble atteindre son paroxysme de nos jours d'un point de vue technologique, mais également du point de vue de son imprégnation, de sa pénétration dans la société. L'élaboration et la construction conjointe entre secteur privé et public du marché du numérique ne suffit pas pour appréhender une telle banalisation de la surveillance dans nos sociétés. La convergence des intérêts du secteur privé et public est essentiellement fondée sur une nouvelle forme de pouvoir qualifiée par certains de soft power⁴¹³ et de storytelling en ce qui concerne les entreprises du secteur privé. En réalité, ces nouvelles expressions correspondent à ce que Foucault envisageait au travers de la notion de gouvernementalité⁴¹⁴ principalement alimentée par la peur, les peurs (paragraphe 1). Cette dernière a permis à la sécurité de devenir le nouveau point de convergence de ces deux secteurs (paragraphe 2).

Paragraphe 1: La convergence des intérêts des leaders du numérique et de leurs alliés institutionnels et politiques: une nouvelle forme de pouvoir au service de la surveillance diffuse

148. Plus qu'un soft power exercé par l'Etat combiné à une forme de storytelling exercée par les entreprises (A), la surveillance diffuse est aujourd'hui pleinement banalisée du fait d'une gouvernementalité par la peur (B).

A. L'organisation de la surveillance diffuse par le secteur privé et le secteur public: entre storytelling et softpower

149. En relation internationale, le soft power s'oppose traditionnellement au hard power. Ce dernier rassemble les ressources traditionnelles de la puissance d'Etat: souveraineté, capacités militaires et économiques. Le soft power, quant à lui, s'organise autour de la capacité d'un Etat à

⁴¹³ NYE Joseph, *Bound to lead: the changing nature of American power*, Basic Books, 1990, p188-201; et du même auteur, *Soft power - the means to success in world politics*, Public Affairs, New York, 2004. Le soft power est à distinguer selon Joseph Nye du hard power, c'est-à-dire des ressources traditionnelles de la puissance d'Etat telles que la souveraineté, les capacités militaires et économiques

⁴¹⁴ Nous empruntons cette notion à Michel Foucault qui voit en ce concept un mode spécifique d'exercice du pouvoir.

faire adhérer et participer pleinement les individus et d'autres Etats à une ambition politique et étatique plutôt que de les contraindre par la force⁴¹⁵. L'exercice d'un soft power par l'Etat correspond alors à une sorte de force de persuasion douce (1). Mis au service de la surveillance diffuse, ce soft power a permis de légitimer la priorité donnée par l'Etat aux développements technologiques. Et c'est dans ce cadre que la convergence des intérêts du secteur public et du secteur privé a pu se développer (2).

1. L'exercice d'un soft power par l'Etat: force de persuasion douce au service de la surveillance diffuse

150. Avant même d'évoquer la convergence des intérêts du secteur public et du secteur privé pour ce qu'elle est vraiment, il existe d'abord une convergence d'un point de vue des besoins et des évolutions technologiques, une sorte d'imitation politique entre les différents Etats dans la construction de l'infrastructure du numérique. Ainsi, la synapse informationnelle, c'est-à-dire le point de contact ayant permis cette convergence a été permise par la priorité politique donnée à ce marché en devenir. Afin de permettre la plénitude économique de ce marché, l'harmonisation internationale des objectifs, l'ouverture de la concurrence sur le marché, la régulation et la réglementation des services et infrastructures de la société de l'information, les actions de soutien à la recherche et au développement sont autant d'éléments qui ont engendré la convergence réelle des intérêts des principaux acteurs dans la société de l'information. Ces éléments doivent servir de base et de cadre général à l'étude et au constat de cette même convergence dans le cadre de la surveillance diffuse. En effet, la nouvelle priorité politique donnée à la préoccupation sécuritaire a engendré les mêmes effets que la préoccupation des autoroutes de l'information: harmonisation et convergence internationales pour parvenir à cet objectif, réglementation des techniques et infrastructures de sécurité, soutien fort à la recherche et développement en la matière, ouverture de la concurrence, et externalisation de la sécurité au profit du secteur privé.

151. Pour parvenir à ces résultats, et justifier de la priorisation politique donnée au développement technologique, des auteurs évoquent très tôt l'apparition d'un soft power. En 1990, le professeur Joseph Nye écrit que le soft power qui « *consiste à tenter d'abord d'obtenir par la persuasion séductrice les résultats que l'on pourrait aussi atteindre par la force. Il s'agit d'amener*

⁴¹⁵ NYE Joseph, *Soft power - the means to success in world politics*, Public Affairs, New York, 2004. L'auteur écrit ainsi que le soft power correspond à « *Co-opt people rather than coerce them* » (p. 5).

les autres à adhérer à des normes et des institutions qui incitent ou induisent au comportement désiré. Le soft power peut prendre appui sur la capacité d'établir l'agenda (ordre du jour) de manière à façonner les préférences des autres⁴¹⁶ ». L'exercice de ce soft power par l'Etat requiert, comme le rappelle, Joseph Nye et Robert Keohane, « de la crédibilité afin de pouvoir exercer cette persuasion séductrice⁴¹⁷ ». Par le ralliement de la recherche, qu'elle soit issue des think tank⁴¹⁸, des associations, d'ONG, sur la question de la société de l'information, de la connaissance, de la communication, ou plus globalement d'Internet, la crédibilité du pouvoir étatique et son ambition au développement technologique ont été légitimées. En effet, et ainsi que le rappelle Nye et Keohane, « la capacité à diffuser librement des informations accroît le potentiel de persuasion en politique internationale. Les ONG et les Etats sont ainsi plus à même d'influencer les croyances des peuples au-delà de leurs propres juridictions⁴¹⁹ ». La recherche a permis l'adoption d'une perception positive sur les nouvelles technologies, Internet, la société de l'information. Bien que Nye et Keohane développent leur analyse au regard de l'expérience américaine, ces conclusions trouvent également application en Europe, et spécialement dans le cadre de la surveillance diffuse. La recherche, qu'elle soit publique, ou privée, a largement contribué à la priorisation sur l'agenda politique des préoccupations liées au développement des technologies, de l'information et de la communication, puis à la sécurité. Se faisant, une véritable convergence des intérêts entre le secteur public et le secteur privé a pu naître et se propager.

152. La sécurité comme enjeu politique, économique et social, n'est pas née avec le 11 septembre 2001. La société de l'information s'est développée dans les années 2000, les entreprises du numérique ont organisé leur activité autour du Web 2.0, des biens informationnels et des nouvelles

⁴¹⁶ Voir en ce sens: NYE Joseph, *Bound to lead: the changing nature of American power*, Basic Books, 1990, p188-201; et du même auteur, *Soft power - the means to success in world politics*, Public Affairs, New York, 2004.

⁴¹⁷ NYE Joseph, KEOHANE Robert, *Power and Interdependence in the Information Age*, Foreign Affairs, vol. 77, n°5, pp; 81-94, p.90. En ligne: <https://fr.scribd.com/document/305854708/56826563-Power-and-Interdependence-in-the-Information-Age-pdf> (dernière consultation: 5 mars 2018)

⁴¹⁸ La société de l'information a vu apparaître avec elle ces sortes de machines à penser d'experts auto-proclamés. Bien qu'Internet ne soit pas le point d'origine du développement de la société de l'information, ces machines à penser, spécialement américaines, ont contribué à développer le phénomène Internet en parallèle des travaux des institutions traditionnelles de la recherche (universités, instituts). Cette participation forte de la société civile dans le cadre de la recherche sur le phénomène Internet a permis quelques années plus tard à la gouvernabilité par la peur de s'installer dans nos sociétés démocratiques. Dans les années 80, Internet devient le domaine de recherches de prédilection de groupements tels que la Rand Corporation, le CATO Institute, l'Internet Policy. En parallèle, les universités et laboratoires de recherches se mobilisent sur le sujet. Des associations se développent tels que l'Electronic Foreign Frontier Foundation, ou encore l'Electronic Privacy Information Center. Cet ensemble brouille les frontières de la recherche traditionnelle, participe à renforcer la propagation des nouvelles technologies, et contribue à la mutation de la puissance étatique.

⁴¹⁹ NYE Joseph, KEOHANE Robert, *Power and Interdependence in the Information Age*, Op. Cit. , p.94.

technologies. L'Etat, quant à lui, a investi massivement dans les infrastructures, la recherche et le développement. Pourtant, dès 1997, deux rapports d'information - l'un rendu par l'office parlementaire des choix scientifiques et technologiques à l'Assemblée Nationale française⁴²⁰, l'autre fait au nom de la mission commune de l'information par Messieurs Joyandet, Hérisson et Türk⁴²¹ - évoquent le déclin potentiel de la société de l'information en France. Ces deux rapports démontrent que « *aucun Etat ne saurait se retrancher à l'écart de ces réseaux, sauf à se résoudre au déclin. L'accès à l'information est en effet la source majeure de création de richesse dans les sociétés post-industrielles où l'investissement immatériel depuis déjà dix ans est devenu plus important que l'investissement matériel*⁴²² ». Aussi, par crainte « *d'une vassalisation culturelle* », « *pour l'avenir de son pays et de sa culture* » le sénateur Laffitte s'emploie à demander une « *vraie mobilisation* » autour de la question de la société de l'information. Il écrit ainsi, que « *si une vraie mobilisation n'est pas déclenchée, avec les moyens financiers et médiatiques adéquats, c'est à coup sûr le déclin. La France, dans ce cas, subirait la Société de l'Information, mais n'en serait ni l'un des bénéficiaires, ni l'un des acteurs majeurs*⁴²³ ».

153. Plus que la société de l'information, le progrès et la technique⁴²⁴, imposent aux individus et à l'Etat de s'adapter de manière permanente. Rappelons ici, les caractéristiques de la Technique que Jacques Ellul mentionnait dès 1954⁴²⁵: l'automatisme du choix technique, l'auto-accroissement, l'unicité ou l'insécabilité, l'entraînement des techniques, l'universalisme et l'autonomie de la technique. A travers son analyse, et les mots des sénateurs précités, on comprend que la société de

⁴²⁰ LAFFITTE Pierre, Office Parlementaire d'évaluation des choix scientifiques et technologiques, *Rapport n° 3335 sur les réseaux grands débits et l'entrée dans la société de l'information*, enregistré à la Présidence de l'Assemblée nationale le 7 février 1997, En ligne: <http://www.assemblee-nationale.fr/10/rap-off/i3335-t1.pdf> (dernière consultation: 5 mars 2018)

⁴²¹ JOYANDET Alain, HERISSON Pierre, TÜRK Alex, *Rapport d'information n° 436 Mission commune d'information sur l'entrée dans la société de l'information*, Sénat, annexe au procès-verbal de la séance du 25 septembre 1997, En ligne: https://www.senat.fr/rap/r96-436/r96-436_mono.html (dernière consultation: 5 mars 2018)

⁴²² Ibid.

⁴²³ LAFFITTE Pierre, Office Parlementaire d'évaluation des choix scientifiques et technologiques, *Rapport n° 3335 sur les réseaux grands débits et l'entrée dans la société de l'information*, enregistré à la Présidence de l'Assemblée nationale le 7 février 1997, p. 3, En ligne: <http://www.assemblee-nationale.fr/10/rap-off/i3335-t1.pdf> (dernière consultation: 5 mars 2018). Aussi et concernant les moyens médiatiques adéquats employés dans ce texte, Laffitte est assez clair à ce sujet, puisqu'il renvoie en note de bas de page au fait que « *commissions, comités, colloques et nouveaux rapports ne changeront pas la face des choses. Les multiples colloques qui se succèdent ne touchent qu'une faible frange d'initiés déjà convaincus* ». Le sénateur Laffitte appelle donc de ces vœux une intervention médiatique au sens propre du terme. les médias, télévisions, journaux, radios doivent se rallier à cet objectif, et l'Etat semble appeler de ces vœux ici un véritable marketing publicitaire lié à la société de l'information.

⁴²⁴ Au sens développé par Ellul et Heidegger

⁴²⁵ Voir ELLUL Jacques, *La Technique ou l'Enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990, p74 à 135.

l'information, le progrès emporte une sorte de darwinisme économique, social et politique effrayant. D'après Charles Darwin, dans son oeuvre sur l'origine des espèces⁴²⁶ les individus les plus aptes survivent au détriment des plus faibles. La diffusion de la surveillance a été permise par le progrès et la Technique. Ces éléments ont été consacrés par la mise sur l'agenda politique de la société de l'information comme nouvelle préoccupation sociale. L'enjeu sécuritaire, son idéologie, a permis de donner un nouveau souffle au développement technique dans la société⁴²⁷ à la fin des années 90⁴²⁸. Cette notion ainsi que la surveillance diffuse participent d'une véritable mécanique sociale, institutionnelle et politique en co-production avec les citoyens et les entreprises du secteur privé.

2. Le storytelling ou la participation pleine et entière du secteur privé à la légitimation technologique

154. Alors qu'il se posait la question de la bonne gouvernance du Prince, et la question de savoir s'il vaut mieux, pour lui, d'être aimé que craint, Machiavel écrit que « *le meilleur serait d'être l'un et l'autre. Mais, comme il est très difficile que les deux choses existent ensemble, je dis que, si l'une*

⁴²⁶ DARWIN Charles, *L'origine des espèces: au moyen de la sélection naturelle ou la préservation des races favorisées dans la lutte pour la vie*, Flammarion, 2008, et spécialement le chapitre 4 de son analyse intitulé : la sélection naturelle ou la persistance du plus apte

⁴²⁷ Sur le lien entre la technique, le progrès et le couple économie et économie politique, il semble nécessaire de citer à nouveau Jacques Ellul: « *Quoique la technique soit certes créatrice de valeurs, il semblait qu'elle provoquait de fortes distorsions entre les divers secteurs de la vie économique, et en même temps il y avait un si grand nombre d'innovations techniques qu'il devenait impossible de les faire entrer toutes en usage pratique, d'aboutir à des marchandises à lancer sur le marché. Non point que l'on atteignît des saturations, mais j'avais l'impression que, à la fois la réalité et la science économique étaient débordées par cette énorme prolifération, qu'il était impossible de rationaliser dans un ensemble économique cohérent, que les modèles, à base de libéralisme, de keynésianisme, ou de socialisme étaient nettement insuffisants (...). Autrement dit, il me semblait que le rapport technique-économie se modifiait. Certes, la technique dans son origine et sa créativité restait toujours autonome, mais ses débouchés dans le concret n'étaient plus assurés. L'économie jouait le rôle de butoir et de limites aux entreprises techniciennes. (...) La croissance technique devenait fonction des possibilités de l'économie. Et nous voilà, dans la dernière décennie parvenus à un quatrième stade de cette relation technique-économie, celui que j'appelle maintenant le stade de la Sagesse de l'économie politique. La technique accélère incessamment son mouvement d'innovation. Mais elle a tout à fait cessé d'être autonome vis-à-vis de l'économie, de la réalité économique, du fonctionnement de cette économie* ». In. ELLUL Jacques, *Le bluff technologique*, préface de Jean-Luc Porquet, Ellul l'éclairer, Hachette, 1988 ; réédition Hachette Littératures, collection « Pluriel », 2004, p.446 447. Cette interdépendance entre technique et économie s'est largement matérialisée en 1997. Et, l'économie politique aidée par les « entreprises techniciennes », ont voulu par l'enjeu sécuritaire réactiver les débouchés économiques, sociaux et politiques du progrès, de la Technique, de la société de l'information et de la connaissance, devenant surveillance diffuse.

⁴²⁸ De manière plus globale, certains auteurs démontrent que la sécurité comme enjeu politique, économique et social est devenue « *incontournable de nos sociétés contemporaines, a connu ces trois dernières décennies des bouleversements majeurs dans ses modes de production, de distribution et de contrôle. Dans un contexte général de recul de l'Etat-providence au profit de la montée d'une idéologie néolibérale, les institutions publiques responsables de la sécurité (la police en tête) ont vu une multitude de nouveaux acteurs - pour la plupart privées - émerger et leur disputer une hégémonie qui leur semblait pourtant acquise* ». In. MULONE Massimiliano, *La marchandisation de la sécurité : facteur de responsabilisation des individus ou des entreprises?*, *Déviance et Société* 2012/3, Vol. 36, p325 - 338, p. 325, En ligne: <http://www.cairn.info/revue-deviance-et-societe-2012-3-page-325.htm> (dernière consultation: 5 mars 2018)

*doit manquer; il est plus sûr d'être craint que d'être aimé*⁴²⁹ ». Le numérique et, par là, la surveillance diffuse, ont réussi à faire coexister ces deux éléments par la transformation des relations internationales non plus dominées par les Etats mais bien par la technologie qui s'est diffusée dans tous les corps sociaux⁴³⁰. En deçà des relations internationales, c'est donc déjà dans le corps social constitué par la société qu'il faut analyser les stratégies d'influence mises en places. Ecrivant sur la diplomatie numérique, Thomas Gomart déclare qu'elle est souvent « *présentée comme un avatar de la diplomatie publique, c'est-à-dire comme un moyen d'entrer directement en contact avec les sociétés civiles en utilisant les réseaux sociaux afin de mettre en oeuvre des stratégies d'influence*⁴³¹ ». Et d'ajouter qu'elle « *trouve ses racines aux Etats-Unis dans le concept de smart power*⁴³² ».

155. La notion de smart power, développée par Joseph Nye⁴³³, doit être analysée à la fois comme une entreprise de communication menée par l'Etat et relayée par les entreprises, mais également comme la combinaison de tous les moyens d'actions possibles. L'exercice de ce smart power se matérialise principalement par l'élaboration de partenariats avec le secteur privé dans le but d'accroître les bénéfices liés au commerce international, principalement aidé par les technologies et l'innovation⁴³⁴. Ainsi dans le cadre spécifique du numérique, selon Thomas Gomart, pour être mis en oeuvre ce smart power repose essentiellement « *sur le principe de connectivité selon lequel la*

⁴²⁹ MACHIAVEL Nicolas, *Le Prince et autres textes*, Union Générale d'Editions, Collection 10-18, Paris, 1962, p. 66 - 67 (spécialement le chapitre 17 intitulé « *de la cruauté et de la clémence, et s'il vaut mieux être aimé que craint* »).

⁴³⁰ Voir en ce sens: GOMART Thomas, « De la diplomatie numérique », *la vie numérique*, Revue des deux mondes, janvier 2013, pp. 131 - 141, Disponible en ligne à l'adresse suivante: https://www.ifri.org/sites/default/files/atoms/files/ifri_gomart_10-01-2013_revuedesdeuxmondes_diplomatie_numerique.pdf (dernière consultation: 5 mars 2018)

⁴³¹ Ibid. p. 134.

⁴³² Ibid.

⁴³³ En ce sens, voir: ARMITAGE Richard, NYE Joseph, *A smarter, more secure America*, Center for Strategic and International Studies, Commission on Smart Power, Library of Congress Cataloging in Publication Data, 2007, En ligne: <https://carnegieendowment.org/files/csissmartpowerreport.pdf> (dernière consultation: 5 mars 2018). Dans ce rapport, les auteurs écrivent que le smart power doit être analysé comme la combinaison habile entre le soft power et le hard power : « *Smart power is neither hard nor soft—it is the skillful combination of both. Smart power means developing an integrated strategy, resource base, and tool kit to achieve American objectives, drawing on both hard and soft power. It is an approach that underscores the necessity of a strong military, but also invests heavily in alliances, partnerships, and institutions at all levels to expand American influence and establish the legitimacy of American action. Providing for the global good is central to this effort because it helps America reconcile its overwhelming power with the rest of the world's interests and values* » (p. 7). Ainsi, le smart power signifie le développement d'une stratégie intégrée, d'une base de ressources et d'une sorte de trousse à outils pour atteindre les objectifs américains, en s'inspirant à la fois du hard power et du soft power. C'est une approche qui envisage à la fois la nécessité d'une armée forte mais qui, également, investit massivement dans des alliances, des partenariats et des institutions à tous les niveaux pour élargir l'influence américaine et établir la légitimité de l'action américaine. Voir également: NYE Joseph, *The future of power*, Public Affairs, New York, 2011.

⁴³⁴ Dans le rapport précité deux chapitres entiers sont consacrés au commerce international, à la force du secteur privé américain et de son système économique, mais également aux solutions créatives que peuvent apporter l'innovation et les technologies (voir spécialement pp. 53 - 60)

centralité d'un acteur dépend de sa capacité à générer des connexions, et ainsi d'imposer son agenda en suscitant l'adhésion. Pour Washington, il s'agissait de se positionner « comme un hub informationnel et idéologique » et de recourir à la diplomatie numérique pour servir « un empire médiatique global », capable de façonner non seulement l'opinion mondiale mais surtout de la segmenter en fonction des objectifs poursuivis. La diplomatie numérique américaine prétend accompagner les efforts de « démocratisation » à travers le monde et, à ce titre, fait de la liberté d'Internet un axe prioritaire, notamment dans son rapport à la Chine⁴³⁵ ». Si les Etats ont joué un rôle de persuasion technologique, les entreprises ont elles-aussi influencé le déterminisme technologique. Dans les faits le smart power, compris comme « une force de persuasion séductrice⁴³⁶ », pour paraphraser Joseph Nye, est également à la disposition des entreprises. Au travers d'une politique marketing visant à rendre séduisant, et nécessaire l'usage de l'informatique et l'accès à Internet, les entreprises du numérique sont parvenues à réaliser le double objectif qu'elles s'étaient fixées: la consommation technologique et à la mise en données du monde.

156. En effet, en termes d'idéologies, la société de l'information est porteuse de plusieurs sens. Plus qu'un enjeu de pouvoir pour les Etats et les entreprises, elle est aussi synonyme d'accès à la connaissance et à la culture. Pour atteindre cet objectif, la numérisation et la dématérialisation sont au coeur des processus innovants des entreprises du secteur privé. Ainsi que le rappelle le rapport Curien-Muet⁴³⁷ « *l'avènement des technologies de l'information et la communication en réseau rend possible une dissociation complète entre l'information et son support physique. (...). Désormais, le lien contenant/contenu est rompu, les réseaux numériques permettant en effet la circulation de contenus d'information - textes, sons, images - débarrassés de la gangue de tout contenant: l'information est ainsi en train de devenir un bien économique autonome⁴³⁸ » ». Le rapport sur la société de l'information énonce, à titre d'exemple la musique, et plus globalement l'édition musicale. L'information, la connaissance et la culture semble donc, dans cette société, être des termes équivalents. Des entreprises tels que Google s'évertuent, comme le rappelle Barbara*

⁴³⁵ Op. Cit. p. 135

⁴³⁶ Op. Cit.

⁴³⁷ CURIEN Nicolas, MUET Pierre-Alain, *Rapport sur la société de l'information*, Conseil d'Analyse économique, La Documentation française, Paris, 2004, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/044000180.pdf> (dernière consultation: 5 mars 2018)

⁴³⁸ Ibid. p. 13

Cassin, à « *faire que tout le savoir du monde soit connecté directement à nos esprits*⁴³⁹ ». Et d'ajouter, concernant ces trois mots (information, connaissance et culture) que « *« nous » nous conformons à cet usage. Cette équivalence fonctionne constamment, en particulier dans tous les textes définitionnels de la société que « nous » constituons, cette littérature grise rédigée par et pour l'Europe. A knowledge-based society, « une société de la connaissance »: c'est ainsi que l'Union Européenne se définit et définit le monde aujourd'hui: le syntagme est tellement répété qu'on croit le comprendre*⁴⁴⁰ ».

157. La consommation technologique et la mise en données du monde sont également permises du fait d'une réelle entreprise de communication mise en place par les entreprises, et envisagée par certains auteurs sous l'expression de storytelling⁴⁴¹. Pour illustrer le propos, on citera notamment: Apple et son slogan du « *Think different*⁴⁴² » pour la promotion de son nouvel ordinateur portable, Google et sa promotion de son navigateur Chrome : « *à vous de créer le web* », SFR et sa solution domotique « *ce qui est smart (intelligent) c'est d'être chez soi même quand on y est pas, pilotez votre maison à distance* », Facebook et sa promotion de ce réseau social « *Facebook, c'est un peu comme une chaise où l'on va s'asseoir pour échanger ensemble* »... Dans l'ensemble de ces cas, le récit semble plus important que la véracité des faits. La question qui se pose alors est de savoir où se situe la limite de ces conteurs d'histoires ? Dans certains cas, il semble bien que l'on dépasse le simple cadre du storytelling. Ce point avait d'ailleurs été soulevé par Jacques Ellul, lorsqu'il écrivait que « *en réalité, lorsque l'État use d'une propagande complète et technique, il devient fatalement totalitaire. M. Driencourt constate d'ailleurs avec surprise que « le pays qui se vante d'être le plus libéral (les États-Unis) est celui où la technique de direction de la pensée est par sa perfection la plus proche des pratiques totalitaires ; où tout un peuple habitué à vivre en groupe s'en remet aux experts pour déterminer sa ligne de conduite spirituelle* »⁴⁴³ ».

⁴³⁹ CASSIN Barbara, *Google-moi, La deuxième mission de l'Amérique*, Collection Banc Public, Editions Albin Michel, 2007, p. 114.

⁴⁴⁰ Ibid.

⁴⁴¹ Sur le rôle des publicitaires, il est nécessaire de lire les travaux de Seth Godin, et spécialement son livre intitulé *Tous les marketeurs sont des menteurs*, traduction de *All Marketers are Liars*, Les éditions Transcontinental, 2006. A la lecture de ce livre, on comprend que les entreprises nous racontent des (belles) histoires devenant ainsi des « storyteller ». Ce qui est vrai pour les entreprises s'applique également à la communication des États sur les notions de sécurité, de terrorisme et de menace (entre storytelling et propagande ?). Pour preuve, l'étude de Christian Salmon : *Storytelling, La machine à fabriquer des histoires et à formater les esprits*, Éditions La découverte, 2007, et le documentaire issu de cette étude disponible à l'adresse suivante : http://www.dailymotion.com/video/xoclpj_storytelling-la-machine-a-raconter-les-histoires_tech (dernière consultation: 5 mars 2018)

⁴⁴² Pensez différemment

⁴⁴³ ELLUL Jacques, *La Technique ou l'enjeu du siècle*, Op. Cit., p. 260 et s.

B. La gouvernementalité par la peur : facteur essentiel de la banalisation contemporaine de la surveillance diffuse

158. En deçà de la modernité des expressions de smart power, de soft power, ou encore de storytelling, il n'y a en réalité qu'une forme d'agencement inédite entre les souhaits de l'Etat et des entreprises, une réelle convergence des intérêts dominée par le déterminisme technologique et par un mode spécifique du pouvoir qui vise moins à prôner la coercition que la séduction. Foucault avait déjà envisagé ce champ stratégique de pouvoir à travers la notion de gouvernementalité. Selon lui, il faut entendre par gouvernementalité: « *l'ensemble constitué par les institutions, les procédures, analyses et réflexions, les calculs et les tactiques qui permettent d'exercer cette forme bien spécifique, quoique très complexe de pouvoir qui a pour cible principale la population, pour forme majeure de savoir l'économie politique, pour instrument essentiel les dispositifs de sécurité. Deuxièmement, par « gouvernementalité », j'entends la tendance, la ligne de force qui, dans tout l'Occident, n'a pas cessé de conduire, et depuis fort longtemps, vers la prééminence de ce type de « gouvernement » sur tous les autres : souveraineté, discipline, et qui a amené, d'une part, le développement de toute une série d'appareils spécifiques de gouvernement, et, d'autre part, le développement de toute une série de savoirs*⁴⁴⁴ ».

159. Appliquée à la surveillance diffuse cette notion signifie que les institutions, spécialement l'Etat, n'exerce plus par le pouvoir souverain de la formulation de la loi, mais par des moyens directs de gouverner la conduite des individus. Et c'est par l'instrumentalisation de la peur, des peurs, que l'Etat et les entreprises parviennent à rendre la surveillance totalement acceptable pour le citoyen. Evoquer la notion de peur dans le cadre d'une analyse juridique de la surveillance diffuse peut paraître original de prime abord. La peur n'est, selon sa définition, qu'un sentiment d'angoisse éprouvé en présence ou à la pensée d'un danger, réel ou supposé, d'une menace (souvent dans avoir, faire peur). En soi, elle n'est qu'une émotion difficilement palpable pour le juriste. Pourtant, son instrumentalisation progressive⁴⁴⁵ a permis l'élaboration d'une nouvelle forme, une pratique de

⁴⁴⁴ FOUCAULT Michel, *Sécurité, territoire, population - Cours au collège de France. 1977 - 1978*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 2004, pp.111-112

⁴⁴⁵ De l'année 1976, où Roger Gicquel introduisait son journal télévisé avec l'invective suivante: « *Bonsoir, La France a peur. je crois qu'on peut le dire aussi nettement. La France connaît la panique (...)* » à nos jours; la peur n'a eu de cesse d'être instrumentalisée, afin de la faire monter au rang des réalités sociales sur laquelle responsables politiques, entreprises et médias s'évertuent à agir. C'est avec cette phrase que Roger Gicquel ouvre son journal télévisé sur TF1, le 18 février 1976, à propos du meurtre d'un enfant et de l'affaire Patrick Henri. En ligne: <http://www.ina.fr/video/CAA87014358> (dernière consultation: 5 mars 2018)

gouvernement qu'il est nécessaire de comprendre et d'analyser.

160. Ainsi que le résumait Vaclav Havel, dans sa lettre à Gustav Husak, il ne faut plus prendre la peur « *dans le sens psychologique courant, à savoir comme une espèce d'émotion concrète: en général, nous ne voyons pas autour de nous des gens tremblant de peur, mais des citoyens à l'allure satisfaite et confiante. Il s'agit d'une peur plus profonde, qui a un sens éthique: une participation plus ou moins consciente à la conscience collective d'un danger permanent et omniprésent, un souci pour ce qui est ou pourrait être menacé, une accoutumance à la menace comme composante essentielle du monde naturel, une assimilation toujours plus complète, évidente et habile des diverses formes d'adaptation au monde extérieur comme seul système de défense efficace*⁴⁴⁶ ». Bien que l'auteur dénonce par cette lettre écrite en 75 l'oppression du régime instauré en Tchécoslovaquie sous la présidence de Gustav Husak, ses conclusions sur le concept de peur comme vecteur de pouvoir restent très actuelles. Le concept de peur est devenu chez les chercheurs contemporains un objet d'étude⁴⁴⁷. En 2007, un ouvrage regroupant chercheurs dans le numérique⁴⁴⁸, historiens⁴⁴⁹ et économiste⁴⁵⁰ introduit la peur comme suit: « *émotions brutes, réactions affolées, déclarations irrationnelles. De toutes parts montent les discours de la peur, des peurs. Peur des agressions, peur de l'insécurité, de la précarité et du chômage. De la violence, de la marginalisation, de devenir SDF, d'être délocalisé. Peur de l'autre, de l'ouvrier chinois, du plombier polonais, du migrant malien, de son collègue de travail, du terroriste. Peur aussi de ce que l'on mange, de ce que l'on boit, de son corps, de son image. Du cataclysme nucléaire, du changement climatique, de la banquise qui disparaît, de la biodiversité qui s'étirole. Peur intime et peur publique. peur de tout. Cette montée de la parole collective sur l'angoisse pourrait être positive (...). Or c'est tout le contraire qui se passe: loin de se réduire, nos peurs grandissent*

⁴⁴⁶ HAVEL Vaclav, *Lettre ouverte à Gustav Husak*, adressée le 8 avril 1975 in. HAVEL Vaclav, *Essais politiques*, textes réunis par Roger Errera et Jan Vladislav, Collection Liberté de l'esprit, Calmann- Lévy, 1989, p. 12.

⁴⁴⁷ On notera trois ouvrages principaux. Les deux premiers présentent les effets de la peur sur nos sociétés. Le dernier est une étude enrichissante sur les usages politiques de peur, son invocation et son instrumentalisation. VIVERET Patrick, *Pourquoi ça ne va pas plus mal ?*, Collection Transversales, Fayard, 2005; SUE Roger, *La société contre elle-même*, Collection Transversales, Fayard, 2005; CREPON Marc, *La culture de la peur - I. Démocratie, identité, sécurité*, Collection La philosophie en effet, Galilée, 2008.

⁴⁴⁸ Valérie Peugeot, prospectiviste au sein du laboratoire de sciences sociales et humaines d'Orange Labs; présidente de l'association Vecam, et ancienne Vice-présidente du Conseil National du Numérique (2013 à 2015), signe l'introduction de cet ouvrage.

⁴⁴⁹ Leyla Dakhli est spécialiste de l'histoire intellectuelle et sociale du monde arabe contemporain. Georges Vigarello est historien spécialisé dans l'histoire de l'hygiène, de la santé, des pratiques corporelles et des représentations du corps, directeur de l'Ecole des hautes études en sciences sociales et co-directeur du Centre Edgar Morin.

⁴⁵⁰ Bernard Maris (1946 - 2015), économiste, écrivain et journaliste notamment pour Charlie Hebdo

*chaque jour un peu plus, mutent dans nos intimités, envahissent notre espace public*⁴⁵¹ ». En 2008, d'autres évoquent la « *géopolitique de l'émotion*⁴⁵² », et mettent en exergue l'approfondissement, l'extension et la diversification de la peur dans un contexte dominé par l'inquiétude et l'actualité anxigène.

161. Les démocraties occidentales, plus globalement l'ensemble des continents sont touchés aujourd'hui par la Peur. On comprend alors que l'on n'évoque plus vraiment le simple sentiment, la simple émotion décrite en introduction. Et c'est bien dans la nature protéiforme de la Peur, par son invocation, son instrumentalisation, que de nouveaux usages politiques et économiques ont pu naître. A travers la liste des peurs⁴⁵³ supposées, de celles relevant de l'imaginaire et des métaphores collectives, ou réelles, chacun d'entre nous se retrouve, s'identifie. Et, si ce n'est pas le cas, le gouvernement nous les rappelle. A cette liste de peurs correspond en effet une action nouvelle du gouvernement. Ainsi, la lutte contre l'obésité, la malbouffe, ou pour reprendre les mots de la liste précédemment citée « la peur de ce que l'on mange », engendre une politique de santé publique très médiatisée: il faut « manger bouger », et comme si cela ne suffisait pas, il faut également manger « cinq fruits et légumes par jour »⁴⁵⁴. Pour lutter contre le cancer, des politiques belges se mettent en scène afin de convaincre leur population de diminuer voire d'arrêter leur consommation d'alcool pendant 150 jours à grands renforts de slogan du type, « à l'eau, Estaimpuis⁴⁵⁵ », et d'usages numérique (application mobile permettant de comprendre sa consommation)⁴⁵⁶. Dans le cadre de la lutte contre la délinquance, un plan national d'équipement en vidéoprotection est mis en place, cela afin de moderniser les moyens de commandement de la Préfecture, tout en étant encadré par un comité d'éthique⁴⁵⁷. Tout un ensemble de questions, de problèmes publics, cristallisé dans cette liste

⁴⁵¹ DAKHLI Leyla, MARIS Bernard, SUE Roger, VIGARELLO Georges, *Gouverner par la peur*, Collection Transversales, Fayard, 2007, p. 7 - 8.

⁴⁵² MOISI Dominique, *La géopolitique de l'émotion*, Nouvelle édition, Collection Champs actuel, Flammarion, 2008

⁴⁵³ Evoquée précédemment

⁴⁵⁴ Ensemble de publicités prouvées scientifiquement inefficace. Cf. REBEIHI Ali, *Quand la publicité alimentaire nous raconte des histoires*, France Inter, 3 Mai 2017, En ligne: <https://www.franceinter.fr/emissions/grand-bien-vous-fasse/grand-bien-vous-fasse-03-mai-2017> (dernière consultation: 5 mars 2018)

⁴⁵⁵ Estaimpuis est une commune de Belgique

⁴⁵⁶ Le député-bourgmestre d'Estaimpuis a lancé en janvier 2017 une grande campagne pour que toute la commune se mette à l'eau, afin de lutter contre le cancer. Voir par exemple: <http://www.nordeclair.be/1772871/article/2017-01-27/estaimpuis-toute-la-commune-se-met-a-l-eau-avec-daniel-senesael> (dernière consultation: 5 mars 2018)

⁴⁵⁷ Exemple pour le plan 1000 caméras de Paris: <http://www.prefecturedepolice.interieur.gouv.fr/layout/set/print/Vous-aider/Actions-de-prevention/Dispositifs-ZSP-et-vidéoprotection/Le-Plan-de-vidéoprotection-pour-Paris> (dernière consultation: 5 mars 2018)

de peurs, est de plus en plus dépolitisé, et perd de sa valeur juridique, par un nouveau mode de traitement: le traitement médiatique⁴⁵⁸. La peur est devenue, ainsi que le rappelait Vaclav Havel le « *matériau essentiel de construction de notre structure sociale actuelle*⁴⁵⁹ », ou comme le précise Marc Crépon « *un principe de gouvernement*⁴⁶⁰ » qui fragilise énormément les fondations d'une démocratie⁴⁶¹.

162. En matière de surveillance diffuse, cette gouvernementalité par la peur s'est traduite dans les discours de légitimation sécuritaire précédemment évoqués, dans la participation active des citoyens, allant jusqu'à leur consentement à être surveillé pour être protégé. Ces glissements de l'action de l'Etat, comme nouvel aspect de la démocratie, rappellent les caractéristiques de la technique évoquées par Ellul, que reprend la surveillance. Puisque cette dernière est recherche d'efficacité et d'universalité, l'organisation de la société devient en elle-même recherche d'efficacité et d'universalité. Cette recherche ne peut se faire sans le soutien de l'État, qui progressivement s'éloigne de l'État démocratique et se transforme en État tentaculaire, planificateur, et s'approche d'une forme de plus en plus totalitaire⁴⁶². Ce glissement de la conception de l'État démocratique à l'État tentaculaire a été décrit par Tocqueville lorsqu'il imaginait « *sous quels traits nouveaux le despotisme pourrait se produire dans le monde*⁴⁶³ » dans « De la démocratie en Amérique ». Il

⁴⁵⁸ Voir en ce sens, les travaux concernant la question climatique du sociologue Jean-Baptiste Comby, qui montre que cette dernière est totalement dépolitisée à travers son traitement médiatique. COMBY Jean-Baptiste, *La question climatique: genèse et dépolitisation d'un problème public*, Collection Raison d'agir - Cours et travaux, Liber, 2015

⁴⁵⁹ Op. Cit. p. 12.

⁴⁶⁰ Voir en ce sens: CREPON Marc, *La culture de la peur - I. Démocratie, identité, sécurité*, Collection La philosophie en effet, Galilée, 2008.

⁴⁶¹ L'instrumentalisation de la peur, des peurs permet de ne plus fonctionner par la force obligatoire de la loi, mais par des invectives gouvernementales. On comprend alors qu'en fonction des cibles d'insécurité que le gouvernement désigne, les médias remplacent l'action légale du gouvernement, et alimentent la peur. Or, la question est de savoir: de quelles actions réelles dispose le citoyen contre cette nouvelle forme ou ce nouveau système de gouvernement ?

⁴⁶² Bien que nous vivions toujours dans des États démocratiques par le fait, entre autres, de la reconnaissance de nos droits et libertés fondamentales, la technique, et la surveillance engendre le totalitarisme. Il faut reprendre l'analyse de Jacques Ellul: « *la technique conduit l'État à se faire totalitaire, c'est-à-dire à tout absorber de la vie. Nous avons noté qu'il en est ainsi par suite de l'accumulation des techniques entre les mains de l'État; que les techniques se relient les unes aux autres en même temps qu'elles s'engendrent mutuellement et que cela forme un réseau qui enserme toutes nos activités ; et lorsque l'État saisit un fil de ce réseau, il amène progressivement à lui (« volens nolens ») toute la matière avec la méthode. Ainsi, même lorsque l'État est résolument libéral et démocratique, il ne peut faire autrement que devenir totalitaire. Il le devient d'ailleurs, soit directement, soit, comme aux États-Unis, par personnes interposées ; mais le système arrive finalement, malgré sa diversité, au même résultat. (...) La technique engendre le totalitarisme.* », in, Ellul Jacques, *La Technique ou l'enjeu du siècle*, Op. Cit., 1990, p. 258-259. Ces quelques mots s'appliquent au phénomène de la surveillance diffuse. Nos droits et libertés fondamentales ont beau être reconnus à travers des textes nationaux, européens, et internationaux, les États se montrent de plus en plus friands de toutes informations concernant les individus: entre accumulation des techniques de surveillance entre les mains de l'État, aidé par le secteur privé, et interconnexion de ces techniques dans un environnement transnational, les États ne peuvent faire autrement que devenir totalitaire et de se rapprocher d'un idéal totalitaire (sans torture, sans brutalité, sans arbitraire)

⁴⁶³ DE TOCQUEVILLE Alexis, *De la démocratie en Amérique II*, (3ème et 4ème parties), Collection Garnier-Flammarion, Éditions Flammarion, 1999, p. 146

écrivait alors : « *au-dessus de ceux-là [les hommes] s'élève un pouvoir immense et tutélaire, qui se charge seul d'assurer leur jouissance et de veiller sur leur sort. il est absolu, détaillé, régulier, prévoyant et doux. Il ressemblerait à la puissance paternelle si, comme elle, il avait pour objet de préparer les hommes à l'âge viril; mais il ne cherche, au contraire, qu'à les fixer irrévocablement dans l'enfance; il aime que les citoyens se réjouissent, pourvu qu'ils ne songent qu'à se réjouir. Il travaille volontiers à leur bonheur; mais il veut en être l'unique agent et le seul arbitre; il pourvoit à leur sécurité, prévoit et assure leurs besoins, facilite leurs plaisirs, conduit leurs principales affaires, dirige leur industrie, règle leurs successions, divise leurs héritages, que ne peut-il leur ôter entièrement le trouble de penser et la peine de vivre ?⁴⁶⁴ » Cet État planificateur, ce monstre doux⁴⁶⁵ vient coordonner l'action de la surveillance diffuse, aidé par le secteur privé, et vice versa. Cette action de coordinateur de la surveillance ne se résume pas à un simple encadrement de l'État, ou à de simples mandats, ou encore à des requêtes faites auprès du secteur privé dans le cadre d'activités de renseignements. Bien au contraire, la diffusion de la surveillance est englobante, recherche d'efficacité et d'universalité dans la société. Elle a pour objectif l'organisation de la plasticité sociale, de la malléabilité des individus. Dans cette recherche permanente d'efficacité, la souveraineté de l'Etat ne semble plus vraiment se manifester par son monopole dans l'usage de la violence, ni même par son pouvoir de décision quant aux mesures d'exception ou d'urgence à envisager. Les événements récents, et les cinq renouvellements de l'Etat d'urgence tendent à confirmer ce propos, et à le rendre particulièrement éclairant, tant la signification de ce terme perd de son caractère exceptionnel. L'Etat d'urgence, tel qu'appliqué de nos jours en France, semble étayer l'argument de la gouvernementalité par la peur, puisqu'il correspond aujourd'hui à une recherche de légitimité et de réassurance politique. La souveraineté de l'Etat démocratique ne s'organise plus seulement autour d'un jeu de balance entre pouvoir et contre-pouvoir. Elle s'organise aussi autour de la désignation de cibles potentielles d'insécurité (la nourriture, les émigrés, la maladie mentale ou physique, les délocalisations d'entreprise, la précarité, l'identité...), et de garantie d'une protection contre ces nouvelles cibles sans cesse renouvelées. Dans cette nouvelle forme de gouvernement, l'Etat à la fois juge et partie, se place lui-même en dehors de toute emprise.*

163. La gouvernementalité par la peur est le facteur essentiel de diffusion, de consentement à la

⁴⁶⁴ Ibid.

⁴⁶⁵ SIMONE Raffaele, *Le Monstre doux - L'Occident vire-t-il à droite ?*, traduit par Katia Bienvenu, Collection Le Débat, Gallimard, 2010

surveillance. Sans que les individus puissent s'en rendre compte, la surveillance diffuse s'est installée dans la vie quotidienne. Elle est devenue banale, naturelle, grâce à cette culture de la peur qui se révèle être la nouvelle façon de gouverner les Hommes, en France, en Europe et à l'international. Pourtant, très tôt des auteurs alertaient l'opinion publique sur la nocivité de cette nouvelle administration des individus. Deux citations donneront le ton et la mesure de cette toxicité. Ainsi que l'écrit Arkadi Vainer: « *Je pense que l'esclavage est le foyer où se nichent toutes nos peurs, qu'elles naissent dans cet abîme gluant et obscur et tissent autour de nous une toile humide et nous enferment comme dans un cocon. Les petites peurs nous enseignent à ne plus penser, à ne plus nous effrayer devant les véritables et grandes pertes: la privation de libertés, la mort de l'âme, la séparation avec l'homme de sa vie. (...). Nous avons accepté de jouer le rôle de gens heureux dans cette représentation cauchemardesque. Nous sommes tous prêts à supporter les défauts provisoires et les quelques excès exceptionnels, puisque, pour le reste, nous sommes globalement heureux et satisfaits. Personne ne peut plus nous aider tant que, dans un élan de dégoût général, nous n'aurons pas arraché avec un cri strident, la répugnante toile d'araignée de la peur greffée en nous comme un second système de circulation sanguine⁴⁶⁶ ».*

164. Bien que les auteurs de cette citation décrivent la situation de l'URSS des années 1970, on comprend par ces mots l'ampleur des possibilités qu'offrent la culture de la peur sur l'organisation sociale et sur les individus. Et, puisque ces mots sont tirés d'un roman, on citera à nouveau Vaclav Havel dans sa lettre à Gustav Husak pour donner plus de poids à cette conclusion. « *L'attention de la société - pour faciliter la domination du Pouvoir - est-elle consciemment détournée d'elle-même, c'est-à-dire des affaires de la société: en fixant toute l'attention de l'individu à « ras de terre » sur ses intérêts de consommateur, on veut le priver de la capacité de percevoir son degré croissant d'asservissement spirituel, politique et moral. Réduit au rôle de porteur unidimensionnel des idéaux de la société de consommation, il doit se transformer en matière souple, sujette à toutes manipulations⁴⁶⁷ ».* La gouvernamentalité par la peur, organisée par les Etats, relayée par les médias et les entreprises, a permis la pleine diffusion de la surveillance dans nos sociétés. Pire encore, elle a engendré sa banalisation, tant dans les usages des technologies, que dans les pratiques individuelles. La modification des comportements humains est, comme le souligne ces deux citations, l'une des conséquences de ce nouveau mode de gouvernement des hommes ou d'administration des choses.

⁴⁶⁶ VAINER Arkadi, VAINER Gueorgui, Traduction Pierre Léon, *La corde et la pierre*, Collection Série Noire, Editions Gallimard, 2006, p. 380 - 381

⁴⁶⁷ Op. Cit. p. 19

Paragraphe 2: La marchandisation de la sécurité: fondement et aboutissement de la convergence des intérêts du secteur public et du secteur privé dans le cadre de la surveillance diffuse

165. L'idéologie de la société de l'information est fortement liée à une logique de marché économique. En cinq années, de 1994 à 1999, une véritable bulle spéculative et boursière s'est créée autour des entreprises « Dot-com », spécialisées dans les technologies de l'information et de la communication. Entre les fusions et acquisitions de sociétés de cet environnement économique à des sommes exorbitantes⁴⁶⁸, et les entrées en bourse des premiers géants d'Internet l'économie de l'information connaît son apogée en 2000. La même année, en mars, la bulle spéculative autour des sociétés spécialisées dans les nouvelles technologies de l'information et de la communication éclate. Malgré la disparition de certaines start-up, cette folie économique et financière qui a accompagné le développement d'Internet a contribué au développement, voire à la consécration des premiers géants d'Internet: Microsoft, Yahoo, Ebay, Apple, Amazon, Google et Facebook entrent en bourse quelques années plus tard en 2004, et en 2012. En quelques années, le krach de 2000 est oublié, et les Google, Amazon, Facebook, Apple et Microsoft deviennent des valeurs boursières fortes⁴⁶⁹, au point tel de devenir des leaders mondiaux appelés les GAFAM⁴⁷⁰. Ces derniers, ainsi que les nouvelles entreprises spécialisées dans les technologies de l'information et de la communication ont su également se renouveler passant de la distribution de biens informationnels et du web 2.0, à une présence nécessaire et sécurisante dans la vie quotidienne des individus.

166. En parallèle, l'Etat renouvelle son intérêt pour la dématérialisation et la technicisation de son espace: le « droit à » la sécurité devient le nouvel enjeu de la convergence institutionnelle, politique et économique (A). Cette convergence institutionnelle, politique et économique, couplée aux nouvelles pratiques managériales de gestion des politiques publiques de l'Etat font de la

⁴⁶⁸ On citera à l'appui de cet adjectif les exemples suivants: en 1998, le rachat par AOL de la société netscape pour une valeur de 4 milliards de dollars, et la capitalisation boursière d'AOL la même année; en 1998 également Walt Disney achète Infoseek et lance sa filiale spécialisée dans la communication et Internet: la Walt Disney Internet Group; en 1999 Yahoo opère l'acquisition de deux sociétés Geocities (pour 3,57 milliards de dollars), puis [broadcast.com](http://www.broadcast.com) (pour 5,7 milliards de dollars). On notera également que la plupart des capitalisations boursières des futurs géants d'internet s'opère dès la fin des années 90. C'est notamment le cas pour AOL, Yahoo et Ebay.

⁴⁶⁹ Pour preuve l'article des Echos paru le 20 février 2015, écrit par Pierrick Fay, intitulé : *Apple, Amazon, Google et Facebook plus forts que le CAC 40*, En ligne: http://www.lesechos.fr/20/02/2015/lesechos.fr/0204174102171_apple--amazon--google-et-facebook-plus-forts-que-le-cac-40.htm# (dernière consultation: 5 mars 2018)

⁴⁷⁰ On apprend dans l'article précité qu'un des leader mondial du courtage sur les marchés financiers, le groupe BCG, titre une de ses notes comme suit: « *tous gaga des Gafa* », et ce, pour souligner la toute-puissance de ces quatre sociétés sur le marché financier. On ajoute aujourd'hui Microsoft à ce conglomérat d'entreprises.

sécurité, puis de la surveillance diffuse, une activité marchande (B).

A. Le « droit à » la sécurité comme renouveau d'une convergence institutionnelle, politique et économique

167. Au-delà de l'analyse des discours tenant à l'idéologie sécuritaire et à la propagation de la surveillance, il est nécessaire de s'interroger sur l'activation du concept de sécurité par la mise sur agenda politique de cette notion et des transformations qui en découlent. Les penseurs de la « société de surveillance » lient régulièrement sa montée en puissance avec les attentats du 11 septembre 2001. Dans son introduction au livre intitulé la globalisation de la surveillance, Armand Mattelart entame son analyse par les événements du 11 septembre 2001. Il écrit ainsi que « *la multiplication des mesures d'exception dans le cadre de la « guerre globale » contre le terrorisme s'est conjuguée, depuis le 11 septembre 2001, sous les régimes démocratiques, avec l'ingérence croissante des dispositifs de surveillance dans la vie quotidienne des citoyens. A surenchère sécuritaire, surenchère technologique⁴⁷¹* ».

168. En réalité, si les attentats du 11 septembre 2001 ont cristallisé les discours sécuritaires et les discours liés à l'aboutissement d'une société de surveillance, c'est parce qu'ils ont permis une convergence tant internationale qu'institutionnelle et politique sur l'objectif de sécurité, l'enjeu de la sécurité humaine, le durcissement des mesures pénales et l'ordinarité de mesures juridiques et légales autrefois considérés comme exceptionnelles⁴⁷². Plus loin, c'est également l'externalisation de la sécurité au profit du secteur privé qui doit être questionnée par la reconnaissance de ce « droit à ». Bien que justifiée par le passage de l'Etat providence à l'Etat gendarme (1), cette

⁴⁷¹ MATTELART Armand, *La globalisation de la surveillance - Aux origines de l'ordre sécuritaire*, Editions la découverte, 2007, p.5. Bien que cet auteur analyse dans les pages suivantes le lien entre surveillance et sécurité vu comme un projet de société construit dès la seconde moitié du 18^{ème} siècle, cette référence aux attentats du 11 septembre 2001 dès l'introduction brouille l'analyse du lecteur dès le départ. L'auteur retrace rapidement les analyses de Michel Foucault, en combinant trois ouvrages de référence en la matière: *Surveiller et Punir*, *Naissance de la biopolitique*, et *Sécurité, territoire et population*. Mattelart indique ainsi : « *De la vision panoptique centrée sur la surveillance comme dressage du corps aux fins de l'éducation de l'âme, Foucault glisse vers un autre paradigme, la « biopolitique » et son projet de « société de sécurité » (...). A la différence de la société disciplinaire qui s'exerce sur les corps, la société de sécurité s'exerce sur l'ensemble de la société, la « vie des hommes » (par contraste avec le pouvoir sur la mort qui caractérisait la prérogative du souverain). La première est centripète; l'individu, enfermé dans son alvéole, qui est vu mais ne voit jamais, est « objet d'une information, jamais sujet dans une communication » insiste Foucault dans *Surveiller et punir*. La seconde est centrifuge; elle désenclave; son mode de communication élargit l'horizon physique et mental ».* (p. 13 - 14)

⁴⁷² Voir sur ce point: DELMAS-MARTY Mireille, *Libertés et sûreté dans un monde dangereux*, Editions du Seuil, Collection La couleur des idées, 2010

reconnaissance de ce droit à la sécurité est la cause d'une transformation plus profonde de la gouvernance dans nos sociétés modernes (2).

1. Le droit à la sécurité comme symptôme d'une transformation du rôle de l'Etat rendue nécessaire par la surveillance diffuse

169. De manière générale, l'avènement de la notion de sécurité dans nos sociétés contemporaines s'inscrit dans un mouvement successif de transformation du rôle de l'Etat, de volonté des réductions des dépenses étatiques, ainsi que d'un intérêt pour un marché économique suscité par les nouvelles pratiques de sécurité. Ainsi que le rappelle Massimiliano Mulone, il faut alors voir en la privatisation de la sécurité et « *le retour en force de l'industrie de la sécurité privée (...) une cause et un symptôme d'une transformation plus profonde de la gouvernance dans nos sociétés modernes*⁴⁷³ ».

170. Elle en est un symptôme qui s'explique par le passage de l'Etat gendarme à l'Etat providence, notion qui se trouve fortement réactivée en France et en Europe du fait de leur inscription dans une économie néo-libérale. Alors qu'à l'origine, l'Etat-providence revêtait en Europe un caractère corporatiste et prévoyait une intervention de l'Etat pour se substituer au marché, si ce dernier ne pouvait assurer le bien-être de la population; il devient aujourd'hui de plus en plus libéral. Tout en conservant l'intention d'assurer le bien-être de la population, le modèle de l'Etat-providence européen se retrouve de plus en plus dans un rôle d'acteur ou de moteur du marché économique. Le martèlement politique des années 80⁴⁷⁴, et la reconnaissance dans la loi de 1995⁴⁷⁵ de la sécurité comme première des libertés et droit fondamental ne fait d'ailleurs que renforcer ce propos de l'oscillation du rôle de l'Etat entre protecteur du bien-être de ses citoyens, et régulateur du marché. Il semble important de rappeler que le début des années 80 est marqué en France par l'évolution des faits de délinquance. Un rapport de décembre 1982⁴⁷⁶, remis au premier

⁴⁷³ Op. Cit. p. 237

⁴⁷⁴ Pour une rétrospective intéressante de la formule politique devenue une sorte de principe juridique, voir: FRADIN Andréa, « *La sécurité est la première des libertés. » Ou l'inverse?*, NouvelObs, Rue 89, 19 novembre 2015, En ligne: <http://tempsreel.nouvelobs.com/rue89/rue89-politique/20151119.RUE8786/la-securite-est-la-premiere-des-libertes-ou-l-inverse.html> (dernière consultation: 5 mars 2018)

⁴⁷⁵ Op. Cit.

⁴⁷⁶ Commission des maires sur la sécurité, *Rapport au Premier Ministre: Face à la délinquance: prévention, répression, solidarité*, Décembre 1982, Collection des rapports officiels, La documentation Française, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/834037801.pdf> (dernière consultation: 5 mars 2018)

ministre par la Commission des maires sur la sécurité, insiste sur l'aggravation du sentiment d'insécurité, la progression de la délinquance depuis les années 60, ainsi que le développement du taux de criminalité. La commission des maires propose dans le cadre de ce rapport une nouvelle politique d'action faite de prévention, de répression et de solidarité face à la délinquance. Dix ans plus tard, le colloque de Villepinte, organisé par le Ministère de l'Intérieur les 24 et 25 octobre 1997⁴⁷⁷, s'interroge également sur les moyens de faire reculer l'insécurité. Selon Lionel Jospin, « *assurer la sécurité des citoyens est un devoir pour l'Etat. l'insécurité est donc un échec pour l'Etat*⁴⁷⁸ ». Fort de ce constat, l'ancien Premier ministre développe trois principes devant guider l'action de l'Etat: « *la sécurité est d'abord une responsabilité de l'Etat; la sécurité doit être égale pour tous; la sécurité dépend pour une large part des relations de confiance établies entre les services en charge de la sécurité et la population*⁴⁷⁹ ».

171. A travers ces mots, on voit bien la double fonction du nouvel Etat-providence, à la fois subjectif et objectif, à la fois planificateur et paternaliste. Et c'est dans cette double fonction de l'Etat que la sécurité a pu se symptomatiser, se révéler. Comme le rappelle Frédéric Ocqueteau, « *dans nos sociétés sécularisées, la protection contre les infortunes du sort (des personnes, des biens et de l'information) est devenue un besoin quasi obsessionnel, considérée comme le premier des droits. Au cours de l'histoire on est passé de l'Etat gendarme à l'Etat providence, au point que les différentes instances de socialisation productrices d'ordre social et de régulation des désordres (famille, école, travail,...) ont été placées sous la dépendance ultime de l'Etat protecteur*⁴⁸⁰ ». Ainsi que cette citation le fait comprendre, l'Etat paternaliste a accoutumé le citoyen à être dépendant de la protection qu'il assure, et donc à solliciter son intervention pour être protégé. Le citoyen s'est donc habitué progressivement à son rôle de « *consommateur-client*⁴⁸¹ », et spécialement de nos jours consommateur-client de « *sécurité-protection*⁴⁸²», mais également de surveillance.

⁴⁷⁷ Ministère de l'intérieur, Service de l'information et des relations publiques, *Des villes sûres pour des citoyens libres: actes du colloque de Villepinte, 24-25 octobre 1997*, La Documentation Française, En ligne: <http://www.vie-publique.fr/documents-vp/villepinte.pdf> (dernière consultation: 5 mars 2018)

⁴⁷⁸ Ibid. p.89

⁴⁷⁹ Ibid. p. 90

⁴⁸⁰ OCQUETEAU Frédéric, *Les nouveaux besoins de protection*, texte de la 157ème conférence de l'Université de tous les savoirs donnée le 5 juin 2000, in. UNIVERSITE DE TOUS LES SAVOIRS, *Le Pouvoir; l'Etat, la Politique*, Volume 9, Odile Jacob, Mars 2002

⁴⁸¹ Ibid.

⁴⁸² Ibid.

172. Les mots de Tocqueville, ainsi que la notion de gouvernementalité par la peur prennent également plus de sens. L'Etat se positionne en tant que gestionnaire des risques et des menaces qui pèsent sur la société, mais également en tant que gestionnaire des peurs de ses citoyens. Aidé par les entreprises du numérique, chaque nouvelle peur trouve une solution technologique maximisant le sentiment de sécurité et de protection. Ces conclusions permettent à des auteurs d'alerter l'opinion publique quant à la logique de « *catastrophisme, d'administration du désastre et de soumission durable*⁴⁸³ » mise en place, correspondant à l'élaboration d'un « *empire du moindre mal*⁴⁸⁴ ». Pour Riesel et Semprun, « *les deux principaux traits de la mentalité progressiste, à son époque triomphante, étaient la foi en la capacité de la science et de la technologie à maîtriser rationnellement la totalité des conditions de vie (naturelles et sociales), et la conviction que pour ce faire les individus devaient se plier à une discipline collective propre à assurer le bon fonctionnement de la machine sociale, afin que la sécurité soit garantie à tous. On voit que ces traits, loin d'être effacés ou estompés, sont plus marqués encore dans ce progressisme honteux qu'est le catastrophisme. D'une part on croit inébranlablement à la possibilité de connaître exactement tous les « paramètres » des problèmes « environnementaux »; d'autre part on accepte comme une évidence que cela passe par un renforcement des contraintes imposées aux individus*⁴⁸⁵ ». La surveillance diffuse se situe aujourd'hui dans cette problématique: l'ambition de connaître exactement de tous les paramètres des problèmes individuels, environnementaux et sociaux. Pour se faire, l'Etat, à travers la reconnaissance du droit à la sécurité renforce les contraintes pesant sur les individus. Pourtant, ainsi que ces auteurs le relèvent « *personne ne peut ignorer qu'à l'image de la guerre toujours perdue que la folie hygiéniste mène contre les microbes, chaque progrès de la sécurisation a entraîné l'apparition de nouveaux dangers, de risques inédits, de fléaux jusque-là insoupçonnés; que ce soit dans l'urbanisme, où les espaces « criminogènes » s'étendent avec le contrôle, la ségrégation, la surveillance, (...). On dirait au contraire que chaque nouvel échec de la sécurisation le renforce dans sa conviction d'une tendance générale vers le mieux*⁴⁸⁶ ».

173. En cela, il est possible de rejoindre Jean-Claude Michéa lorsqu'il évoque « *l'empire du*

⁴⁸³ RIESEL René, SEMPRUN Jaime, *Catastrophisme, administration du désastre et soumission durable*, Editions de l'encyclopédie des Nuisances, Paris, 2008

⁴⁸⁴ MICHEA Jean-Claude, *L'empire du moindre mal - Essai sur la civilisation libérale*, Editions Flammarion, Collection Champs Essai, 2010

⁴⁸⁵ RIESEL René, SEMPRUN Jaime, Op. Cit., p. 37

⁴⁸⁶ Ibid. p. 37 - 38.

*moindre mal*⁴⁸⁷ ». Cette tendance générale vers le mieux envisagée par Riesel et Semprun correspond en tout point à la démonstration de Michéa. Se livrant à un essai sur la civilisation libérale, Michéa avertit son lecteur dès les préliminaires de son ouvrage: « *c'est précisément la tentation d'instituer ici-bas, le règne du Bien et de la Vertu, qui constitue la source ultime de tous les maux qui n'ont cessé d'accabler le genre humain. Cette critique de la « tyrannie du Bien » a, naturellement, un prix. Elle oblige à considérer la politique moderne comme un art purement négatif: celui de définir, en somme, la moins mauvaise société possible. C'est en ce sens que le libéralisme doit être compris, et se comprend lui-même, comme la politique du moindre mal*⁴⁸⁸ ». L'Etat, aidé par le marché, est le principal acteur de cette politique du moindre mal. Cette dernière engendre sécurisation, sécurité, protection, prévention, surveillance. Elle est, ainsi que le relève Riesel et Semprun, sans cesse renouvelée, transformant ainsi toujours plus le rôle de l'Etat et renforçant la surveillance diffuse. Pire encore, elle permet l'entretien d'une véritable culture de la surveillance⁴⁸⁹.

2. Le droit à la sécurité comme transformation profonde de la gouvernance dans nos sociétés modernes

174. La sécurité, son externalisation au profit du secteur privé, plus récemment sa privatisation, est la cause d'une transformation plus profonde de la gouvernance dans nos sociétés modernes. Face à la demande croissante des citoyens en quête de protection et donc de sécurité, l'offre de sécurité proposée par l'Etat coûte cher. Un double déficit se constate: d'une part au niveau purement économique; d'autre part l'Etat a de plus en plus de mal à pourvoir seul à la sécurité de ses citoyens. Ainsi que le démontre Frédéric Ocqueteau, bien que « *les polices publiques civiles et militaires ont historiquement réussi à s'imposer comme les seules agences de régulation ou de canalisation des désordres publics (...), il n'en va pas de même de la défense de la paix publique au quotidien, (...); cette fonction majeure de la police apparaît aujourd'hui en crise et la sécurité urbaine demande à être repensée à la lumière des mutations affectant les modes de vie contemporains*⁴⁹⁰ ». La reconnaissance du droit fondamental à la sécurité s'inscrit dans cette pensée nouvelle de la défense de la paix publique au quotidien. Entre promotion d'une économie de la sécurité et séduction

⁴⁸⁷ Op. Cit.

⁴⁸⁸ MICHEA Jean-Claude, Op. Cit., p. 10.

⁴⁸⁹ Voir section 2 de ce chapitre.

⁴⁹⁰ OCQUETEAU Frédéric, Op. Cit.

politique, la fundamentalité du droit à la sécurité, reconnue légalement, permet en effet à l'Etat de transformer la gouvernance de cette activité régalienn⁴⁹¹.

175. Ainsi que le note Massimiliano Mulone, « *la centralité de l'Etat comme pourvoyeur principal, voire monopolistique, de la sécurité étant notamment remise en cause. Et bien que la prolifération de récentes lois(...) puisse à première vue faire croire à une volonté de l'Etat d'affirmer sa préséance dans le champ de la sécurité, une lecture plus attentive nous indique plutôt une volonté de promouvoir l'autorégulation de l'industrie, en mettant l'accent sur les conditions d'épanouissement de cette dernière*⁴⁹² ». La centralité de l'Etat comme pourvoyeur principal de la sécurité décrite par Mulone doit être mise en relation avec la notion d'ordre public. Traditionnellement, ce concept prétorien est lié pour le Conseil Constitutionnel au bon ordre, la sécurité, la salubrité, la tranquillité publique et, plus globalement la paix publique. Il n'est explicitement mentionné qu'une fois dans les textes constitutionnels à l'article 11 de la Déclaration de 1789 qui dispose clairement que « *nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble par l'ordre public établi par la loi*⁴⁹³ ». Conçu à la fois comme un bouclier et une limite de certaines libertés fondamentales⁴⁹⁴, l'ordre public représente une garantie pour la sécurité globale des personnes et des biens. Combiné au droit à la sûreté⁴⁹⁵, l'ordre public tel qu'envisagé traditionnellement représente une vaste conception de vie ensemble

⁴⁹¹ La sécurité, l'armée, la justice et la monnaie font partie des activités régaliennes de l'Etat.

⁴⁹² MULONE Massimiliano, *La marchandisation de la sécurité : facteur de responsabilisation des individus ou des entreprises?*, Déviance et Société 2012/3, Vol. 36, p325 - 338, p. 327, En ligne: <http://www.cairn.info/revue-deviance-et-societe-2012-3-page-325.htm> (dernière consultation: 5 mars 2018). Nous rejoignons totalement les conclusions de Massimiliano Mulone concernant la promotion de l'autorégulation de l'industrie tout en mettant l'accent sur les conditions d'épanouissement de cette dernière. La reconnaissance du droit fondamental à la sécurité au niveau national, et au niveau international, la reconnaissance de la sécurité humaine en sont des parfaits exemples.

⁴⁹³ Déclaration des Droits de l'Homme et du Citoyen de 1789 (DDHC), En ligne: <https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789> (dernière consultation: 5 mars 2018)

⁴⁹⁴ Par exemple au sujet de la liberté d'expression, l'article 10 alinéa 2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales déclare que « *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, 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* », http://www.echr.coe.int/documents/convention_fra.pdf (dernière consultation: 5 mars 2018)

⁴⁹⁵ Définit à l'article 2 de la DDHC comme suit: « *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* ». Les articles 7, 8 et 9 de la Déclaration précisent ce droit à la sûreté comme étant: le droit de n'être accusé, arrêté ou détenu que dans les cas prévus par la loi et selon les formes qu'elle a prescrites, le droit de n'être condamné qu'à des peines strictement et évidemment nécessaires établies par une loi qui ne peut être rétroactive et la présomption d'innocence. L'article 5 de la Convention européenne de sauvegarde des droits de l'Homme évoque le droit à la liberté et à la sûreté en son article 5, avant d'évoquer les conditions dans lesquelles il peut être porté atteinte à la liberté individuelle.

dans un espace démocratique. Garantie d'une protection des citoyens, droit des citoyens face au gouvernement, garantie judiciaire du respect des droits et libertés individuelles, et prescriptions de droits et de devoirs dans la société démocratique, sûreté et ordre public représentent dans les faits la mise en jeu de pouvoirs et contre-pouvoirs de l'ensemble des acteurs de cette société. Par la réduction contemporaine de l'ordre public et de la sûreté, à la notion de sécurité, cet ensemble est bouleversé par des règles, non plus juridiques, mais économiques (du marché) de la sécurité. En réalité, par la reconnaissance de ce « droit à » la sécurité, tout se passe comme si l'Etat s'imposait un droit-créance. Pour la doctrine, la notion de droits-créances, donc par extension le droit à la sécurité, désigne les droits sociaux mettant à la charge des obligations positives supposant une mise en oeuvre législative⁴⁹⁶. On retrouve ici la logique mise en place dans le cadre de l'élaboration de la société de l'information où l'Etat se fixe des principes et des buts à atteindre de concert avec la société civile. Ces éléments permettent alors plusieurs conclusions que l'on empruntera pour partie à Mireille Delmas-Marty. Pour parvenir à cet objectif de sécurité, l'Etat retrouve un rôle de préconisateur, il anticipe les besoins et influence les choix de la société civile, incitant par exemple la recherche scientifique et les investissements dans ce domaine⁴⁹⁷. Delmas-Marty estime que du fait d'une urgence devenue permanente⁴⁹⁸, l'Etat se lance dans une anticipation de la sécurité fondée sur la prévention et le principe de précaution. Elle écrit ainsi que « *certaines des dangers planétaires évoqués ont des effets potentiellement illimités dans le temps. Selon qu'ils sont liés à la*

⁴⁹⁶ Pour une analyse pertinente des droits-créances, voir: GAY Laurence, *La notion de « droits-créances » à l'épreuve du contrôle de constitutionnalité*, Cahiers du Conseil Constitutionnel n° 16, juin 2004, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/nouveaux-cahiers-du-conseil/cahier-n-16/la-notion-de-droits-creances-a-l-epreuve-du-controle-de-constitutionnalite.51982.html> (dernière consultation: 5 mars 2018); RAPOPORT Cécile, *L'opposabilité des « droits-créances » constitutionnels en droit public français*, communication présentée aux journées de l'association française de droit constitutionnel, En ligne: <http://www.droitconstitutionnel.org/congresParis/comC8/RapportTXT.pdf> (dernière consultation: 5 mars 2018); RANGEON François, *Droits - libertés et droits créances : les contradictions du préambule de 1946*, CURAPP, https://www.u-picardie.fr/curapp-revues/root/37/francois_rangeon.pdf_4a083159afa30/francois_rangeon.pdf (dernière consultation: 5 mars 2018)

⁴⁹⁷ En ce sens: DELMAS-MARTY Mireille, Op. Cit., p. 192

⁴⁹⁸ Qui n'est pas ici à entendre comme la notion juridique d'Etat d'urgence, totalement vidée de son sens aujourd'hui. En ce sens: DELMAS-MARTY Mireille, *De l'état d'urgence au despotisme doux*, Libération, 16 juillet 2017, En ligne: http://www.liberation.fr/debats/2017/07/16/de-l-etat-d-urgence-au-despotisme-doux_1584185 (dernière consultation: 5 mars 2018); ou encore: JACQUIN Jean-Baptiste, *Ce que des juristes reprochent au projet de loi de sortie de l'état d'urgence*, Le Monde, 18 juillet 2017, En ligne: http://www.lemonde.fr/police-justice/article/2017/07/18/des-juristes-vent-debout-contre-le-projet-de-loi-de-sortie-de-l-etat-d-urgence_5161786_1653578.html (dernière consultation: 5 mars 2018). S'appuyant sur les mots de Michel Troper, Mireille Delmas-Marty conclut à la suspension de l'Etat de droit. Elle écrit ainsi que « *dans un article intitulé « l'état d'exception n'a rien d'exceptionnel », Michel Troper propose d'appeler état d'exception « une situation dans laquelle, en invoquant l'existence de circonstances exceptionnelles particulièrement dramatiques et la nécessité d'y faire face (...) on suspend alors provisoirement l'application des règles qui régissent ordinairement l'organisation et le fonctionnement des pouvoirs publics et l'on en applique d'autres, évidemment moins libérales, qui conduisent à une plus grande concentration du pouvoir et à des restrictions aux droits fondamentaux ».* Mais en incluant les actes terroristes dans la liste des circonstances exceptionnelles, Troper introduit nécessairement un doute sur le caractère provisoire de cette « suspension » car il est difficile, reconnaît-il d'imaginer « un moment où cesserait toute menace de terrorisme ». C'est pourquoi cet état d'exception « n'a rien d'exceptionnel », et c'est pourquoi, conclut-il, il tend à devenir permanent et à justifier de très graves atteintes aux droits de l'homme ». in. DELMAS-MARTY Mireille, *Libertés et sûreté dans un monde dangereux*, Op. Cit., 2010, p. 121 - 122.

violence interhumaine (terrorisme global) ou à la surpuissance de l'homme sur la nature (dangers écologiques ou biotechnologies) - les deux pouvant d'ailleurs se combiner (terrorisme biochimique ou nucléaire) - ces dangers conduisent à diverses formes de sécurité anticipée: tantôt c'est l'instant qui se prolonge quand l'urgence devient permanente, tantôt c'est le futur que l'on intègre au droit positif, par des techniques allant de la prévention à la précaution, des générations présentes aux générations futures⁴⁹⁹ ». Mutation de l'Etat de droit, société de suspicion, droit pénal de l'ennemi, anthropologie guerrière sont autant de conséquences fines de cette reconnaissance du droit à la sécurité.

176. Plus globalement, il est possible d'affirmer que l'Etat à travers ce « droit à » la sécurité a inscrit, dans son agenda politique, la sécurité comme nouvelle préoccupation économique, et a permis à la sécurité, puis à la surveillance de devenir une activité marchande, un bien de consommation nécessaire. Mis en parallèle avec la gouvernementalité par la peur et la banalisation de la surveillance, l'Etat au travers de ce « droit à », prépare ses citoyens à leur propre malléabilité.

B. De la privatisation de la sécurité à sa marchandisation au service de la surveillance diffuse

177. Entre la transformation du rôle de l'Etat et son objectif de sécurité imposé par le droit fondamental à la sécurité se situe un nouveau mode de production de la sécurité. Ces deux éléments sous-tendent en effet l'apogée de la sécurité entendue comme une activité marchande en co-production par l'Etat et les entreprises du secteur privé. Cet ensemble marchand, qui produit, distribue, contrôle et consomme de la sécurité permet à la surveillance de se diffuser largement dans la vie quotidienne des individus. Il faut au préalable voir en la sécurité un problème financier et politique pour l'Etat. Pour lutter contre ce problème et assurer le droit à la sécurité, l'Etat français a mis en place une véritable gestion managériale de la sécurité (1), qui ont conduit à la marchandisation de cette activité et, plus loin, de la surveillance (2).

1. Le choix de la gestion managériale de la sécurité par l'Etat comme prémices à sa marchandisation

⁴⁹⁹ Ibid. p. 188

178. Entre les années 2000 et 2010, deux études écrites par Alain Bauer sont consacrées à un état des lieux des effectifs policiers disponibles sur la voie publique afin d'en clarifier les affectations et les sujétions⁵⁰⁰. Bien que moquée par le Ministre de l'Intérieur en 1999⁵⁰¹, ces études tendent à démontrer le manque de productivité des effectifs de police; question, qui selon Alain Bauer, « *fait très souvent l'objet de débats, de polémiques et d'échanges tant au regard de la question des effectifs présents sur un territoire, et donc de leur répartition territoriale, que concernant la problématique de la répartition des fonctionnaires entre services ou directions*⁵⁰² ». A grands renforts de statistiques, de chiffres et de méthodes de calculs discutables, Alain Bauer s'efforce à prouver les bienfaits des transferts de certaines tâches auprès d'entreprises de sécurité privée⁵⁰³, ainsi que de démontrer les avantages du développement des nouvelles technologies au service de la sécurité publique⁵⁰⁴. Bien que l'on puisse être en désaccord profond avec ce criminologue, il n'en reste pas moins qu'un premier élément d'analyse de la marchandisation de la sécurité est contenu dans cette étude. La marchandisation de la sécurité est d'abord et avant tout construite autour d'une forme de privatisation de la sécurité. Cette privatisation de la sécurité se traduit par un double mouvement: d'une part, le développement de la présence des entreprises de sécurité privée dans l'espace public⁵⁰⁵; d'autre part, l'importation dans le secteur public de logiques de gestion

⁵⁰⁰ BAUER Alain, *Où sont les policiers?*, La gazette des communes, 8 février 1999, et, BAUER Alain, SOULLEZ Christophe, *Où sont les policiers et les gendarmes?*, La gazette des communes, 16 avril 2010, En ligne: http://www.lagazettedescommunes.com/telechargements/etude_policiers_gendarmes_bauer_04_2010.pdf (dernière consultation: 5 mars 2018). On soulignera que ces auteurs se présentent comme étant « criminologues ». L'expression de criminologie, ou encore la « profession » de criminologue n'en est pas une, puisqu'aucun diplôme universitaire d'Etat ne le garantit en France. Elle n'est donc en aucun cas une discipline universitaire, et pourrait être assimilé tout au plus à une sorte de lobby économique. Pour une étude intéressante à ce sujet, voir MUCCHIELLI Laurent, *Criminologie et lobby sécuritaire - Une controverse française*, Collection Mouvements de société, Editions La dispute, 23 janvier 2014

⁵⁰¹ Voir en ce sens, un article de l'express intitulé *Où sont les policiers?*, 21 février 2002, En ligne: http://www.lexpress.fr/informations/ou-sont-les-policiers_647422.html (dernière consultation: 5 mars 2018)

⁵⁰² BAUER Alain, SOULLEZ Christophe, *Où sont les policiers et les gendarmes?*, Op. Cit. p. 2

⁵⁰³ Ainsi dans l'étude précitée, le criminologue déclare que: « *en 10 ans, grâce aux réformes mises en place mais également au développement de la protection situationnelle ou du transfert de certaines gardes à des entreprises de sécurité privée, 303 équivalents temps plein ont pu ainsi être récupérés* ». (p. 17, de l'étude de 1010). Plus loin, on peut aussi lire que des missions de types charges d'escortes et de transfèrement des personnes détenues, ou de garde lors des audience des juridiction du siège d'instruction ne correspondent « *ni à la formation dispensée en école de police, ni aux missions de sécurité publique ou judiciaire. Cette mission pourrait être partagée entre la Police et la gendarmerie nationales et des unités de l'administration pénitentiaire dédiées, organisées en plateformes régionales ou d'agglomération, sans omettre la possibilité de confier certaines de ces missions à des entreprises de sécurité privée qui seraient spécialement habilitées* ». (p.29 de l'étude précitée).

⁵⁰⁴ Ainsi, « *La baisse importante des coûts de certaines technologies (caméras, par exemple), les progrès très rapides des produits technologiques, mais également la nécessité d'adapter les réponses policières aux nouvelles formes de délinquance, ont conduit peu à peu certains services de police à acquérir de nouveaux matériels. (...) L'usage des moyens technologiques peut permettre d'améliorer la performance policière tout en contribuant, parallèlement, à un meilleur usage des ressources humaines* » (p. 30) L'auteur appelle ainsi à la création d'une doctrine nationale ou une harmonisation des pratiques en la matière.

⁵⁰⁵ C'est le cas dans les années 80 pour des activités de gardiennage, de surveillance physique de bâtiments d'entreprises.

managériale en vigueur dans le secteur privé dans le but d'augmenter la productivité⁵⁰⁶ du secteur public. Et c'est dans le cadre de ce second élément que l'externalisation de la sécurité au profit du secteur privé, sa marchandisation est permise.

179. Entre 1986 et 1988, sous la Présidence de François Mitterrand, et dans le cadre du gouvernement Chirac, Edouard Balladur devient Ministre d'Etat, ministre de l'économie, des Finances et de la Privatisation. Cette dénomination témoigne d'une remise en cause de l'intervention de l'Etat dans certains secteurs de production comme le secteur bancaire et le secteur de l'énergie. Dans une période fortement marquée par la croissance de la dette publique, de méfiance vis-à-vis des fonctionnaires, et de double mouvement de décentralisation et de régionalisation (Union Européenne), l'action de l'Etat doit se moderniser, et l'Etat doit trouver sa place. Cette transition va s'opérer au moyen de l'application des principes de fonctionnement du nouveau management public. L'Etat, les institutions publiques deviennent des managers publics devant être au service de leurs citoyens, pouvant être contrôlés par ces derniers (le principe de transparence), et devant rendre compte (principe d'accountability)⁵⁰⁷. Ces principes se cristallisent autour de quatre formes d'actions: la poursuite de la décentralisation, l'amélioration de l'efficacité interne des services publics, la réduction de la taille de l'Etat, l'externalisation de la production dans un souci d'économie, d'efficacité et d'efficience. De 1996 à 2007, le concept de nouveau management public inspire les institutions européennes au travers de la notion de « services d'intérêt général ». Dès 1996, la Commission européenne rappelle le rôle des services publics dans la construction européenne dans le cadre d'une Communication parue en 1996, modifiée en 2000⁵⁰⁸. Ces derniers apparaissent pour la Commission comme « *des éléments clés du modèle européen de société* », et appartiennent « *à un ensemble de valeurs qui sont communes à tous nos Etats et font l'originalité de l'Europe* ». Avec la modification de l'article 16 du Traité d'Amsterdam sous

⁵⁰⁶ Le management public se traduit par une double approche: il faut rentabiliser les activités et les rendre plus efficiente (approche comptable), et il faut rendre performant le service public (approche gestionnaire)

⁵⁰⁷ De ces principes de fonctionnement découlent de nouvelles pratiques: le benchmarking, les guides de bonnes conduites, les best practices, ou encore le Knowledge management

⁵⁰⁸ Communication de la Commission, *Les services d'intérêt général en Europe*, Journal Officiel C281 du 26 septembre 1996 modifiée par la Communication de la Commission, les services d'intérêt général en Europe, Journal Officiel C17 du 19 janvier 2001.

impulsion de la France et de la Belgique⁵⁰⁹, la reconnaissance des services d'intérêt économique général est consacrée dans le cadre des textes constitutifs de l'Union européenne. Selon la Commission, les services d'intérêt général sont alors des services, tant économiques que non économiques, que les autorités publiques considèrent comme d'intérêt général et soumettent à des obligations spécifiques de service public⁵¹⁰. Dans les deux communications précitées, la Commission présente les principes qui fondent les services d'intérêt général: la neutralité⁵¹¹, la subsidiarité qui laisse aux Etats membres la capacité de définir leur propre champ d'action et les modes d'intervention possibles, la proportionnalité qui définit les modes de concurrence européens pour éviter des pratiques pouvant contribuer à développer une concurrence déloyale avec le secteur privé. L'inspiration européenne des services d'intérêts généraux s'articule autour de la territorialisation de l'action publique, la démocratie participative⁵¹², le partenariat public-privé.

180. A travers ces orientations, le secteur privé devient un partenaire au service de l'intérêt général. La transformation du rôle de l'Etat est ainsi consommée: le « mieux d'Etat » passe par des services publics, y compris régaliens, réalisés à la fois par des régies publiques mais aussi par des acteurs privés sous la supervision de responsables publics. Ces partenariats peuvent alors toucher à titre d'exemple les communications⁵¹³, les services postaux, l'électricité, le gaz, le transport, la santé, la sécurité, la gestion des déchets. Dans sa volonté de créer un concept communautaire des services d'intérêt général, la Commission prône l'instauration d'une base commune d'application: le

⁵⁰⁹ « Sans préjudice des articles 73, 86 et 87, et eu égard à la place qu'occupent les services d'intérêt économique général parmi les valeurs communes de l'Union ainsi qu'au rôle qu'ils jouent dans la promotion de la cohésion sociale et territoriale de l'Union, la Communauté et ses Etats membres, chacun dans les limites de leurs compétences respectives et dans les limites du champ d'application du présent traité, veillent à ce que ces services fonctionnent sur la base de principes et dans des conditions qui leur permettent d'accomplir leurs missions », Article 16 du Traité d'Amsterdam, JOCE C 340 du 10 novembre 1997

⁵¹⁰ Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions accompagnant la communication, *Un marché unique pour l'Europe du 21ème siècle - Les services d'intérêt général, y compris les services sociaux d'intérêt général: un nouvel engagement européen*, Com. (2007) 725 final, 20 novembre 2007, p. 4, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TEXT/PDF/?uri=CELEX:52007DC0725&from=FR> (dernière consultation: 5 mars 2018)

⁵¹¹ Ces services peuvent être dispensés par le secteur public, comme par le secteur privé.

⁵¹² Le citoyen, désormais usager, client, consommateur, contribuable et électeur devient un acteur territorial reconnu et obtient, en principe, une place privilégiée.

⁵¹³ On rappellera la privatisation de France Telecom en 2004.

service universel⁵¹⁴, la continuité du service⁵¹⁵, la qualité du service⁵¹⁶, l'accessibilité tarifaire⁵¹⁷ ainsi que la protection des utilisateurs et des consommateurs⁵¹⁸. Ces obligations communes peuvent être complétées par des obligations plus spécifiques en fonction du secteur concerné. En matière de sûreté et de sécurité, le livre vert de la Commission européenne de 2003 sur les services d'intérêt général⁵¹⁹ est très clair: « *les citoyens de l'Union européenne doivent se sentir et être en sécurité. (...). La sûreté et la sécurité constituent dès lors des principes essentiels du modèle de société européen. La sûreté et la sécurité se réfèrent à un ensemble commun d'objectifs existant dans presque tous les États membres. Il s'agit notamment de prévenir les actes nuisibles à la société et les attaques à son encontre. Ces objectifs peuvent revêtir différentes formes. En règle générale, ils ont été poursuivis en Europe au moyen des services d'intérêt général. Ils ont le plus souvent été réalisés sous l'égide de l'État et sans toujours viser des fins commerciales*⁵²⁰ ».

181. L'ensemble de ces éléments se traduit en France par l'adoption de ce nouveau management public par l'adoption de la loi organique relative aux lois de finances du 1er août 2001⁵²¹. Cette loi introduit la prise en compte des préoccupations européennes à travers une démarche de performance dans les services de l'Etat ainsi que d'une véritable idéologie du résultat. Encore une fois, l'objectif est ici de dépenser mieux, d'optimiser les finances publiques en fixant des objectifs, en prenant en compte les attentes des citoyens, des usagers et des contribuables.

⁵¹⁴ Ensemble d'exigences d'intérêt général dont l'objectif est de veiller à ce que certains services soient mis à la disposition de tous les consommateurs et utilisateurs sur la totalité d'un Etat membre, indépendamment de leur position géographique, au niveau de qualité spécifié et, compte tenu de circonstances nationales particulières, à un prix abordable (touchant notamment les industries de réseaux).

⁵¹⁵ Un certain nombre de services d'intérêt général se caractérisent par une exigence de continuité, ce qui signifie que le fournisseur de service est tenu de veiller à ce que celui-ci soit fourni sans interruption. Selon la Commission, « *il peut être dans l'intérêt commercial des fournisseurs de certains services de fournir un service ininterrompu, de sorte qu'il ne se révèle inutile d'imposer une obligation légale de continuité aux opérateurs* ». Commission des communautés européennes, *Livre vert sur les services d'intérêt général*, COM (2003) 270 final, 21 mai 2003, Bruxelles, p. 17, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52003DC0270&from=FR> (dernière consultation: 5 mars 2018)

⁵¹⁶ Dans le livre vert précité, la Commission déclare que « *la définition, le suivi et la mise en oeuvre des exigences de qualité par les autorités publiques sont devenus des éléments clés de la réglementation relative aux services d'intérêt général* ». Ibid. p. 18

⁵¹⁷ Un service d'intérêt économique général doit être offert à un prix abordable pour être accessible à tous, afin de contribuer à la cohésion économique et sociale dans les Etats membres.

⁵¹⁸ Les droits des consommateurs et des utilisateurs sont définis dans le cadre de législation sectorielle concernant notamment les communications électroniques, les services postaux, l'énergie, le transport et la radiodiffusion.

⁵¹⁹ Commission des communautés européennes, *Livre vert sur les services d'intérêt général*, Op. cit.

⁵²⁰ Ibid. p. 20

⁵²¹ Loi organique n°2001-692 du 1er août 2001 relative aux lois de finances, JORF n°177 du 2 août 2001, p. 12480, texte n°1, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000394028 (dernière consultation: 5 mars 2018)

2. La marchandisation de la sécurité et de la surveillance

182. En matière de sécurité - protection, la révision générale des politiques publiques de 2007, puis la modernisation de l'action publique de 2012, emportent réduction des effectifs de police et transformation du métier de la police par la rationalisation constante et la culture du chiffre⁵²². La sécurité-protection, se transforme dans une logique d'économie de services. Mais aussi dans une production d'économie qui vise la qualité, l'amélioration continue et la rentabilité. Ainsi, et pour pallier les réductions des effectifs humains, l'Etat systématise l'usage des technologies de l'information et de la communication fourni par le secteur privé⁵²³. Bien que l'on puisse poser la question de la (croyance en la) performance et en l'efficacité réelle ou supposée de ces outils pour accroître la qualité du service, l'Etat impose la technicisation de l'espace public à grands renforts de techniques de promotion et de marketing.

183. A ce titre, l'observation de la mise en place des dispositifs de vidéosurveillance est éclairante. La loi d'orientation et de programmation relative à la sécurité de 1995⁵²⁴, mentionne, au

⁵²² Dans une étude réalisée en 2012, Anne Wyvekens écrit : « *Les années 2000 sont marquées par la suppression de la police de proximité qu'avait tenté – avec difficulté – d'instaurer le gouvernement de gauche. Ce mode d'action policier est définitivement et publiquement disqualifié par Nicolas Sarkozy. Parallèlement, on assiste à une diminution des moyens de la police nationale : les effectifs décroissent, des commissariats ferment leurs portes. Le désengagement de l'État va de pair avec un renvoi – implicite – au local des missions policières de proximité. Ce renvoi prend la forme, essentiellement, de l'encouragement à créer des polices municipales. Le législateur tend à élargir leurs prérogatives, les faisant ainsi « ressembler » de plus en plus à la police nationale. Les maires se trouvent ainsi placés devant ce que le président du Forum français pour la sécurité urbaine appelle une décentralisation de fait des questions de sécurité. La police nationale se transforme, en outre, sous la pression des impératifs gestionnaires de la LOLF et de la RGPP, en machine à faire du chiffre. Si l'intention est légitime – mesurer l'efficacité de la police – les chiffres sont produits par des acteurs se trouvant à la fois juges et parties : évalués sur la base de ces statistiques, les policiers sont conduits, pour les améliorer (baisse du taux de délinquance, hausse du taux d'élucidation), à modifier leurs pratiques dans un sens qui les éloigne de la population – refus d'enregistrer les plaintes, focalisation sur les petits délits (éucidés) au détriment du travail d'enquête au long cours ».* In. WYVEKENS Anne, *La sécurité urbaine, affaire d'Etat ou problème local ?*, Métropolitiques, 2012, p. 2, <https://halshs.archives-ouvertes.fr/halshs-00673473/document> (dernière consultation: 5 mars 2018)

⁵²³ Notamment dans le domaine de la santé, de la sécurité, de l'e-administration. A titre d'exemple, en février 2010, en France, l'Agence des systèmes d'information partagés de santé (ASIP) a décidé d'attribuer le marché de l'hébergement du Dossier Médical Partagé (DMP) au consortium industriel mené par les groupes Atos Origin et La poste. Aujourd'hui, la liste des hébergeurs agréés de données de santé à caractère personnel est essentiellement constituée d'entreprises du secteur privé : Almerys, Bull, IBM France, Orange Business Services, SFR. La liste des hébergeurs agréés de données de santé à caractère personnel est disponible en ligne à l'adresse suivante: <http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees> (dernière consultation: 5 mars 2018). A l'international, et spécialement aux États-Unis, la clinique Mayo a, dans le cadre d'un partenariat avec la société Apple, adopté l'utilisation d'Iphone, d'Ipad et d'applications personnalisés pour « *transformer la portée des soins personnalisés* ». La publicité de cette « *innovation en matière de soins* » est d'ailleurs promue par la société Apple elle-même sur son site : <https://www.apple.com/hk/en/iphone/business/profiles/mayo-clinic/> (dernière consultation: 5 mars 2018).

⁵²⁴ Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, spécialement son article 10, JORF n°0020 du 24 janvier 1995, page 1249, Op. Cit.

titre des dispositions relatives à la prévention de l'insécurité, exclusivement la notion de vidéosurveillance, tout comme la LOPPSI en 2002⁵²⁵. En 2004, le Groupement des Industries Electroniques et numériques⁵²⁶, sorte de lobby économique français, fait paraître un livre bleu⁵²⁷. Ce dernier déclare que « *le marché national ne soutient pas suffisamment les développements possibles de ces technologies à cause des faibles budgets qui ont été jusqu'alors consacrés par les pouvoirs publics et par une législation contraignante. L'objectif est d'augmenter la sécurité tout en évitant de nuire à la liberté de chacun, l'informatique et la biométrie devraient y parvenir. Le politique doit assouplir la législation afin de favoriser le développement des technologies de la sécurité électronique et informatique*⁵²⁸ ». A partir de 2008, les budgets alloués en matière de technologies de l'information et de la communication augmentent, le terme vidéoprotection est avalisé dans sa dimension marketing par le gouvernement, et spécialement par Michèle Alliot-Marie, dans son « plan vidéoprotection », et par Brice Hortefeux, rédacteur de la préface du guide méthodologique sur la vidéoprotection⁵²⁹, fortement influencé par le Président Nicolas Sarkozy. Dès 2009, un rapport « *qui ne prouve rien*⁵³⁰ » s'interroge sur l'efficacité de la vidéoprotection⁵³¹ dans le cadre du « plan vidéoprotection ». Alors qu'en 2008, les promoteurs de la vidéosurveillance mettaient en avant le rôle des caméras dans la prévention du risque terroriste suite aux attentats de Londres, les débats parlementaires liés à l'examen de la LOPPSI 2⁵³² se focaliseront sur l'utilisation des caméras dans la lutte contre la délinquance. Le terme de vidéoprotection est consacrée définitivement à la section 4 de cette loi et devient un outil de lutte contre la délinquance et d'atténuation du sentiment

⁵²⁵ Loi n°2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, JORF du 30 août 2002, page 14398, texte n° 1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000780288&categorieLien=id> (dernière consultation: 5 mars 2018). On peut ainsi lire dans le cadre de la deuxième annexe à cette loi que le travail des enquêteurs sera facilité par « *des dotations de caméras vidéos (qui) seront prévues dans les zones sensibles* », ou encore que « *afin de réduire les charges dues aux gardes statiques, les dispositifs de vidéosurveillance des bâtiments seront accrus; le transfert de ces gardes au secteur privé et à des agents relevant d'autres statuts sera développé partout où cela sera possible* ».

⁵²⁶ Autrement appelé: le GIXEL

⁵²⁷ GIXEL, *Livre Bleu - Grands programmes structurants - Propositions des industries électroniques et numériques*, Juillet 2004, En ligne: http://bigbrotherawards.eu.org/IMG/pdf/Livre_bleu.pdf (dernière consultation: 5 mars 2018)

⁵²⁸ Ibid. p.35.

⁵²⁹ Op. Cit.

⁵³⁰ Nous reprenons les propos de Messieurs Tanguy Le Goff et Eric Heilmann. In. LE GOFF Tanguy et HEILMANN Eric, *Videosurveillance: un rapport qui ne prouve rien*, En ligne: <https://www.laurent-mucchielli.org/public/Videosurveillance.pdf> (dernière consultation: 5 mars 2018)

⁵³¹ SALLAZ Jean-Pierre, DEBROSSE Philippe, HAN Dominique, *Rapport sur l'efficacité de la vidéoprotection*, Ministère de l'intérieur, de l'Outre-Mer et des collectivités territoriales, Octobre 2009, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000540.pdf> (dernière consultation: 5 mars 2018)

⁵³² Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n° 0062 du 15 mars 2011, page 4582, texte n°2, Op. Cit.

d'insécurité dans l'espace public.

184. L'ensemble des pratiques décrites dans l'exemple précédent participe à la privatisation de la sécurité et de la surveillance, à sa marchandisation influencée par le nouveau management public et par le secteur privé. Deux éléments donneront également le ton de ces propos conclusifs. Dès 2011, le livre blanc sur la sécurité publique, rédigé par Michel Gaudin et Alain Bauer, déclarait: « *le développement de la vidéoprotection et son utilisation quotidienne comme moyen permettant d'élucider des enquêtes de toutes natures constituent une autre innovation qui comporte encore aujourd'hui un potentiel de progression important. En subventionnant⁵³³ le développement de l'implantation de caméras dans les communes, le renvoi des images vers les services de police et les unités de gendarmerie, et en facilitant les partenariats public-privé⁵³⁴, les politiques publiques impulsent depuis quelques années une dynamique qui est de nature à transformer les usages et les modalités de travail des forces de sécurité⁵³⁵ ».* Ces conclusions, vraies pour la vidéosurveillance, le sont tout autant pour la technicisation de l'espace public, et pour l'ensemble de ce que recouvre le concept de marchandisation de la sécurité. Le dernier exemple en date du 20 février 2017, et relatif à l'expérimentation des voitures-radar conduites, sous le contrôle de l'Etat, par des opérateurs privés⁵³⁶ ne fait que renforcer le propos tendant à la marchandisation de la sécurité et de la surveillance en co-production entre le secteur public et le secteur privé. L'ensemble de ces éléments tendent également à l'élaboration des fondations d'une culture de la surveillance que les individus semblent aujourd'hui avoir pleinement intégrés.

Section 2: L'intégration de la surveillance diffuse par les individus: la culture de la surveillance et son apogée

185. Evoquer le rôle des individus dans le cadre de la surveillance diffuse revient à évoquer leur adaptation aux nouvelles technologies de l'information et de la communication, puis à la

⁵³³ Notamment avec le Fonds interministériel de prévention de la délinquance

⁵³⁴ Par exemple la partenariat entre INEO/IRIS

⁵³⁵ GAUDIN Michel, BAUER Alain, *Livre blanc sur la sécurité publique*, Ministère de l'intérieur, de l'outre mer, des collectivités territoriales et de l'immigration, Collection des rapports officiels, La documentation française, novembre 2011, p. 173, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/114000645.pdf> (dernière consultation: 5 mars 2018)

⁵³⁶ Communiqué du Ministère de l'Intérieur, *Expérimentation des voitures-radar conduites sous le contrôle l'Etat, par des opérateurs privés*, 20 février 2017, En ligne: <http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Experimentation-des-voitures-radar-conduites-sous-le-contrôle-de-l-Etat-par-des-operateurs-privés> (dernière consultation: 5 mars 2018)

surveillance. Norbert Wiener décrivait la notion d'information comme « *un nom pour désigner le contenu de ce qui est échangé avec le monde extérieur à mesure que nous nous y adaptons et que nous lui appliquons les résultats de notre adaptation. Le processus consistant à recevoir et à utiliser l'information est le processus que nous suivons pour nous adapter aux contingences du milieu ambiant et vivre dans ce milieu. Les besoins et la complexité de la vie moderne rendent plus nécessaire que jamais ce processus d'information. (...). Vivre, c'est vivre avec une information adéquate. Ainsi, la communication et la régulation concernent l'essence de la vie intérieure de l'Homme, même si elles concernent sa vie en société*⁵³⁷ ». Ainsi que le précise Wiener, communication, régulation et information concernent « *l'essence de la vie intérieure de l'Homme* ».

186. Le processus évolutif lancé par la société de l'information a certes forcé l'Etat et les entreprises à s'adapter, à adapter leur offre; mais étant inscrit dans un projet de société, les individus, par ce darwinisme social, ont également dû s'adapter. Ainsi, les théoriciens de la société de l'information et de la communication ont souligné ce processus d'adaptation s'entendant à évoquer « *un homme nouveau*⁵³⁸ », « *un homme fasciné*⁵³⁹ », « *une Petite Poucette*⁵⁴⁰ ». D'autres évoqueront les « digital natives », la « e-generation », la « app-génération⁵⁴¹ ». Bien que ces expressions et ces adjectifs traduisent l'adaptation de l'homme au numérique, à la communication et aux technologies, ils ne suffisent pas à comprendre l'imprégnation de la surveillance diffuse dans nos sociétés, ni même de l'absence de contestations de la part des individus. Si la surveillance diffuse semble être culturellement intégrée, c'est bien parce qu'elle s'inscrit dans ce que Hannah Arendt qualifie de « *crise de la culture*⁵⁴² ». La surveillance diffuse est l'une des caractéristiques de la culture contemporaine dominée par la peur, la consommation, et l'aliénation par les technologies (paragraphe 1). Du fait de la diffusion et de la banalisation de la surveillance, le citoyen devient à la fois client et consommateur de sécurité, de protection, de technologies et de surveillance. Il est

⁵³⁷ Op. Cit.

⁵³⁸ C'est le cas de Philippe Breton qui dans le cadre de son ouvrage concernant l'utopie de la communication, évoque cette notion. in. BRETON Philippe, *L'utopie de la communication - le mythe du village planétaire*, Collection Essais, Editions La Découverte / Poche, 1997, p. 51 et suivants.

⁵³⁹ Jacques Ellul consacre la quatrième partie de son ouvrage concernant le bluff technologique à cet homme d'un nouveau genre, absorbé par la technique. in. ELLUL Jacques, *Le bluff technologique*, préface de Jean-Luc Porquet, *Ellul l'éclairé*; Hachette, 1988 ; réédition Hachette Littératures, collection « Pluriel », 2004, p. 580 à 712.

⁵⁴⁰ SERRES Michel, *Petite Poucette*, Le pommier, 2012

⁵⁴¹ GARDNER Howard, DAVIS Katie, *The App Generation - How today's Youth navigate identity, intimacy, and imagination in a digital world*, intervention du 21 octobre 2013 à la Harvard Graduate School of Education, Askwith Forum, Disponible en ligne à l'adresse suivante: <http://theappgenerationbook.com> (dernière consultation: 5 mars 2018)

⁵⁴² ARENDT Hannah, *La crise de la culture - Huit exercices de pensée politique*, Traduit de l'anglais sous la direction de Patrick Lévy, Collection Folio Essais, n°113, Editions Gallimard, 2016

toutefois partagé entre ces désirs de sécurité, de protection, mais également d'exhibitionnisme. Le mythe de Narcisse et la culture du narcissisme doivent, à ce titre, être aussi réactivés (paragraphe 2).

Paragraphe 1: De l'homo-numericus au philistin consommateur de sécurité

187. L'homo-numericus est d'abord un homme fasciné par les technologies de l'information et de la communication (A). Il a progressivement été préparé à la normalisation et à la banalisation des systèmes socio-techniques, des nouvelles technologies de l'information et de la communication. Placé dans une position de consommateur de technologies, il en devient progressivement aliéné par ces dernières. L'analyse de Hannah Arendt concernant la crise de la culture prend alors tout son sens (B).

A. L'homo-numericus ou la fascination pour les technologies de l'information et de la communication

188. Adaptable, l'homo-numericus est un acteur essentiel (1) dans l'apparition de la culture de la surveillance diffuse. Poussé par ce que les sociologues appellent « *la croyance en la toute puissance libératrice*⁵⁴³ » des technologies de l'information et de la communication (2), l'homo numericus a en effet permis à la surveillance de se diffuser pleinement dans sa vie quotidienne.

1. Un acteur essentiel et adaptable...

189. Très tôt, les relations qu'entretiennent, dans les sociétés industrielles, l'individu et la Technique ont été analysées. Georges Friedmann a élaboré, dès 1966, ses sept études sur l'homme et la technique⁵⁴⁴. Dans cette analyse, l'auteur distingue le « milieu naturel » et le « milieu technique », ce « nouveau milieu » que le progrès et la technique ont permis de développer. Selon lui, avec la fin du 18ème siècle, le « milieu naturel » subit de nombreuses mutations, qui engendreront le « milieu technique », et un développement qualitatif du milieu social de manière globale. Dans son étude, Friedmann décrit les conditions de production de ce nouveau milieu social et évoque le conditionnement spécifique de l'homme sur le plan de sa mentalité, ses modes de

⁵⁴³ En ce sens, voir BRETON Philippe, *L'utopie de la communication - le mythe du village planétaire*, Collection Essais, Editions La Découverte / Poche, 1997

⁵⁴⁴ FRIEDMANN Georges, *Sept études sur l'homme et la technique*, Collection Bibliothèque Médiations, Gallimard 1971, Première parution en 1966

pensée, sa perception. Cette dernière étant de plus en plus guidée par l'interprétation, l'intellectualisation, la rationalisation. L'individu passe alors, selon l'auteur, du vital au rationnel. Ces descriptions ne sont pas sans rappeler les mots de Max Weber lorsqu'il évoquait le sauvage et l'homme moderne. Weber écrivait ainsi que « *il ne s'agit plus pour nous, comme pour le sauvage qui croit à l'existence de ces puissances, de faire appel à des moyens magiques en vue de maîtriser les esprits ou de les implorer mais de recourir à la technique et à la prévision. Telle est la signification essentielle de l'intellectualisation*⁵⁴⁵ ». Friedmann ajoute néanmoins un élément fondamental de compréhension des relations qu'entretiennent l'homme et son nouveau milieu technicisé. L'individu s'adapte, certes, à son nouveau milieu par sa capacité à être malléable; mais il change également ses comportements dans ce nouveau milieu, et donc, opère une transformation de ce milieu. L'individu doit donc être considéré comme un acteur central des modifications issues du progrès, de la technique, de la société de l'information et de la connaissance, mais également, plus loin, de la diffusion de la surveillance.

190. On sait par exemple que la société de l'information et de la communication a dématérialisé⁵⁴⁶ les échanges, notre représentation du monde; qu'elle a numérisé⁵⁴⁷ la connaissance, la culture. En 1988, le président Reagan aux Etats-Unis déclarait déjà que « *l'invention humaine rend de plus en plus obsolètes les ressources matérielles*⁵⁴⁸ ». A travers ces lignes la faculté d'adaptation de l'individu à son monde, ainsi que sa faculté à façonner son nouveau monde sont compréhensibles. Omniprésence de l'informatique, dématérialisation et numérisation de l'information, de la communication et de la culture ont transformé l'individu et le citoyen comme un consommateur, un client dépendant des technologies de l'information et de la communication. Alors qu'il décrivait cette « *société computationnelle* » devenue « *automatique*⁵⁴⁹ », Bernard

⁵⁴⁵ Op. Cit.

⁵⁴⁶ Qui transforme le matériel en immatériel.

⁵⁴⁷ La numérisation est souvent assimilée à la dématérialisation dans notre histoire moderne. Toutefois, il est nécessaire par précision de langage de noter que la numérisation est l'acte de transformation en codification numérique binaire, ce qui produit une donnée informatique, résultant de la dématérialisation.

⁵⁴⁸ In. TURNER Fred, *Aux sources de l'utopie numérique - de la contre-culture à la cyberculture*, Stewart Brand, un homme d'influence, C&F éditions, décembre 2012, p. 277.

⁵⁴⁹ STIEGLER Bernard, *La société automatique - 1. L'avenir du travail*, Editions Fayard, 2015, p. 32

Stiegler esquisse une conclusion particulièrement éclairante quant au nouveau paradigme⁵⁵⁰ de la surveillance diffuse. Selon lui, tout se passe aujourd'hui « *comme si la data avait pris la place du Coca-cola dans l'Amérique d'Andy Warhol*⁵⁵¹ ». En 2009, Eric Sadin évoque quant à lui le nouveau paradigme de la surveillance diffuse qui permet de « *cerner l'humain par l'entrelacs du marketing et de la sécurité*⁵⁵² ». Selon lui, la situation actuelle peut se résumer en ces termes: « *une collecte ininterrompue d'informations en vue de définir des profils les plus individualisés, précis et « collés » à la multiplicité de nos actions quotidiennes (achats, déplacements, actes médicaux, communications...). Ces « portraits hautement détaillés » déterminent des usages divers selon des objectifs d'ordre prioritairement sécuritaire et marketing. L'enjeu ne consiste plus à circonscrire les individus distribués sur un territoire, à fixer les limites de leurs actions, et à en vérifier le respect (charge revenant historiquement aux préfets disposant des forces de police), mais à se tenir à distance des personnes en vue de recueillir des données à flux tendu, destinées à être analysées et traitées de façon à pénétrer les pratiques, et à dessiner les cartographies relationnelles. Constats qui pourront être utilisés en vue d'estimer le degré de « dangerosité » des personnes, ou dans le champ commercial, les pratiques de consommation dans l'objectif d'offrir les offres les plus adaptées à la singularité de chaque consommateur*⁵⁵³ ».

191. Permettant de mettre sur le même plan d'analyse la sécurité, la lutte contre le terrorisme et la délinquance, et le marketing, le marché du numérique, ce « recueil de données à flux tendus » décrit

⁵⁵⁰ Selon Thomas Kuhn, , un paradigme naît « *d'une découverte scientifique universellement reconnue qui, pour un temps, fournit à la communauté de chercheurs des problèmes type et des solutions* » (in. KUHN Thomas, *La structure des révolutions scientifiques*, Flammarion, Paris, 1970, p. 11). Et de préciser que « *l'utilité d'un paradigme est de renseigner les scientifiques sur les entités que la nature contient ou ne contient pas et sur la façon dont elles se comportent. Ces renseignements fournissent une carte dont les détails seront élucidés par les travaux scientifiques plus avancés. En apprenant un paradigme, l'homme de science acquiert à la fois une théorie, des méthodes et des critères de jugement, généralement en un mélange inextricable. (...). Il (le paradigme) détermine la légitimité des problèmes et aussi des solutions proposées* » (p. 155). On notera que selon l'auteur, l'étude du paradigme doit être conçu dans la dimension globale d'une révolution scientifique. Le paradigme, une fois établi, permet à, ce qu'il appelle « la science normale », d'opérer et de comprendre la situation en place. Dans cette conception, les paradigmes se succèdent par l'effet des révolutions. Les changements de paradigmes aboutissent selon lui « *à des révolutions dans la vision du monde* » (p. 157). Ces éléments d'analyse du terme paradigme semble donc bien correspondre à la situation contemporaine liée à la surveillance diffuse. Aidée par la révolution numérique, la surveillance est devenue diffuse et culturellement intégrée, et c'est ce changement de paradigme qu'il faut analyser dans ses différences, sa complexité et ses ressemblances avec le précédent. Pour une étude approfondie de l'étude de Thomas Kuhn, voir: JUIGNET Patrick, « Les paradigmes scientifiques selon Thomas Kuhn », *Philosophie, science et société [en ligne]*, 2015, <https://philosciences.com/Pss/philosophie-et-science/methode-scientifique-paradigme-scientifique/113-paradigme-scientifique-thomas-kuhn> (dernière consultation: 5 mars 2018)

⁵⁵¹ Op. Cit. p. 110.

⁵⁵² SADIN Eric, « Le nouveau paradigme de la surveillance. Cerner l'humain par l'entrelacs du marketing et de la sécurité », *Multitudes*, 2010/1 (n°40), p. 60 - 66, En ligne: <https://www.cairn.info/revue-multitudes-2010-1-page-60.htm> (dernière consultation: 5 mars 2018), Voir également: SADIN Eric, *Surveillance Globale - enquête sur les nouvelles formes de contrôle*, Flammarion, Climats, 2009

⁵⁵³ Ibid. p. 60

par Sadin tend à mettre en données le monde et les individus y consentants. Ainsi que le démontre Sadin en 2015 dans son ouvrage consacré à la vie algorithmique, après s'être attaqué à la numérisation des « *différents champs symboliques*⁵⁵⁴ » de notre vie tel que l'écrit, le son et l'image, un « *mouvement de numérisation post-symbolique*⁵⁵⁵ » est massivement à l'oeuvre depuis les années 2000. Ce nouveau mouvement tire sa puissance de capteurs présents dans la sphère publique et privé qui collectent et traitent des données variés⁵⁵⁶ « *à la source même de notre quotidien*⁵⁵⁷ ».

192. C'est donc bien la faculté d'adaptation des individus qui permet à la surveillance diffuse de saisir aujourd'hui en temps réel, de manière permanente et en tous lieux, à la fois l'ensemble de ce qu'intentionnellement ils lui permettent (son, écrit, vidéos, billet d'humeur, images), mais également de scruter l'ensemble de nos actions non intentionnelles (gestes, prédiction de comportements d'achats, prédiction du sommeil...). Tout, aujourd'hui peut devenir une donnée, une trace, qui peut être capté, qu'il s'agisse du simple fait de prendre l'ascenseur connecté, de se peser sur une balance connectée, de conduire, de réaliser un achat, ou encore de passer devant une caméra de vidéo-protection. Nos usages, nos comportements intentionnels et non intentionnels sont numérisés, captés, traités et utilisés afin de les analyser. Toutes les données de notre environnement (individuelles et collectives) devient source d'information pour la garantie d'une sécurité, ou d'un marché.

2. ... Poussé par la croyance en la toute puissance libératrice des technologies de l'information et de la communication

193. Entièrement tourné vers la communication, l'individu partage un peu plus son intimité, ses compétences, ses connaissances, son temps. Ce dernier utilise des pseudos, des représentations virtuelles, des avatars dans un but affiché d'interactivité, d'instantanéité, de communauté et de solidarité. Pour un bénéfice quelconque, il rend disponible pour les Etats, les entreprises et les autres individus, des traces, des informations, des données personnelles, sa vie privée, son identité.

⁵⁵⁴ SADIN Eric, *La vie algorithmique - Critique de la raison numérique*, Editions L'échappée, Collection Pour en finir avec, 2015. Voir spécialement l'ensemble du chapitre 1 consacré à la « *totalisation numérique* »

⁵⁵⁵ Ibid.

⁵⁵⁶ A travers son ouvrage, Sadin en donnent quelques exemples: météorologiques, de transports, de présence, d'activité dans les domiciles, les lieux professionnels ... et finis par les regrouper sous l'évocation suivante: « *ce sont des (...) phénomènes du réel (...) captés et transformés en données, saisis sous forme numérique à la source* ». Ibid.

⁵⁵⁷ Ibid.

En réalité, cet ensemble permet l'interconnexion des individus.

194. Cette mise en relation numérique et ces services collaboratifs transforment l'individu en ce que Philippe Breton nomme l'homo-communicans⁵⁵⁸, ou encore en ce que Nicholas Negroponte⁵⁵⁹ nomme l'homo-numericus, l'homme numérique. De manière plus globale, Breton affirme l'apparition d'une utopie de la communication par le développement de trois facteurs clés: « *une société idéale, une autre définition anthropologique de l'homme, la promotion de la communication comme valeur. Ces trois niveaux se concentrent autour du thème d'un homme nouveau que l'on appellera ici l'Homo-communicans. (...). L'Homo-communicans est un être sans intériorité et sans corps, qui vit dans une société sans secret, un être tout entier tourné vers le social, qui n'existe qu'à travers l'information et l'échange, dans une société rendue transparente grâce aux nouvelles « machines à communiquer »⁵⁶⁰ » ». Plus qu'un simple acteur individuel de la société de l'information et de la communication, l'individu devient un « *réacteur*⁵⁶¹ » qui prend place dans la société de l'information et de la communication où la « *transparence sociale*⁵⁶² » est de rigueur. L'analyse de Breton conclut à l'avènement par cette nouvelle utopie d'une « *illusion majeure, celle de la toute-puissance libératrice de la communication*⁵⁶³ » qui « *s'articule autour de deux croyances. D'une part, le seul fait de communiquer serait suffisant pour vivre harmonieusement en société. D'autre part, la communication pourrait s'instrumentaliser, c'est-à-dire être l'objet d'un savoir pratique aisément manipulable. « Parlez et tout ira mieux » est devenu un lieu commun moderne*⁵⁶⁴ ». Negroponte, quant à lui, présente les avantages de cette révolution technologique, dont l'homme numérique sera le premier bénéficiaire. Bien que son analyse souffre d'une prise de*

⁵⁵⁸ BRETON Philippe, *L'utopie de la communication - le mythe du village planétaire*, Collection Essais, Editions La Découverte / Poche, 1997, p17 mais surtout p. 50 et suivantes

⁵⁵⁹ Informaticien américain. Il a participé, en collaboration avec Jean-Jacques Servan-Schreiber, à la création en France du Centre mondial informatique et ressource humaine en 1980. Il crée aux Etats-Unis en 1982 le Media Lab, un laboratoire de recherche sur la communication et les nouveaux médias, au MIT. Ce laboratoire est selon lui le meilleur endroit pour faire « *de l'individu le pilote des nouvelles technologies* » (in. TURNER Fred, Op. Cit. p. 183). Il occupera une place importante dans la fondation du magazine Wired lancé par Stewart Brand, l'acteur principal de la cyber-culture aux Etats-Unis. Negroponte tient une chronique du numérique dans ce magazine. Les idées qu'il développe dans le cadre de ces chroniques seront affinées dans le cadre de l'ouvrage intitulé en anglais « *Being Digital* » paru en 1995. NEGROPONTE Nicholas, *L'homme numérique*, Robert Laffont, 1995.

⁵⁶⁰ BRETON Philippe, Op. Cit. p. 50

⁵⁶¹ Ibid. p. 60

⁵⁶² Ibid. p. 58

⁵⁶³ Ibid. p. 157

⁵⁶⁴ Ibid. p. 157 - 158

partie technophile⁵⁶⁵ quant aux implications de la révolution numérique, son concept d'homme numérique ou homo numericus marquera notamment les esprits politiques⁵⁶⁶ à l'international, en Europe mais également en France.

195. Les analyses de Negroponte, et plus particulièrement les analyses de Breton ont le mérite de renvoyer le lecteur attentif à son propre comportement d'individu, de citoyen, de client et de consommateur. Le projet de société lié à l'information et à la communication a pour objectif la modification du comportement des individus⁵⁶⁷. Ainsi que le rappelle Barbara Cassin⁵⁶⁸, en 2007, dans son ouvrage intitulé « *Google-moi, la deuxième mission de l'Amérique* », « *la notion contemporaine d'information a, qu'on l'oublie ou non, pour horizon explicite un comportementalisme étayé sur du feed-back*⁵⁶⁹ ». Mis en parallèle avec les mots de Breton

⁵⁶⁵ On notera l'intitulé de l'épilogue de son livre « *une ère d'optimisme* », ou encore d'un chapitre dédié aux « *légendes et les marottes du numérique* ». Negroponte est un informaticien, un technicien. Ainsi que le rappelle Jacques Ellul dans sa description de la fascination des individus à l'égard des technologies: « *Quand on proclame que l'homme peut et doit maîtriser et conduire à son gré la technique, j'avais posé la question bête, quel homme? L'Homme en soi? Il n'existe pas. Vous, moi, le citoyen quelconque? Je peux refuser le téléphone ou le magnétoscope, qu'est ce que ça changera? L'homme politique? Il n'y connaît rien et ne peut rien. Le cadre supérieur? Il n'a de pouvoir que sur son domaine, et non l'ensemble de la technique. Le technicien? Lui aussi est limité dans sa sphère, et il a bien trop intérêt à appliquer au mieux, en la perfectionnant, sa technique. Ici joue pleinement le jeu de la technostructure: l'application de la technique renforce le statut social (et pécuniaire) du technicien. Le renforcement l'induit à appliquer plus encore sa technique. Enfin le scientifique? Mais le plus souvent ce scientifique ne sait pas quelles peuvent être les conséquences techniques de sa « découverte » (voir l'affaire d'Einstein), et l'intérêt passionné pour la recherche scientifique l'empêche de s'autolimiter. Donc, personne* ». in. ELLUL Jacques, *Le bluff technologique*, Op. Cit., p. 581

⁵⁶⁶ Il est intéressant de trouver la mention de ce concept d'homo-numericus dans le cadre de rapport d'information français, notamment: DETRAIGNE Yves, ESCOFFIER Anne-Marie, *Rapport d'information n° 441 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, Sénat, Session ordinaire de 2008 - 2009, Annexe au procès verbal de la séance du 27 mai 2009, En ligne: <http://www.senat.fr/rap/r08-441/r08-4411.pdf> (dernière consultation: 5 mars 2018). Ce rapport consacre une section entière sur la possibilité de *faire du citoyen un « homo numericus » libre et éclairé, protecteur de ses propres données* (p. 67 à 79).

⁵⁶⁷ Le comportementalisme ou béhaviorisme est une branche de la psychologie qui étudie uniquement les aspects visibles et observables des comportements, et les analyse en relation avec des événements environnementaux immédiats. Evoquer le comportementalisme dans le cadre des relations qu'entretient l'individu avec la société de l'information et de la connaissance semble donc approprié puisqu'il est au coeur de cette doctrine psychologique qui s'efforce à analyser le comment des comportements humains. Les tenants de cette doctrine sont Pavlov; Watson et Skinner. Pour ce dernier par exemple, nous vivons dans une société punitive où l'homme est soumis à la punition afin qu'il apprenne à être meilleur et à se perfectionner. D'où des résultats décevants. Son ouvrage débute par ces mots: « *quand nous cherchons à résoudre les problèmes terrifiants auxquels nous sommes confrontés dans le monde d'aujourd'hui, nous nous tournons tout naturellement vers les choses que nous faisons le mieux. Nous jouons sur nos points forts, et nos points forts, ce sont la science et la technologie* ». in. SKINNER Burrhus, *Par delà la liberté et la dignité*, traduit de l'américain par Anne-Marie et Marc Richelle, Collection Libertés 2000, Editions Robert Laffont, 1971, p. 11. Ces mots ne sont pas sans rappeler l'idéologie du solutionnisme technologique précédemment développée.

⁵⁶⁸ Barbara Cassin, docteur ès-lettres en philosophie, directrice de recherches émérite au Centre National de la Recherche Scientifique à Paris. Sur les pratiques issues du nouveau management public sous Sarkozy, ainsi que sur la crise de la culture de nos sociétés modernes, voir un article paru dans le journal Le Monde le 28 février 2009, mis à jour le 2 mars 2009, intitulé « *Sarkozy « m'à tuer »* », qui comporte la chapeau introductif suivant: « *Les fautes d'orthographe qui parsèment le site de l'Élysée seraient anecdotiques si elles ne témoignaient d'une inquiétante désinvolture à l'égard de la culture* », En ligne: http://www.lemonde.fr/idees/article/2009/02/28/sarkozy-m-a-tuer-par-barbara-cassin_1161665_3232.html (dernière consultation: 5 mars 2018)

⁵⁶⁹ CASSIN Barbara, *Google-moi, La deuxième mission de l'Amérique*, Collection Banc Public, Editions Albin Michel, 2007, p. 113

concernant l'utopie de la communication, et sa « *toute puissance libératrice*⁵⁷⁰ », on comprend l'influence sur les choix et comportements de l'individu par ce nouveau milieu. En croyant en cette liberté individuelle et absolue promue par cette utopie⁵⁷¹, les citoyens se sont pleinement insérés dans le projet de société de l'information et de la communication, et ont, par la suite, transformé ce milieu allant vers toujours plus de techniques, de technologies, d'informations, de communications. Ils ont permis à la surveillance de se diffuser pleinement. Notons en guise de propos conclusifs les mots de Skinner, « *notre culture a produit la science et la technologie dont elle a besoin pour se sauver elle-même. Elle dispose des richesses nécessaires à une action efficace. Elle a, à un haut degré, le souci de son propre avenir. Mais elle s'obstine à considérer la liberté ou la dignité plutôt que sa propre survie. Rien n'exclut dès lors qu'une autre culture fasse une contribution plus importante au futur. Le défenseur de la liberté et de la dignité peut alors, comme le Satan de Milton, continuer à se réciter qu'il possède « un esprit que rien ne peut changer ni dans le temps ni dans l'espace » et une identité personnelle satisfaite d'elle-même (« qu'importe où je suis, si je reste le même? »); mais il se retrouvera néanmoins en enfer sans autre consolation que l'illusion qu'ici au moins nous serons libres*⁵⁷² ».

196. Pour paraphraser les mots de Skinner, notons qu'aujourd'hui nombreux sont ceux qui, sous couvert d'un accès facilité à (l'arbre de) la connaissance, d'une liberté de « *penser différemment*⁵⁷³ », auront « croqué » la marque à la pomme. Cette consommation irréfléchie des individus s'est faite sans se soucier réellement des conséquences potentiellement néfastes pour

⁵⁷⁰ Op. Cit.

⁵⁷¹ Voir également en ce sens l'ouvrage de Skinner précédemment cité. A travers une liste d'exemples d'usages scientifiques et technologiques envisagés comme des solutions aux maux de la société, l'auteur répertorie en contre-champs une liste de leurs effets néfastes. Il conclut son analyse en citant Darlington: « *Toute source nouvelle de laquelle l'homme a tiré un accroissement de son pouvoir sur la terre a été utilisée de manière à rétrécir les perspectives de ses descendants. L'homme a payé chacun de ses progrès d'une atteinte à son environnement, qu'il ne pouvait prévoir et qu'il n'est pas capable de réparer* ». Skinner démontre, dans les paragraphes suivants, que l'application du progrès technique, scientifique, technologique et médical, ne suffit pas à résoudre tous ces problèmes. Il développe l'idée que nous devrions nous employer à mieux comprendre les comportements humains. Pour ce faire, nous aurions tout intérêt à mieux utiliser les connaissances de la psychologie scientifique pour réduire notamment les comportements d'agression, d'exploitation, de surconsommation, de pollution, et pour développer des comportements altruistes, des loisirs de qualité, la recherche scientifique. Skinner conclut à travers les pages suivantes qu'il est étonnant d'affirmer que la dignité de l'homme réside essentiellement dans la liberté souveraine de chaque individu de satisfaire sans réserve tous ses désirs égoïstes. Par ailleurs, en faisant croire aux citoyens qu'ils sont des êtres parfaitement libres, on leur fait endosser la responsabilité de tous leurs malheurs, on discolpe l'organisation sociale et les politiciens au pouvoir. Voir spécialement p 11 à 76.

⁵⁷² SKINNER Burrhus, *Par delà la liberté et la dignité*, traduit de l'américain par Anne-Marie et Marc Richelle, Collection Libertés 2000, Editions Robert Laffont, 1971, Quatrième de couverture.

⁵⁷³ Slogan publicitaire d'Apple pour son nouvel ordinateur portable. On pourrait également citer Google et sa promotion de Chrome : « *à vous de créer le web* », SFR et sa solution domotique « *ce qui est smart (intelligent) c'est d'être chez soi même quand on y est pas, pilotez votre maison à distance* », Facebook et sa promotion de ce réseau social « *Facebook, c'est un peu comme une chaise où l'on va s'asseoir pour échanger ensemble* ».

l'individu. L'une d'entre elles étant sa préparation à la normalisation et à la banalisation d'un ensemble de systèmes socio-techniques intégré dans sa vie quotidienne. La nouvelle culture qui se développe est ainsi celle d'une surveillance diffuse, qui donne l'illusion aux individus d'être libres et dignes car en sécurité permanente.

B. La banalisation des technologies de l'information et de la communication dans une société de masse : la philistin et la crise de la culture technicisée

197. La banalisation des technologies de l'information et de la communication dans la société contemporaine doit être analysée comme une consommation technologique dans une société de masse. Les individus totalement conditionnés (2) à la consommation technologique permet à la surveillance diffuse de se développer, et de s'inscrire durablement dans la culture contemporaine « en crise » (1).

1. La surveillance diffuse et la culture contemporaine « en crise »

198. La banalisation des outils technologiques, et de la surveillance diffuse, ne font que rendre l'individu un peu plus docile, dans un monde, une société de masse, où les technologies sont devenues acceptables, et ceci peu important leurs conséquences potentiellement néfastes. En ce sens, l'analyse de la crise de la culture décrite par Hannah Arendt permet de comprendre l'individu comme un consommateur, et la culture comme un bien de consommation assimilable aux loisirs dans une société de masse.

199. Hannah Arendt entame son analyse concernant la crise de la culture par ces mots: « *depuis plus de dix ans, nous constatons une inquiétude sans cesse croissante parmi les intellectuels quant au phénomène relativement nouveau de la culture de masse. Le terme lui-même provient visiblement du terme guère plus ancien de « société de masse »; l'hypothèse tacite, sous-jacente à toutes les discussions sur ce sujet, est que la culture de masse, logiquement et inévitablement, est la culture de la société de masse*⁵⁷⁴ ». Partant de ce constat, Arendt s'interroge sur la relation entre société de masse et culture de masse, en opérant une comparaison avec la société et la culture qui l'a précédée. Selon l'auteur, les deux concepts de société de masse et de culture de masse doivent être corrélés

⁵⁷⁴ ARENDT Hannah, *La crise de la culture - Huit exercices de pensée politique*, Traduit de l'anglais sous la direction de Patrick Lévy, Collection Folio Essais, n°113, 2016, Editions Gallimard, p. 253

dans le sens où leur « *commun dénominateur n'est pas tant la masse, que la société dans laquelle les masses aussi ont été incorporées*⁵⁷⁵ ». Et de préciser que si la société devient une société de masse, c'est parce qu'elle « *indique un nouvel état de choses, où la masse de la population a été soulagée du fardeau du labeur physiquement épuisant, et peut, elle aussi, disposer d'assez de loisir pour la « culture »*⁵⁷⁶ ». Cette transformation dans l'accès aux loisirs et à la « culture » engendre alors l'évolution de la société en société de masse, accompagnée du développement d'une « culture de masse ».

200. Ces transformations sociétales ont des conséquences palpables pour l'individu. En citant Brentano, l'auteur explique ce qu'il faut entendre par « philistin ». Elle déclare ainsi, que ce concept désigne « *un état d'esprit qui juge de tout en termes d'utilité immédiate et de « valeurs matérielles », et n'a donc d'yeux pour des objets et des occupations aussi inutiles que ceux relevant de la nature et de l'art*⁵⁷⁷ ». Et d'ajouter plus loin, « *la difficulté avec la société des périodes modernes est que ses membres, même après s'être délivrés des nécessités de la vie, ne pouvaient se libérer des préoccupations en rapport étroit avec eux-mêmes, leur rang et leur situation dans la société, la réflexion sur leur moi individuel; ils n'entretenaient aucune relation d'aucune sorte avec le monde d'objets et d'objectivité où ils se mouvaient. La difficulté relativement nouvelle avec la société de masse est peut être encore plus sérieuse, non en raison des masses elles-mêmes, mais parce que cette société est essentiellement une société de consommateurs, où le temps du loisir ne sert plus à se perfectionner ou à acquérir une meilleure position sociale, mais à consommer de plus en plus, à se divertir de plus en plus*⁵⁷⁸ ». L'ensemble de cette analyse a une résonance particulièrement familière encore aujourd'hui.

201. Le citoyen, l'individu vivant dans une société de masse globalisée, et libéré des incidences des classes sociales opérantes il y a encore une cinquantaine d'années, est attiré par le loisir. Il voit en toutes choses un bien de consommation permettant d'accéder à un loisir de masse, à travers la culture. Il ne cherche pas à s'élever de son rang social, mais simplement à se divertir. L'avènement des technologies de l'information et de la communication, et les promesses liées à la « toute

⁵⁷⁵ Ibid. p. 255

⁵⁷⁶ Ibid.

⁵⁷⁷ Ibid. p. 258

⁵⁷⁸ Ibid. p. 270.

*puissance libératrice*⁵⁷⁹ » de ce projet de société ont rendu l'individu consommateur de toujours plus de technologies pour parvenir au but d'un divertissement total. Ainsi, ce dernier consomme la technologie de l'information et de la communication, sous couvert d'un accès à la connaissance, à la culture, à l'information, non plus pour s'enrichir personnellement, mais bien pour satisfaire un besoin, combler un ennui, ou pour citer à nouveau Arendt pour « *consommer de plus en plus, se divertir de plus en plus*⁵⁸⁰ ».

2. Le conditionnement des masses à la consommation technologique

202. Afin de parvenir à ce but de divertissement total, l'individu est aidé massivement par ce que Hannah Arendt appelle « *l'industrie des loisirs confrontée à des appétits gargantuesques*⁵⁸¹ », qui, « *puisque la consommation fait disparaître ses marchandises, (...) doit sans cesse fournir de nouveaux articles*⁵⁸² ». Nicolas Curien et Pierre-Alain Muet, citant Paul Baran, l'un des fondateurs d'Internet, rappellent l'une des caractéristiques principale de la société de l'information déjà envisagée par Ellul: son auto-accroissement. Ils en précisent néanmoins les contours et écrivent qu'en 1990, Paul Baran énonçait que « *le processus du développement technologique est comparable à la construction d'une cathédrale, chaque nouvel arrivant laisse un bloc au sommet des fondations antérieures, de sorte que chacun peut dire qu'il a construit la cathédrale*⁵⁸³ ». Cette citation démontre la conception d'un « *système technicien*⁵⁸⁴ », d'un ensemble où chacun des acteurs, y compris les individus, souhaitent apporter sa pierre à l'édifice, porté par une croyance quasi-religieuse de la « *toute puissance libératrice*⁵⁸⁵ » des technologies, du progrès, de la surveillance diffuse.

203. Ainsi que le rappelle Hannah Arendt, « *comme il n'y a pas assez de biens de consommation alentour pour satisfaire les appétits croissants d'un processus vital dont la vivante énergie, qui ne*

⁵⁷⁹ BRETON, Op. Cit.

⁵⁸⁰ Op. Cit.

⁵⁸¹ ARENDT Hannah, *La crise de la culture - Huit exercices de pensée politique*, Traduit de l'anglais sous la direction de Patrick Lévy, Collection Folio Essais, n°113, 2016, Editions Gallimard, p. 265

⁵⁸² Ibid.

⁵⁸³ CURIEN Nicolas, MUET Pierre-Alain, *Rapport sur la société de l'information*, Conseil d'Analyse économique, La Documentation française, Paris, 2004, p. 19, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/044000180.pdf> (dernière consultation: 5 mars 2018)

⁵⁸⁴ Au sens développé par Jacques Ellul. Voir: ELLUL Jacques, *Le Système Technicien*, Op. Cit.

⁵⁸⁵ BRETON, Op. Cit.

se dépense plus dans le labeur et la peine d'un corps au travail, doit s'user dans la consommation, tout se passe comme si la vie elle-même sortait de ses limites pour se servir de choses qui n'ont jamais été faites pour cela. Le résultat est non pas, bien sûr, une culture de masse qui, à proprement parler, n'existe pas, mais un loisir de masse, qui se nourrit des objets culturels du monde⁵⁸⁶ ». Dès 2011, le sociologue Wolfgang Sofsky décrit la situation contemporaine en ces termes: « la plupart de nos contemporains n'ont même pas conscience d'être soumis à cette surveillance sans faille. La technique et le fonctionnement de l'espionnage quotidien passent le plus souvent inaperçu. Il y a très longtemps que les gens se sont habitués aux caméras, aux cartes de fidélité et aux courriels publicitaires. Certaines choses paraissent pesantes, d'autres inévitables, beaucoup sont invisibles et inconnues. Les caméras promettent la sécurité, la saisie des données personnelles apporte un certain confort. Hormis quelques moments de mauvaise humeur, le citoyen de verre apprécie les facilités que lui apporte l'ère digitale⁵⁸⁷ ». Le citoyen de verre décrit par Sofsky représente ce que nous sommes devenus, par la consommation à outrance de nouvelles technologies. Englué dans les bénéfices hypothétiques des systèmes socio-technique, l'individu n'a jamais questionné l'acceptabilité de ces mesures, ni même leur légitimité. Il a simplement utilisé ces outils, puisqu'étant mis à sa disposition, il ne pouvait que les consommer, incité par le secteur public et le secteur privé. Pire encore, il ne questionne pas les potentialités néfastes de ces dernières « hormis quelques moments de mauvaise humeur⁵⁸⁸ », et ne voit en elles, encore et toujours, seule leur « toute puissance libératrice⁵⁸⁹ ».

204. La prise en charge des individus par la surveillance diffuse provoquent à la fois un effet d'aubaine au profit des gouvernements, et représentent une véritable manne économique pour le secteur privé. L'Etat devient un acteur principal de la surveillance, tantôt prestataire de ce service, tantôt régulateur de ce dernier par la main mise qu'il détient sur ce secteur assurant la sécurité et propageant la gouvernementalité par la peur. Elle est ensuite une véritable manne économique pour

⁵⁸⁶ ARENDT Hannah, *La crise de la culture - Huit exercices de pensée politique*, Traduit de l'anglais sous la direction de Patrick Lévy, Collection Folio Essais, n°113, 2016, Editions Gallimard, p. 270

⁵⁸⁷ SOFSKY Wolfgang, *Le citoyen de verre - entre surveillance et exhibition*, Traduit de l'allemand et préfacé par Olivier Mannoni, Editions de l'Herne, Paris, 2011, p. 18 - 19

⁵⁸⁸ Ibid. A titre d'illustration de ces moments de mauvaise humeur, on citera le dernier exemple français en date: le fichier TES, et plus particulièrement l'ensemble des polémiques liées au Décret n°2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, JORF n° 0254 du 30 octobre 2016, texte n° 18, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000033318345 (dernière consultation: 5 mars 2018), voir également l'*avis rendu par le Conseil National du numérique sur le fichier TES*, décembre 2016, En ligne: https://cnnumerique.fr/files/2017-10/Avis-tes_CNNuWeb_0.pdf (dernière consultation: 5 mars 2018)

⁵⁸⁹ BRETON, Op. Cit.

le secteur privé, au fait de l'importance de la réalité économique du marché de la surveillance, de la sécurité et des données personnelles. Derrière la gratuité de certains services numériques (moteur de recherches, réseaux sociaux...), ou des services rattachés au numérique (carte de fidélité, profiling commercial), le secteur privé a profité de la crédulité des individus pour les tracer en toute impunité⁵⁹⁰. Au delà du conditionnement⁵⁹¹ mené par l'Etat et les entreprises⁵⁹², l'individu lui-même a participé à la diffusion de la surveillance. Comme le souligne Jean-Gabriel Ganascia, progressivement la connaissance ne « *procure donc plus de supplément de pouvoir particulier. En revanche, perdu dans l'immensité du dispositif, l'individu risque d'être ignoré en tout ce qu'il fait. Plus que tout, il lui faut donc apparaître, être connu et reconnu. Le lien entre pouvoir et regard se renverse alors: on passe d'une logique de surveillance à une logique de sousveillance. Dans un cas, celui qui regarde domine, parce qu'il possède des informations grâce auxquelles il peut agir plus efficacement; dans l'autre, celui qui est regardé prend l'ascendant du fait même qu'il est vu. La première éventualité renvoie à une économie de la connaissance où la possession du savoir donne accès à la maîtrise du monde et donc à l'argent; la seconde est une économie de l'attention où ce qui rapporte tient non pas à la production de biens ou à l'utilité de l'activité, mais aux regards attirés, qui se monnayent directement* »⁵⁹³.

⁵⁹⁰ Pour attester de ce propos, il est utile de citer Alex Türk qui écrivait en 2001 qu'il faut bien reconnaître que « *les groupes qui développent ces systèmes ont réussi l'un des coups les plus géniaux qui aient jamais été réalisés dans la société capitaliste. D'envergure planétaire, ces sociétés, qui réalisent des chiffres d'affaires se comptant en milliards d'euros, sont parvenues à substituer au concept marchand classique entre un fournisseur et son client, une relation fondée - semble-t-il - sur le partage, l'enrichissement mutuel, la gratuité et même l'amitié! L'agrégation de profits sur fond d'exaltation libertaire. (...) Concilier l'efficacité économique et l'humanisme* ». TURK Alex, *La vie privée en péril. Des citoyens sous contrôle*, Paris, Odile Jacob, 2011, p. 114 - 115.

⁵⁹¹ Nous empruntons ce terme à Ignacio Ramonet. Ce dernier envisage dès 1994 « *les nouvelles armes du contrôle social* ». Il écrit alors: « *la crise des grandes machines à conditionner - famille, école, Eglise, armée - et l'échec des Etats totalitaires pratiquant à grande échelle l'endoctrinement de masse ont pu laisser croire que le citoyen retrouvait une autonomie sans entraves. C'est une illusion. Sous un apparent apaisement, tout indique, au contraire, le renforcement du contrôle social, cet « ensemble des ressources matérielles et symboliques dont dispose une société pour s'assurer de la conformité du comportement de ses membres à un ensemble de règles et de principes prescrits et sanctionnés* ». En effet, de nouvelles méthodes de conditionnement plus subtiles, plus insidieuses et plus efficaces se mettent en place alors que surgissent des techniques dernier cri, à base d'électronique et d'informatique, pour suivre à la trace le parcours des citoyens, relever les déviations et châtier les écarts. Nul n'est à l'abri. ». RAMONET Ignacio, *Les nouvelles armes du contrôle social - Citoyens sous surveillance*, Le Monde Diplomatique, Mai 1994, pages 15 et 20, En ligne: <http://www.monde-diplomatique.fr/1994/05/RAMONET/46012> (dernière consultation: 5 mars 2018)

⁵⁹² Entre la gouvernementalité par la peur des Etats et le storytelling des entreprises, la production des discours se multiplient. Les discours publicitaires des entreprises et les discours politiques tendent de plus en plus à se confondre. Sur ce point, voir: SOUCHIER Emmanuel, JEANNERET Yves, *Publicité et mensonges*, in. Le Monde Diplomatique, *Médias et contrôle des esprits*, Manière de voir, n° 27, Août - Septembre - Octobre 1995, En ligne: <http://www.monde-diplomatique.fr/mav/27/> (dernière consultation: 5 mars 2018)

⁵⁹³ GANASCIA Jean-Gabriel, *Voir et pouvoir: qui nous surveille ?*, Editions Le pommier, Collection Les essais, 2009, p. 201

Paragraphe 2: Le mythe de Narcisse au service de la culture de la surveillance diffuse

205. Dans la description de cet imbroglio des intérêts étatiques, institutionnels, politiques et ceux des leaders économiques du numérique, l'individu doit trouver sa place, tantôt dans son rôle de consommateur, que dans celui de citoyen. Afin de questionner le rôle de l'individu dans ces différentes fonctions, deux éléments importants devront être mis en avant: d'une part, la montée en puissance d'une « économie de l'attention⁵⁹⁴ » (B) qui conduit l'individu à toujours plus de consommation technologique; d'autre part, le rôle du citoyen numérique. L'activation du mythe de Narcisse permettra de comprendre l'individu, dans cette nouvelle économie, comme une cible en quête d'attention (A).

A. L'individu narcissique: un individu dépersonnifié par les objectifs marchands...

206. L'individu narcissique, est d'abord et avant tout une cible économique dans un marché en perpétuelle évolution (1). La culture de la surveillance qui engendre peur et besoin de sécurité fait de l'individu contemporain un nouveau Narcisse en quête d'attention et de réassurance (2).

1. L'individu narcissique: une cible dans un marché économique...

207. La parution en 2015 du rapport de l'Union Internationale des Télécommunications⁵⁹⁵ tend à enserrer l'individu dans un rôle d'acteur passif dans le marché économique: une cible du marché. Intitulé « mesurer la société de l'information », ce rapport exhorte les pays membres à tenir compte « *de l'immense potentiel que renferment les technologies de l'information et de la communication et invite les pays à accroître sensiblement l'accès⁵⁹⁶* » à ces dernières. Et d'ajouter que ces mesures contribueront « *de manière significative à la mise en oeuvre de tous les objectifs de développement durable⁵⁹⁷* ».

208. Le rapport de l'Union Internationale des Télécommunications s'inscrit dans le cadre du

⁵⁹⁴ Nous empruntons ce concept à Jean-Gabriel Ganascia.

⁵⁹⁵ Union Internationale des Télécommunications, *Rapport mesurer la société de l'information 2015 - Résumé analytique*, 2015, UIT, Genève, Suisse, En ligne: <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-F.pdf> (dernière consultation: 5 mars 2018)

⁵⁹⁶ Ibid. p. iii

⁵⁹⁷ Ibid.

programme de développement durable des Nations Unies à l'horizon 2030. Adopté le 25 septembre 2015, ce programme vise à « *transformer notre monde*⁵⁹⁸ » et fait la part belle aux technologies de l'information et de la communication. On peut ainsi lire que nous vivons un « *moment où les possibilités sont immenses. Des progrès considérables ont été accomplis et de nombreux problèmes de développement sont en passe d'être surmontés. En l'espace d'une génération, des centaines de millions de gens sont sortis de l'extrême pauvreté. L'accès à l'éducation a été nettement amélioré, pour les garçons comme pour les filles. L'expansion de l'informatique et des communications et l'interdépendance mondiale des activités ont le potentiel d'accélérer les progrès de l'humanité, de réduire la fracture numérique et de donner naissance à des sociétés du savoir, sans parler de l'innovation scientifique et technologique dans des domaines aussi différents que la médecine et l'énergie*⁵⁹⁹ ». Afin de remplir cet objectif, l'Union Internationale des Télécommunications va même plus loin en créant un indice de développement des technologies de l'information et de la communication, et ce, dans le but de mesurer les progrès des pays membres en termes d'accès à ces technologies.

209. Au-delà de cet indice de développement, deux points sont à soulever dans ce rapport. L'un est prospectif; et démontre que cet indice de développement doit être amélioré afin de permettre à l'internet des objets, considéré comme un nouvel eldorado libertaire et économique, de connaître sa pleine progression. Le Directeur du Bureau de développement des télécommunications de l'Union Internationale des télécommunications, Brahim Sanou, insiste sur l'accélération de la progression de l'internet des objets permise par le développement rapide des infrastructures et des dispositifs des technologies de l'information et de la communication. Il démontre également les bénéfices offerts par cette nouvelle possibilité technique en écrivant que « *l'Internet des objets devrait avoir une incidence significative sur presque tous les secteurs d'activité socio-économiques, notamment l'éducation, la santé, l'agriculture, les transports et l'industrie manufacturière. L'essentiel de la valeur produite par l'Internet des objets procède de la génération, du traitement et de l'analyse de nouvelles données. Le présent rapport montre comment l'Internet des objets et l'analyse des mégadonnées peuvent aider à relever certains défis majeurs du développement, comme ceux que posent les mégapoles, le changement climatique, la sécurité alimentaire et la gestion des*

⁵⁹⁸ ONU, Résolution adoptée par l'Assemblée générale le 25 septembre 2015, 70/1. Transformer notre monde, le Programme de développement durable à l'horizon 2030, A/ RES/ 70/ 1, Soixante-dixième session, Points 15 et 116 de l'ordre du jour, Distribution générale le 21 octobre 2015, En ligne: <http://www.ipu.org/splz-f/unga16/2030-f.pdf> (dernière consultation: 5 mars 2018)

⁵⁹⁹ Ibid. p. 5-6

*ressources*⁶⁰⁰ ». Le second point questionne l'individu et sa place concernant la société de l'information et de la communication, voire ce « *système technicien* ». En effet, le rapport indique, dès sa première partie, « *le suivi des objectifs et des cibles à l'échelle mondiale en matière de technologies de l'information et de la communication*⁶⁰¹ ». Les buts répertoriés dans ce rapport correspondent à ce que la Conférence de plénipotentiaires de l'UIT avait adopté en 2014 dans le cadre du Programme Connect 2020⁶⁰².

210. La croissance⁶⁰³, l'inclusion⁶⁰⁴, la durabilité⁶⁰⁵, l'innovation et les partenariats⁶⁰⁶ sont les quatre grands buts stratégiques que l'UIT s'était fixé en 2014 afin de « *stimuler la croissance et l'utilisation des technologies de l'information et de la communication, et à encourager le développement socio-économique à moyen et à long terme* ⁶⁰⁷». A chacun de ces buts correspondent des cibles. En ce qui concerne l'inclusion et la croissance, l'UIT transforme les « *ménages, la population des pays moins avancés, des pays en développement, rurale, urbaine, à l'échelle mondiale, les hommes, les femmes, les personnes handicapées, les internautes*⁶⁰⁸ » en « cibles » c'est-à-dire en individu dépersonnifié, en objectif à atteindre en tant que futur consommateur dans un marché économique sans cesse renouvelé.

2. ... en quête d'attention

211. L'image du philistin cultivé numérisé évolue vers celle d'un Narcisse 2.0: un philistin cultivé numérisé narcissique. Dans cette nouvelle description de l'individu, il ne s'agit plus, pour

⁶⁰⁰ Union Internationale des Télécommunications, *Rapport mesurer la société de l'information 2015 - Op. Cit.*, p. iv.

⁶⁰¹ Ibid. p. 1.

⁶⁰² Voir: UIT, *Document d'information sur l'UIT - Connect 2020: définir un programme d'action mondial pour le secteur des TIC*, Conférence de plénipotentiaires de l'UIT, 2014, Busan, Corée, En ligne: <https://www.itu.int/en/plenipotentiary/2014/newsroom/Documents/backgrounders/pp14-backgrounder-connect-2020-fr.pdf> (dernière consultation: 5 mars 2018)

⁶⁰³ Pour l'UIT, la croissance correspond au fait de « *permettre et d'encourager l'accès aux technologies de l'information et de la communication et leur utilisation accrue* ». Ibid.

⁶⁰⁴ Selon l'UIT, l'inclusion correspond au fait de « *réduire la fracture numérique et de mettre le large bande à la portée de tous* ». Ibid

⁶⁰⁵ Qui correspond, pour l'UIT, au fait de « *gérer les problèmes résultant du développement des technologies de l'information et de la communication* ».Ibid.

⁶⁰⁶ L'UIT précise qu'il s'agira de « *jouer un rôle de premier plan dans l'évolution de l'environnement technologique, de mieux contribuer à cette évolution et s'y adapter* ». Ibid.

⁶⁰⁷ Ibid. p. 1

⁶⁰⁸ Union Internationale des Télécommunications, *Rapport Mesurer la société de l'information 2015- Op. Cit.*, p. 3

lui, seulement d'accéder à la connaissance, à l'information et à la culture, mais bien plutôt d'être vu et reconnu dans cette « *économie de l'attention*⁶⁰⁹ ». L'individu, participant ainsi à la diffusion de la surveillance, développe des comportements relevant quasiment de la pathologie - individualisme, égoïsme, comportements égotiques, exhibitionnisme, voyeurisme, narcissisme - afin de s'insérer dans cette économie de l'attention. Cette dernière guidée par le nombre de « likes » ou de « retweet », devient la nouvelle mesure de l'échelle sociale.

212. Ces constats sont également perceptibles à la lecture de deux rapports d'information rendus, l'un au Sénat⁶¹⁰, l'autre à l'Assemblée Nationale⁶¹¹, à quelques années d'intervalle entre 2009 et 2011. Ces deux rapports doivent nécessairement être analysés de manière concomitante. Ces derniers sont liés tout d'abord dans leur prise en compte de la modification du comportement de l'individu liée à la technicisation de son milieu. Alors que le premier de ces rapports évoque les moyens de « *faire du citoyen un « homo numericus » libre et éclairé, protecteur de ses données*⁶¹² », le second s'adresse « *au citoyen numérique en lui permettant d'user de sa raison et de sa liberté*⁶¹³ » en vue de « *faire de l'univers numérique un lieu d'épanouissement des droits des individus*⁶¹⁴ ». Ces deux rapports possèdent également la même trame interrogative quant à la difficulté de protéger la vie privée dans un monde où la vie sociale et privée ont tendance à se confondre. Ainsi, ces deux rapports identifient des facteurs de remises en cause de la protection de la vie privée et des données personnelles que l'on pourrait classer comme suit: la construction d'une « *économie de l'attention* » qui se caractérise par « *une tendance croissante à « l'exposition de soi* »⁶¹⁵ » sur les réseaux sociaux et à travers le « *Web 2.0* », la construction d'un paradoxe entre

⁶⁰⁹ GANASCIA Jean-Gabriel, *Voir et pouvoir: qui nous surveille ?*, Editions Le pommier, Collection Les essais, 2009, p. 201

⁶¹⁰ DETRAIGNE Yves, ESCOFFIER Anne-Marie, *Rapport d'information n° 441 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, Op. Cit.

⁶¹¹ BLOCHE Patrick, VERCHERE Patrice, *Rapport d'information n° 3560 déposé en application de l'article 145 du Règlement par la mission d'information commune sur les droits de l'individu dans la révolution numérique*, Assemblée nationale, 13^{ème} législature, enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011, En ligne: <http://www.assemblee-nationale.fr/13/pdf/rap-info/i3560.pdf> (dernière consultation: 5 mars 2018)

⁶¹² DETRAIGNE Yves, ESCOFFIER ANNE-Marie, Op. Cit., p. 67 et suivants

⁶¹³ BLOCHE Patrick, VERCHERE Patrice, Op. Cit., p. 17

⁶¹⁴ Ibid.

⁶¹⁵ Les deux rapports évoquent cette tendance. Voir: DETRAIGNE Yves, ESCOFFIER ANNE-Marie, Op. Cit., p. 31 et suivantes, BLOCHE Patrick, VERCHERE Patrice, Op. Cit., p. 128 à 135.

d'un côté une « *protection*⁶¹⁶ » de soi, « *une demande accrue de sécurité*⁶¹⁷ » et de l'autre, la vie privée, et des « *facilités offertes par les nouvelles technologies*⁶¹⁸ » de plus en plus « *invasives*⁶¹⁹ ». Et le rapport de 2009 d'ajouter: « *la vie privée tend à se déverser dans la vie publique, dès lors qu'un individu diffuse au public des informations relatives à sa vie privée. Les raisons sont multiples: banalisation de l'usage des techniques, stratégies de projection de soi, arbitrage en faveur d'une vie sociale riche (la « course aux amis » sur les réseaux sociaux), nouveau rapport à la pudeur, décloisonnement des cercles relationnels, sensibilisation insuffisante aux risques d'une exposition de soi et des autres sur Internet, etc*⁶²⁰ ».

213. Bien qu'il soit louable de soulever dans ces deux rapports la question de la vie privée, ces derniers interrogent beaucoup plus la fonction de l'individu et son positionnement face aux nouvelles technologies. Qu'il soit salarié, administré, consommateur ou plus globalement citoyen, ces deux rapports montrent de manière subtile, la soumission latente de l'individu aux nouvelles technologies, et donc, à ceux qui disposent du pouvoir sur cette soumission⁶²¹. Bien qu'essentielles à la bonne compréhension du phénomène de diffusion de la surveillance, ces pistes de réflexions proposées dans le cadre de ces rapports ne sont que des informations. A leur lecture, on comprend à quel point ces pistes n'engagent pas le citoyen. Ces deux rapports se contentent essentiellement d'appliquer l'adage « nul n'est censé ignorer la loi » par un rappel du droit au respect de la vie privée, ainsi que du droit à la protection des données personnelles. Pour la doctrine, ces rapports, et les concepts de citoyen numérique, d'homme numérique ont fait de l'individu « *un citoyen digitalisé et numérisé conscientisé*⁶²² ». Ainsi, le Professeur Guglielmi rappelle que « *l'exercice de la citoyenneté n'a pas pour seul horizon la loi à laquelle il devrait obéir ; il ne se limite pas au dépôt d'un bulletin dans une urne ; il ne se borne pas au vote, à l'élection ; il n'est pas non plus strictement enserré par les circuits de « participation » aux affaires publiques, voire encore à la vie culturelle d'un espace pré-délimité ; il est aussi activité et fonction de « vigilance » pour la défense*

⁶¹⁶ BLOCHE Patrick, VERCHERE Patrice, Op. Cit., p. 124 et suivantes

⁶¹⁷ DETRAIGNE Yves, ESCOFFIER ANNE-Marie, Op. Cit., p. 17 à 26

⁶¹⁸ DETRAIGNE Yves, ESCOFFIER ANNE-Marie, Op. Cit., p.26 à 31. Au titre de ces facilités, les deux rapports évoquent la géolocalisation, la biométrie, la vidéosurveillance, ou encore le ciblage publicitaire

⁶¹⁹ BLOCHE Patrick, VERCHERE Patrice, Op. Cit., p. 139 à 148. Ce rapport évoque particulièrement l'invasion des puces RFID.

⁶²⁰ DETRAIGNE Yves, ESCOFFIER ANNE-Marie, Op. Cit., p.35

⁶²¹ Le secteur privé et le secteur public

⁶²² Voir en ce sens: GUGLIELMI Gilles, « *Homo numericus* », *un citoyen digitalisé et numérisé conscientisé*, [en ligne] 10 Juin 2009, En ligne: <https://www.guglielmi.fr/spip.php?article199#nh2> (dernière consultation: 5 mars 2018)

*des libertés et des droits*⁶²³ ». Et de conclure ainsi, « *ce ne sont pas les considérations relatives au cadre juridique de la protection de la vie privée qui fondent les recommandations exposées pour « faire du citoyen un « homo numericus » libre et éclairé » mais plutôt un souci de (re)légitimation des utilisations faites par les pouvoirs publics, comme par les institutions privées, de ces nouvelles technologies pour étendre la surveillance et repérer les déviances ou les dissidences...*⁶²⁴ ».

B. ... Participant pleinement à l'économie de l'attention: de la malléabilité des individus à la plasticité sociale

214. Principalement réduit à une position de consommateur docile, l'individu ne questionne pas la légitimité et l'acceptabilité des technologies, de la surveillance diffuse. Ses possibilités de remise en question de la surveillance diffuse, en tant qu'acteur de sa propre liberté, sont totalement occultées par la consommation irréfléchie de technologies dans l'économie de l'attention. Ces éléments tendent à conforter la crédulité et la ductilité des individus (1). Plus globalement, l'individu, le consommateur est totalement aliéné par la consommation technologique (2).

1. Le mythe de Narcisse ou la ductilité des individus-consommateur de surveillance diffuse

215. On connaît les liens qu'entretient la surveillance diffuse avec les notions de sécurité, de peur, et plus encore de gouvernementalité par la peur. Le Professeur Guglielmi rappelait déjà dans son article de 2009, que « *les turbulences de la notion de vie privée empêchent l'édification d'un cadrage juridique cohérent dès lors qu'un climat de suspicion généralisée se diffuse. La « peur » qui se répand ainsi suivant les méandres des discours sécuritaires paralyse, tétanise et assure les pouvoirs publics d'une résignation docile qui se comprendrait comme un consentement social aux méthodes de sécurité appliquées. Ainsi, sur le plan individuel, derrière toute réticence affirmée à l'égard de ces techniques d'identification, de repérage, de localisation, de surveillance, etc., se profilerait une sourde culpabilité*⁶²⁵ ». Bien que d'un point de vue juridique « *la sourde culpabilité* » décrite par le Professeur Guglielmi soit exacte - par les méthodes de surveillance, on assiste effectivement à un renversement de la présomption d'innocence pour y préférer une présomption de culpabilité - il ne faut pas, comme nous avons pu le démontrer, réduire cette

⁶²³ Ibid.

⁶²⁴ Ibid.

⁶²⁵ Ibid.

« peur » ou cette demande de sécurité à de simples discours politiques.

216. L'individu a peur de tout, de l'insécurité au chômage, en passant par la précarité, l'environnement, la santé, la nourriture ... Pour chacune de ces peurs s'organise une sécurité correspondante: sécurité alimentaire, sécurité sanitaire, sécurité des médicaments, sécurité des flux bancaires, et progressivement, sécurité humaine. Ce cercle de peur et de sécurité conduit à une nouvelle consommation technologique. Car ainsi que le rappelait Valérie Peugeot en 2007, *« loin de se réduire, nos peurs grandissent chaque jour un peu plus, mutent dans nos intimités, envahissent notre espace public. Elles suscitent deux types de réactions. Soit la sidération: tétanisé par ses peurs, l'individu-citoyen se replie sur sa sphère privée et se réfugie dans la consommation. Soit le rejet pur et simple: les uns niant les peurs des autres ou les dénonçant comme irrationnelles, sans voir qu'ils souffrent parfois d'un syndrome identique⁶²⁶ »*. Cette société de consommateurs est alors placée dans l'incapacité de relativiser ses peurs diabolisées, de contrôler la demande en sécurité correspondante, ni même de réfléchir aux conséquences de la diffusion de la surveillance. Ainsi que le déclarait Hannah Arendt, à propos de la crise de la culture, *« croire qu'une telle société deviendra plus « cultivée » avec le temps et le travail de l'éducation est, je crois, une erreur fatale. Le point est qu'une société de consommateurs n'est aucunement capable de savoir prendre en souci un monde et des choses qui appartiennent exclusivement à l'espace de l'apparition au monde, parce que son attitude centrale par rapport à tout objet, l'attitude de la consommation, implique la ruine de tout ce à quoi elle touche⁶²⁷ »*.

217. Partagés entre la réaction - le repli sur soi - et l'action - l'exhibition - nos contemporains consomment toujours plus de technologies, et sont en quête de reconnaissance dans une « économie de l'attention » où il faut être visible. En cela, l'individu s'inscrit pleinement dans la description que Christopher Lasch envisage lorsqu'il évoquait en 2000 la montée en puissance de la culture du narcissisme. Il écrivait ainsi que *« le nouveau Narcisse est hanté, non pas par la culpabilité mais par l'anxiété. Il ne cherche pas à imposer ses propres certitudes aux autres, il cherche un sens à la vie. Libéré des superstitions du passé, il en arrive à douter de la réalité de sa propre existence. Superficiellement détendu et tolérant, (...), il se trouve également privé de la sécurité que donne la loyauté du groupe et se sent en compétition avec tout le monde pour l'obtention des faveurs que dispense l'État paternaliste.(...). Avidé, dans la mesure où ses appétits sont sans limites, il*

⁶²⁶ DAKHLI Leyla, MARIS Bernard, SUE Roger, VIGARELLO Georges (sous la direction de), *Op. Cit.*, p. 8.

⁶²⁷ ARENDT Hannah, *La crise de la culture - Huit exercices de pensée politique*, *Op. Cit.* p. 270

n'accumule pas les biens et la richesse à la manière de l'individu âpre au gain de l'économie politique du XIX^{ème} siècle, mais il exige une gratification immédiate, et vit dans un état de désir inquiet et perpétuellement inassouvi⁶²⁸ ».

2. La plasticité sociale engendrée par la surveillance diffuse ou l'aliénation des individus

218. La culture du narcissisme décrite par Christopher Lasch se présente à la fois comme la poursuite de la crise de la culture décrite par Arendt, mais également comme une conséquence de la gouvernementalité par la peur et de la modernisation du capitalisme *« dont la fausse conscience libérale-libertaire a fini par devenir l'esprit du temps⁶²⁹ »*. Ces éléments ne sont pas sans rappeler ce que Jacques Ellul évoquait comme conclusion à l'atomisation de la société⁶³⁰. Selon l'auteur, *« cette atomisation confère à la société la plus grande plasticité possible. Et ceci est aussi, du point de vue positif, une condition décisive de la technique. (...). Tout cela n'est possible que lorsque l'homme n'est plus qu'un élément rigoureusement isolé; lorsqu'il n'y a littéralement plus de milieu, de famille, de groupe qui pourra résister à la pression du pouvoir économique, avec sa séduction et sa contrainte; lorsqu'il n'y a déjà presque plus de style de vie propre. (...). Voilà l'influence de la plasticité sociale. Sans elle, pas d'évolution technique possible. Dans cette société atomisée, en face de l'individu, il n'y a plus que l'Etat, qui est fatalement l'autorité suprême, et qui se change aussi bien en autorité toute puissante. Ceci nous donne une société parfaitement malléable et d'une ductilité remarquable au point de vue intellectuel comme au point de vue matériel. Le phénomène technique y a son milieu le plus favorable depuis le début de l'histoire humaine. Or en même temps, coïncidence historique (fortuite ou non, ceci nous dépasse), s'éveille ce que nous avons appelé l'intention technique claire. Dans toutes les autres civilisations, il y a eu un mouvement technique, il y a eu un travail plus ou moins profond dans ce sens, mais on trouve rarement une intention de masse, clairement reconnue et orientant délibérément dans le sens de la technique la société entière⁶³¹ »*. Cette longue et nécessaire citation⁶³¹ permet d'appréhender la société contemporaine en

⁶²⁸ LASCH Christopher, *La culture du Narcissisme – La vie américaine à un âge de déclin des espérances*, Collection Sisyphé, Éditions Climats, 2000, p. 24 - 25.

⁶²⁹ Ibid. Quatrième de couverture.

⁶³⁰ Ellul écrit ainsi que *« Toute la technique est freinée par ces fractionnements sociaux. or, on constate la disparition de tous ces obstacles de façon très brutale et simultanée au moment de la Révolution de 1789. (...). Il n'y a pas de liberté des groupes, mais seulement de l'individu isolé. (...). En réalité, nous avons une société atomisée et qui s'atomisera de plus en plus: l'individu reste la seule grandeur sociologique, mais on s'aperçoit que bien loin de lui assurer sa liberté, cela provoque le pire des esclavages »*. In. ELLUL Jacques, *La Technique ou l'enjeu du siècle*, Op. Cit, p. 47.

⁶³¹ Ibid. p. 47 - 48.

crise, peuplée d'individu isolé et d'une masse narcissique, comme une société entièrement malléable et ductile, entièrement tournée vers la surveillance diffuse. La surveillance diffuse devient la principale caractéristique de la société en crise.

219. Cette affirmation prend tout son sens au regard de certaines manifestations récentes de nouvelles professions⁶³² ou encore des nouveaux usages liés à Internet et aux objets connectés permettant l'émergence du *quantified self*, la quantification de soi, renommée récemment comme auto-mesure connectée par la Commission générale de terminologie et de néologie. Ainsi que le note Alain Desrosières, quantifier consiste à « *exprimer et faire exister sous une forme numérique ce qui, auparavant, était exprimé par des mots et non par des nombres* » alors que « *l'idée de mesure implique que quelque chose existe sous une forme déjà mesurable (...) comme la hauteur de la Tour Eiffel*⁶³³ ». Le nouveau Narcisse cherche à se sentir en sécurité dans sa vie quotidienne, il se mesure en permanence, il jauge sa bonne santé, ou sa bonne humeur, il calcule le nombre de calories de ses repas, il analyse le nombre de pas parcourus dans une journée, estime la régularité des battements de son coeur, la qualité de son sommeil. Il n'hésite alors pas à quantifier toutes ses activités en continu, en temps réel, et contribue par là à « *la production sociale de normes de comportements, de performance et de santé, éminemment évolutives (...) et permettant la visualisation et, éventuellement, la mise en comparaison de leurs progrès respectifs par les utilisateurs reliés directement à l'Internet à travers les capteurs qui les « quantifient »*⁶³⁴ ».

220. Que ce soit par ces nouvelles professions narcissiques ou à cause du *quantified self*, le problème posé par le narcissisme dans nos sociétés, est qu'il porte en son sein une sorte de conformisme social. Il a permis la production dans nos sociétés de normes sociales, de comportements, de logique de performance de soi, de logique de santé, qui, par les progrès

⁶³² On pense notamment aux « youtubeurs » ou encore aux « influenceurs »: des acteurs de la diffusion de la surveillance, conscientisés, rémunérés et cherchant à capter l'attention et à la diffuser.

⁶³³ DESROSIERES Alain, *Pour une sociologie historique de la quantification. L'argument statistique I*, Presses de l'École des mines, 2008, p. 10-11

⁶³⁴ CNIL, *Le corps, nouvel objet connecté – Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde*, Cahiers Innovation et Perspectives n°02, Mai 2014, p.4, En ligne: https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf (dernière consultation: 5 mars 2018)

technologiques, sont de plus en plus évolutives. Une littérature abondante⁶³⁵ insiste depuis quelques années sur les dérives produites par ces comportements narcissiques⁶³⁶, ou pour reprendre les termes de Christopher Lasch cette « *stratégie de la survie narcissique de l'individu, (...) l'homme psychologique de notre temps*⁶³⁷ ». Emmanuel Kessous décrit par exemple deux formes de comportements narcissique que notre société a permis de produire: le « *monopoleur d'attention versus le distributeur d'attention*⁶³⁸ ». Alors que le distributeur d'attention correspond à un être « *responsable de ses troupes, cherchant à les orienter vers les bons sujets ou les bonnes thématiques à traiter, capable également de porter la focale sur un des membres de son équipe, disposé à faire circuler l'attention qu'il reçoit sur d'autres êtres ou d'autres choses*⁶³⁹ », le monopoleur d'attention, quant à lui, « *mobilise les dispositifs de captation dans le but unique d'en retirer un profit personnel, que cela soit un transfert de grandeur attentionnelle dans les mondes marchands ou de l'opinion, ou une forme de profit plus directement liée au monde attentionnel*⁶⁴⁰ ». Ce besoin d'attention décrit par Kessous et Ganascia, et « l'état de désir inquiet » évoqué par Christopher Lasch, se retranscrivent complètement dans des pratiques contemporaines d'auto-

⁶³⁵ A titre d'exemple, on pourra citer ici l'ouvrage publié sous la direction de Nicole Aubert et Claudine Haroche, *Les tyrannies de la visibilité, être visible pour exister ?*, Collection « sociologie clinique », Éditions érès, 2013, et spécialement les contributions de Joël Birman, *Je suis vu, donc je suis : la visibilité en question*, p.39-52, et de Francis Jauréguiberry, *L'exposition de soi sur Internet : un souci d'être au-delà du paraître*, p.131-144, où ces auteurs développent l'idée d'une mise en œuvre par les technologies de l'information et de la communication d'un cyber-narcissisme. Mais surtout, il faut ici citer l'œuvre de Christopher Lasch en commençant par son livre intitulé, *La culture du Narcissisme – La vie américaine à un âge de déclin des espérances*, Collection Sisyphe, Éditions Climats, 2000, préfacé par Jean-Claude Michéa (préface intitulée : *Pour en finir avec le XXIe siècle*) ; ainsi que la retranscription de son entretien avec Cornelius Castoriadis in., *La culture de l'égoïsme*, Climats, 2012.

⁶³⁶ Christopher Lasch insiste ainsi sur la bonne compréhension de la culture du narcissisme: « *ce livre décrit une manière de vivre qui est en train de mourir – la culture de l'individualisme compétitif. Celle-ci, dans sa décadence, a poussé la logique de l'individualisme jusqu'à l'extrême de la guerre de tous contre tous, et la poursuite du bonheur jusqu'à l'impasse d'une obsession narcissique de l'individu par lui-même.* » (Op. Cit. p. 24)

⁶³⁷ Ce concept « *d'homme psychologique de notre temps* » est à comprendre dans le sens de l'acclimatation de l'individu à son milieu de la technologique poussé d'abord, à l'époque industrielle par la recherche du gain économique, puis avant et pendant la crise de la culture, par la connaissance, et enfin dans le cadre de l'économie de l'attention, par la reconnaissance. Pour preuve, Christopher Lasch écrit: « *« la stratégie de la survie narcissique de l'individu se présente maintenant comme une libération des conditions répressives du passé, donnant ainsi naissance à une « révolution culturelle » qui reproduit les pires traits de cette même civilisation croulante qu'elle prétend critiquer. Le « radicalisme culturel » en vogue est devenu si pernicieux par le soutien qu'il apporte, sans le vouloir, au statu quo, que toute critique de la société contemporaine, qui ne veut pas se contenter des apparences, doit également remettre en question bien des actions qui se réclament du radicalisme. Les événements ont rendu totalement périmés, tant les critiques visant à libérer la société, qu'une grande partie de l'ancienne analyse marxiste. De nombreux radicaux s'insurgent encore contre la famille autoritaire, la moralisme anti-sexuel, la censure littéraire, la morale du travail et autres piliers de l'ordre bourgeois, alors que ceux-ci ont déjà été sapés ou détruits par le capitalisme avancé. Ces radicaux ne voient pas que la « personnalité autoritaire » n'est plus le prototype de l'homme économique. Ce dernier a lui même cédé la place à l'homme psychologique de notre temps – dernier avatar de l'individualisme bourgeois.* » (Op. Cit. p. 24)

⁶³⁸ KESSOUS Emmanuel, *L'attention au monde, sociologie des données personnelles à l'ère du numérique*, Editions Armand Colin, Collection Recherches, 2012, p. 204 à 206.

⁶³⁹ Ibid. p.206.

⁶⁴⁰ Ibid. p. 205

surveillance⁶⁴¹, de sous-veillance⁶⁴², ou encore de participation consciente à la surveillance.

221. Pour la compréhension de cette logique de transformation des comportements des individus par le narcissisme, il importe d'évoquer également des exemples de participation pleinement consciente de l'individu, du « citoyen conscientisé » à la diffusion de la surveillance. Couplée à l'analyse de la marchandisation de la sécurité, il faut, en effet, comprendre aujourd'hui le citoyen - le philistin cultivé numérisé narcissique - comme consommateur de sécurité-protection, mais aussi comme producteur de sécurité-protection⁶⁴³, et donc de surveillance. Le fait de transformer la sécurité en un bien de consommation a permis de faciliter son accès. Le citoyen a pu acheter de la sécurité auprès de fournisseurs privés, et peut, en plus de consommer la sécurité et la surveillance, la produire. Il est ainsi en capacité d'installer des caméras de vidéosurveillance⁶⁴⁴, d'investir dans des systèmes d'alarmes contrôlés par des fournisseurs privés, ou par lui-même grâce à la domotique. Présentées comme neutres, ces technologies de sécurité sont mises à la disposition de Narcisse en vue de diminuer ses craintes, ses peurs, et d'augmenter son sentiment de sécurité et de protection. Producteur conscientisé, il le devient également au travers d'initiatives dites populaires de vigilance citoyenne, ou de surveillance de quartier⁶⁴⁵. Si, à l'origine, la participation des citoyens à la surveillance de leurs biens et de leurs quartiers n'a pas forcément fonctionné, ce dispositif s'est progressivement développé en France depuis 2011. Généralement piloté par convention par le Préfet et encadré strictement par les forces de sécurité de l'Etat, il consiste à faire appel aux citoyens volontaires d'une commune pour accroître le niveau de sécurité. La volonté première de ce dispositif est donc de mener une action concertée de vigilance dans une démarche collective, ainsi que de restaurer une confiance entre la population et les acteurs de sécurité. Selon le Ministère de l'intérieur; c'est en cela, que « *ce dispositif s'intègre dans la gamme des outils dédiés à la prévention de la délinquance et demeure complémentaire de l'action quotidienne des forces de sécurité de l'État, notamment des services de prévention de proximité*⁶⁴⁶ ».

⁶⁴¹ Le quantified self précédemment évoqué

⁶⁴² Analysé par Ganascia comme la surveillance des surveillants.

⁶⁴³ Les exemples qui précèdent concernant spécialement le quantified self s'inscrivent également pleinement dans cette démarche de sécurité protection

⁶⁴⁴ Avec comme seule limite, le fait de respecter les prescriptions issues de la loi.

⁶⁴⁵ Fortement inspiré du concept anglo-saxon des « *neighbourhood watch* », ce dispositif se généralise en France.

⁶⁴⁶ Réponse du Ministère de l'intérieur publiée dans le JO, Sénat, 16 avril 2015, p. 887, à la question écrite n°13406 de M. Hervé Maurey publiée dans le JO, Sénat, 23 octobre 2014, p. 2375, En ligne: <https://www.senat.fr/questions/base/2014/qSEQ141013406.html> (dernière consultation: 5 mars 2018)

222. Plus qu'une re-légitimation des services de sécurité de l'Etat, on cherche ici à banaliser la notion de surveillance, tout en la faisant entrer dans les moeurs par son versant sécurité-protection. Il faut noter que, de manière globale, les procédés mis en place - qu'il s'agisse d'auto-surveillance, de sous-veillance, ou encore de surveillance - sont de plus en plus discrets. Ils deviennent transparents pour les citoyens qui les considèrent comme devant s'intégrer pleinement à sa vie quotidienne. Par là, la surveillance devient un bien de consommation banal. La surveillance diffuse, quant à elle, devient la caractéristique essentielle de la culture contemporaine.

223. Pour Lucien Jerphagnon, Narcisse a péché, non pas par le fait de « *s'être complu dans sa beauté - c'est précisément le châtiment -, mais bien d'avoir prétendu à l'auto-suffisance érotique*⁶⁴⁷ ». Le nouveau citoyen que la société de l'information et de la communication, puis la diffusion de la surveillance a créé est un philistin cultivé, numérisé, conscientisé, et narcissique. Entre le mythe de Narcisse et cet individu contemporain, il faut noter les ressemblances: fascination par l'image et par son image, plongée vers elle, volonté d'attirer l'attention, de connaître et volonté de reconnaissance, véritable aliénation par l'image. Reste alors à savoir si Narcisse 2.0, frustré de son image, dépérira également.

⁶⁴⁷ JERPHAGNON Lucien, *Plotin, ou l'anti-Narcisse*, In: *Platonisme et néoplatonisme. Antiquité et temps modernes*. Actes du 1er colloque de la Villa Kérylos à Beaulieu-sur-Mer du 27 au 30 septembre 1990. Paris : Académie des Inscriptions et Belles- Lettres, 1991. pp. 46-50. (Cahiers de la Villa Kérylos, 1); En ligne: http://www.persee.fr/docAsPDF/keryl_1275-6229_1991_act_1_1_864.pdf (dernière consultation: 5 mars 2018)

Conclusion de Titre

224. La surveillance diffuse s'est progressivement institutionnalisée dans les sociétés contemporaines. Le premier temps de l'analyse de ce phénomène de société démontre que cette institutionnalisation a été permise grâce aux progrès technologiques et scientifiques, mais également à l'investissement de nombreux acteurs en ce sens. Contribuant à la création d'un projet de société, la société de l'information, ces éléments ont fait des notions d'information et de communication des véritables enjeux de pouvoir et de domination principalement réduits à leurs versants économiques.

225. Des stratégies de marketing des entreprises aux stratégies de communication des Etats, cette volonté de construction de l'économie du numérique a engendré une banalisation de la surveillance. Gouvernamentalité par la peur, marchandisation de la sécurité, consommation technologique irréfléchie en sont les principales conséquences. En s'institutionnalisant dans la culture contemporaine en crise, la surveillance est devenue l'une des caractéristiques essentielles de la société contemporaine. Cette société globalisée a permis aux principaux leaders du numérique et de leur alliés institutionnels et politiques d'émettre toujours plus de technologies dans l'espace public et privé en vue de la réception de toujours plus d'informations. Revêtant deux formes principales, la surveillance diffuse vise alors à entretenir ce que Breton évoque sous l'expression de croyance en la toute puissance libératrice des technologies. A visée sécuritaire, la surveillance diffuse protège les individus contre les risques et les menaces contemporaines, qu'il s'agisse de terrorisme, de délinquance ou de risques écologiques et sanitaires. A visée marketing, la surveillance diffuse offre un bénéfice à l'individu: auto-contrôle, réassurance sur sa santé, fluidité d'accès à la culture, aux savoirs et à la connaissance. Ces éléments permettent alors de constater que la surveillance diffuse doit être analysée comme le nouveau projet de société élaboré en co-production entre le secteur privé et public, et culturellement intégré par les individus.

226. Se situant dans le prolongement des analyses de Arendt et de Lasch concernant la crise de la culture et la culture du narcissisme, la surveillance diffuse s'est aujourd'hui définitivement institutionnalisée du fait même des individus. Dans la société de masse, les individus conscientisés sont entièrement tournés vers la consommation technologique. Ces nouveaux Narcisse ont-ils conscience de l'amoindrissement progressif de leur sphère privée ? A travers la mise en donnée du monde de leurs activités, de leurs vies mêmes, ont-ils conscience d'être progressivement mis en marché par la captation et le traitement de leurs données personnelles ? Comprennent-ils que la

surveillance diffuse porte en son sein la prise en charge et l'organisation de la plasticité sociale ? Plus Narcisse dévoilera sa vie privée de manière consciente ou non, plus il se placera dans la position d'un citoyen-consommateur, plus il dévoilera ses données personnelles et plus il participera à sa fragilisation au profit d'acteurs publics et privés.

Titre 2: Une intégration délicate de la surveillance diffuse dans la protection offerte au titre du droit des données personnelles sous l'empire de la loi de 1978 et de la directive de 1995

227. La surveillance diffuse doit être analysée comme une attention permanente du secteur privé et du secteur public permettant à la fois l'organisation de la traçabilité des activités humaines, mais également la réduction de l'individu à une trace, à une empreinte numérique. Ces éléments engendrent la normalisation des comportements des individus, et à l'échelle de la société, une forme de plasticité sociale. Nulle référence ici à la notion de donnée personnelle, ni même à celle de vie privée. Pourtant ces deux notions représentent l'enjeu du siècle de la surveillance diffuse. En face des problèmes de droit posés par la surveillance diffuse, qu'elle soit utilisée dans le cadre de son objectif sécuritaire, ou qu'elle le soit dans le cadre global de la poursuite du marché du numérique, le juriste a parfois quelques difficultés à situer son intervention face au traitement de données.

228. Les possibilités offertes par les technologies en constante évolution troublent de plus en plus la notion même de données personnelles. Le traitement absolu par la surveillance diffuse de toutes informations personnelles et non personnelles, pour reprendre les termes de Liesbeth van Zoonen⁶⁴⁸, rend complexe l'opération de qualification de la donnée et du traitement de la donnée, en tant que personnelle. Pour le dire autrement, certains traitements opérés par la surveillance diffuse ne permettent pas d'identifier ou de rendre identifiables des individus, mais ces traitements ne sont pas pour autant anodins pour les Droits et Libertés de ces derniers. Ainsi que le notaient Antoinette Rouvroy et Thomas Berns, « *l'abondance des études, rapports et publications dédiés à la problématique attestent des difficultés d'application, de l'insuffisance, voire de l'inadéquation, des régimes juridiques de protection de la vie privée et de protection des données à caractère personnel face à la gouvernementalité découlant du recueil massif et continu de données personnelles et contextuelles en tous genres, de leur traitement à des fins générales de profilage notamment, de leur conservation par défaut sans que soit énoncée a priori de finalité spécifique. Il est d'ailleurs loin d'être établi que, techniquement, toutes ces données soient assimilables à des données à caractère personnel (c'est-à-dire relatives à des individus identifiés ou identifiables) au sens du régime juridique de protection, alors même que l'impact de ces traitements sur les personnes peut être au*

⁶⁴⁸ VAN ZOONEN Liesbet, Privacy concerns in smart cities, *Government Information Quarterly*, 2016, En ligne: <http://www.sciencedirect.com/science/article/pii/S0740624X16300818> (dernière consultation: 5 mars 2018)

moins aussi significatif et potentiellement défavorable que le traitement de données à caractère personnel au sens traditionnel du terme⁶⁴⁹ ».

229. Cette affirmation représente l'enjeu essentiel de la confrontation de la surveillance diffuse et de la protection des données personnelles et de la vie privée. Elle démontre de l'intégration délicate de la surveillance diffuse à ce titre. Pour analyser cet enjeu, il est important d'évoquer la protection offerte aux individus au titre de la loi de 1978 et de la directive de 1995. Du fait de leur champ d'application, ces instruments permettent d'envisager un large panel de situations engendrées par la surveillance diffuse. Toutefois, l'intégration de cette dernière dans la protection offerte au titre du droit des données personnelles et de la protection de la vie privée reste délicate. Ces dispositions souffrent en effet d'un déficit d'effectivité global (chapitre 2) favorisé par un déficit de conscience des enjeux de la surveillance diffuse (chapitre 1). C'est alors de ce double déficit que l'on peut conclure à l'intégration délicate de la surveillance diffuse dans la protection offerte aux individus sous l'empire de la loi de 1978 et de la directive de 1995.

⁶⁴⁹ ROUVROY Antoinette, Berns Thomas, « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événements car constitué de corps « numériques »... », *Multitudes* 2010 / 1 (n° 40), p. 88 - 103, p. 99 - 100, En ligne: <https://www.cairn.info/revue-multitudes-2010-1-page-88.htm> (dernière consultation: 5 mars 2018).

Chapitre 1: Un déficit de conscience des enjeux de la surveillance diffuse sous l'empire de la loi de 1978 et de la directive de 1995:

230. Afin d'opérer une confrontation réelle entre la surveillance diffuse et la protection offerte aux individus au titre du droit des données personnelles, il est nécessaire de comprendre la surveillance diffuse comme l'élaboration de ce que Eric Sadin nomme le « *data-panoptisme*⁶⁵⁰ » permis par la « *totalisation numérique*⁶⁵¹ ». Par ces concepts, on comprend d'une part la surveillance diffuse comme un panoptique numérique. A ce titre, les études de Bentham, Foucault et Deleuze doivent être activées. Ces dernières permettront de dessiner les contours des effets insidieux de la surveillance et de les appliquer à la surveillance diffuse.

231. Du principe d'inspection de Bentham à l'importance du regard dans l'analyse du panoptique réalisée par Foucault, tout se passe aujourd'hui comme si le curseur de la surveillance se déplaçait de l'individu à ses données et ses traces. La surveillance diffuse ne s'opère pas aujourd'hui en milieu clos ou encore en milieu d'enfermement. Et si le panoptique représente une technique de pouvoir, il ne semble plus réellement d'actualité aujourd'hui. En effet, le principal moyen de surveillance réside, dans nos sociétés contemporaines, dans la puissance des ordinateurs et systèmes informatiques à collecter, traiter, stocker, enregistrer, appairer, commercialiser, transférer et faire circuler des données. C'est bien la croissance massive des usages liés à l'informatique et à son application dans des domaines de plus en plus variés qui fait des technologies de l'information et de la communication l'architecture même de la surveillance diffuse.

232. Le recours au concept de data-panoptisme (section 2) permet de comprendre la notion de data comme étant au coeur de la problématique que pose la surveillance diffuse. Malgré le champ d'application large des dispositions en place (section 1), le data-panoptisme permet d'éluder de la protection un large champ de données, principalement non personnelles, et ainsi de contribuer à la traçabilité des individus et à la réduction des ces derniers à une trace numérique.

⁶⁵⁰ SADIN Eric, *La vie algorithmique - Critique de la raison numérique*, Editions L'échappée, Collection Pour en finir avec, 2015, p. 169

⁶⁵¹ Ibid. p. 44 et suivantes.

Section 1: La protection des données personnelles issue de la loi de 1978 et de la directive de 1995: une volonté de protéger l'individu par un champ d'application large

233. Dans sa mouture originelle, la loi informatique et libertés évoquait la notion d'information nominative en lieu et place du concept de données personnelles. Avec sa modification en 2004, les concepts de données personnelles, de traitement de données à caractère personnel sont devenus les notions opérantes de la protection des personnes physiques à l'égard de l'informatisation de la société. Les principales dispositions du droit français et européen doivent être exposées (paragraphe 1). Elles permettent en effet de comprendre le respect de la vie privée appliqué aux données à caractère personnel, ainsi que le champ d'application large envisagé par ces instruments (paragraphe 2).

Paragraphe 1: Le respect de la vie privée appliqué aux données à caractère personnel

234. Les mécanismes de protection propres aux données à caractère personnel sont mis en place dès qu'un traitement de telles données est opéré. Le respect de la vie privée appliqué aux données à caractère personnel doit alors être étudié en deux temps: en amont du traitement (A) et en aval (B).

A. En amont du traitement de données à caractère personnel

235. Les principales définitions (1) et les modalités de collecte et de traitement de données personnelles (2) doivent ici être évoquées.

1. Les principales définitions posées par la loi de 1978 et la directive de 1995

236. Le régime applicable aux données à caractère personnel est principalement issu de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette dernière a fait l'objet d'un grand nombre de modifications afin d'être en adéquation avec l'avancée des technologies et l'évolution du droit Européen en la matière⁶⁵². Ces dispositions possèdent un large champ d'application, puisqu'elles concernent tous les traitements de données à caractère personnel, qu'ils soient automatisés ou non. Dans le but de prévenir d'éventuels abus, le législateur a opéré un travail

⁶⁵² Directive 95/46/CE, du Parlement Européen et du Conseil, en date du 24 octobre 1995, transposée en droit Français par la loi n°2004-801 du 6 Août 2004

de définition des différentes notions visées⁶⁵³. La loi de 1978, dans sa première mouture, évoquait clairement la notion d'informations nominatives, et encadrait la collecte et l'utilisation des ces dernières. Définies à l'article 4 de la loi, cette notion devait s'entendre comme les « *informations qui permettent sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale*⁶⁵⁴ ». L'article 45 de la loi excluait de son champ d'application les traitements dont « *l'usage relève du strict exercice du droit à la vie privée*⁶⁵⁵ ». Dans les faits, la loi de 1978 s'appliquait alors aux traitements automatisés entendus dans le sens de l'article 5 de cette dernière comme « *tout ensemble d'opérations réalisées par les moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation des fichiers ou bases de données et notamment les interconnexions et rapprochements, consultations ou communications d'informations nominatives*⁶⁵⁶ ».

237. Avec le développement croissant de l'informatique au sein de l'ensemble des activités humaines, de nouveaux défis liés à « *la convergence technologique*⁶⁵⁷ » et à l'apparition « *des milliers de Big brother privés potentiels*⁶⁵⁸ » ont poussé l'Europe à envisager un cadre d'harmonisation de la protection des personnes physiques à l'égard du traitement des données personnelles au travers de la directive 95/46 précitée, transposée en France en 2004. Aujourd'hui, la définition d'une donnée à caractère personnel vise « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un*

⁶⁵³ Et spécialement au sein de l'article 2 de la Loi du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004, En ligne: https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive-annotee.pdf (dernière consultation: 5 mars 2018)

⁶⁵⁴ Loi n° 78-17 du 6 Janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, Journal Officiel du 7 Janvier 1978, p.227, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000886460 (dernière consultation: 5 mars 2018)

⁶⁵⁵ Ibid. Art. 45

⁶⁵⁶ Ibid. Art. 5

⁶⁵⁷ TURK Alex, *Rapport n°218 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif 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*, Sénat, session ordinaire de 2002-2003, annexe au procès-verbal de la séance du 19 mars 2003, p. 21, En ligne: <https://www.senat.fr/rap/l02-218/l02-2181.pdf> (dernière consultation: 5 mars 2018)

⁶⁵⁸ Ibid.

numéro d'identification ou à un ou plusieurs éléments qui lui sont propres⁶⁵⁹ ». La loi va jusqu'à préciser que pour déterminer si une personne est identifiable, il faudra considérer « l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne⁶⁶⁰ ». De la même manière, la définition du traitement applicable aux données à caractère personnel va toucher non seulement un grand nombre d'algorithmes informatiques, mais, dans l'ensemble, « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé⁶⁶¹ ». Il est donnée une liste, non exhaustive, des différents traitements concernés tels que « la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction⁶⁶² ».

238. Cette définition très large vient s'appliquer à la plupart des traitements, et a été complété par extension jurisprudentielle à l'égard d'opérations particulières telles que, par exemple, les recueils d'adresses électroniques composés à des fins de prospections⁶⁶³ ou les dispositifs d'écoutes téléphoniques des salariés⁶⁶⁴. Il est également à noter que la définition distincte de fichier, donnée par la loi, en tant que « tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés⁶⁶⁵ » n'est pas une notion isolée, mais relève bien d'une sous-partie du régime applicable aux traitements. Dans le cadre du rapport de la Commission des lois du Sénat rendu le 19 mars 2003, Alex Türk déclare que « la directive s'applique à toutes les formes de traitements automatisés, qu'ils se rapportent ou non à l'exploitation de fichiers ou de bases de données, la Commission européenne ayant jugé dépassée la notion de « fichier ». La seule référence à la notion de traitement doit permettre d'appliquer les règles de la protection à toute technologie et à toute organisation particulière de données. Les opérations de collecte constituent en elles-mêmes un traitement, et la mise en œuvre d'une seule des opérations énoncées par l'article

⁶⁵⁹ Article 2 de la loi précitée

⁶⁶⁰ Ibid.

⁶⁶¹ Ibid.

⁶⁶² Ibid.

⁶⁶³ Voir par exemple: Cass. Crim. 14 mars 2006, n° de pourvoi: 05-83423, Publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007069872> (dernière consultation: 5 mars 2018)

⁶⁶⁴ Voir par exemple: TGI Paris, 1ere Ch. 4 avril 2006

⁶⁶⁵ Article 2 de la loi précitée

2,b) de la directive suffit à caractériser le traitement de données⁶⁶⁶ ». Dans ce même rapport, il est précisé que « la notion de fichiers traditionnels apparaît largement obsolète et incapable de recouvrir l'ensemble des problèmes. La directive opère d'ailleurs un glissement sémantique substituant à l'expression « informations nominatives » celle de « données à caractère personnel » afin de garantir la protection de la vie privée « quelles que soient les techniques concernées » et adopte une neutralité technologique visant à préserver la loi d'évolutions aujourd'hui imprévisibles⁶⁶⁷ ».

239. L'ensemble de ces dispositions est applicable aux responsables de traitement. Ces derniers sont définis comme étant « sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens⁶⁶⁸ ». Le législateur a choisi ici de se démarquer de la position Européenne et de la directive 95/46/CE en supprimant la possibilité d'une co-responsabilité dans la détermination des finalités pour éviter une éventuelle pluralité de responsabilité. Au titre de ces dispositions, un seul responsable de traitement, personne physique ou morale⁶⁶⁹, est désigné.. Le contrôle portera donc principalement sur la finalité du traitement, qui doit être déterminée, et dont tout détournement est passible de 5 ans d'emprisonnement et de 300 000€ d'amende⁶⁷⁰. Entre autres conditions, celle-ci devra être précise et cohérente avec les informations recueillies. Ce principe reste l'un des fondamentaux de la protection, et un des principaux point auquel la Commission Nationale de l'Informatique et des Libertés⁶⁷¹ s'attache lorsqu'elle effectue un contrôle. Cette autorité administrative indépendante, définie par la loi du 6 janvier 1978, est chargée de veiller à la protection des données personnelles et dispose d'un pouvoir de contrôle et de sanction dont le montant peut atteindre 300 000 euros. Celle-ci peut accéder à tous les locaux professionnels, demander la communication de tous documents pour recueillir les informations nécessaires et avoir accès aux programmes informatiques.

⁶⁶⁶ TURK Alex, *Rapport n°218 (...) relatif 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*, Op. Cit., p. 49

⁶⁶⁷ Ibid. p. 22

⁶⁶⁸ Op. Cit.

⁶⁶⁹ Désignée comme étant une entité pouvant réunir plusieurs personnes, employés ou sous-traitants, et étant celle qui réalise les traitements pour son compte

⁶⁷⁰ Art. 226.21 du Code Pénal

⁶⁷¹ CNIL

240. Ce retour sur les concepts opérants de la protection des données à caractère personnel permet d'offrir un traitement intelligible de la question de la protection de la vie privée au vu de la surveillance diffuse. Inscrit à l'article 9 du Code civil, le droit à la protection de la vie privée⁶⁷² est l'une des plus essentielles déclinaisons de la liberté individuelle inscrite à l'article 66 alinéa 2 de la Constitution de 1958. Les atteintes que la surveillance diffuse est susceptible de faire peser sur le respect des données personnelles et sur le respect de la vie privée sont nombreuses. Elles résultent de l'activité des individus, qu'elle soit numérique ou non, mais également du traitement automatisé de données personnelles concernant l'individu, ainsi que de l'interconnexion de bases de données.

2. Les modalités de collecte et de traitement de données à caractère personnel

241. Le régime applicable aux responsables de traitement se caractérise par un certain nombre de principes applicables aux conditions d'acquisition des données et au processus de traitement. Il s'agit tout d'abord de respecter, ainsi que le mentionne l'article 6 de la loi de 78 modifiée, un principe de loyauté et de licéité dans la collecte et le traitement de données personnelles⁶⁷³. Globalement, ces deux éléments visent à répondre à un impératif général de transparence quant au mode opératoire développé dans le cadre du traitement. Plus largement, le principe de loyauté est à mettre en parallèle avec l'examen de la finalité du traitement qui doit être déterminée, explicite et légitime. Principe issu de la nouvelle rédaction de l'article 6.2 amenée par la loi du 6 août 2004, il vise à informer les sujets du traitement autant qu'à juger de la cohérence des informations recueillies avec ses objectifs affichés. En principe, ce principe de loyauté dans l'utilisation des données personnelles collectées permet d'établir un cadre strict dans la collecte de données. Fortement lié à l'obligation de consentement préalable de la personne concernée par le traitement de données, le principe de loyauté permet de faire en sorte que les données obtenues fassent l'objet d'une information de la personne concernée, qui jouit alors de la possibilité de s'opposer à leur utilisation⁶⁷⁴. Si la licéité fait essentiellement référence aux droits du sujet du traitement, le principe de loyauté est plus large dans son applicabilité. Par exemple, le fait de recourir à un sondage politique pour recueillir, sans le consentement des personnes sondées, leurs données personnelles et

⁶⁷² En matière numérique, la protection de la vie privée mélange à la fois la liberté, la confidentialité et la sauvegarde des intérêts personnels.

⁶⁷³ Article 6.1 de la loi du 6 janvier 1978

⁶⁷⁴ Article 38 de la loi du 6 janvier 1978

leurs emails a été jugé déloyal⁶⁷⁵. Est considéré également comme constitutif d'une collecte déloyale, le fait de procéder à la collecte d'adresses de courrier électronique sur des forums de discussion, listes de diffusion, sites Internet, sans que les personnes concernées n'en aient eu connaissance⁶⁷⁶. Au titre de ce principe de loyauté et au vu de l'article 226-15 du Code Pénal, il est donc impossible en principe « *d'intercepter, de détourner, d'utiliser, ou de divulguer des correspondances émises, transmises ou reçues par voie de télécommunications* ». C'est ainsi que, depuis 2001 et l'arrêt Nikon⁶⁷⁷, il est nécessaire de distinguer, sur le lieu de travail, les correspondances appartenant à l'entreprise, des correspondances privées, dont l'accès est réservé au destinataire du message. Ainsi, l'inscription sur un mail échangé sur le lieu de travail d'un contenu « privé » ou « professionnel » (sorte de finalité), détermine son régime juridique. Il y a donc, par l'arrêt Nikon, reconnaissance d'une obligation de loyauté pesant sur l'employeur vis-à-vis du salarié quant au respect de sa vie privée. La loyauté et le respect de la finalité inspireront le traitement jusqu'à la destruction des informations nominatives, puisque celles-ci ne pourront être « *traitées ultérieurement de manière incompatible avec les finalités* » initialement déterminées.

242. En plus du respect strict de la finalité, le législateur a inséré une autre exigence, d'origine internationale⁶⁷⁸, qui s'attache à vérifier la proportionnalité du traitement avec les données personnelles collectées. Celui-ci devra porter sur des données « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*⁶⁷⁹ ». Dans ce contexte, le recueil d'information sur le logement et la situation financière de l'hébergeant a été jugé adéquat et pertinent au regard de la finalité du fichier de demandes de validation des attestations d'accueils étrangers⁶⁸⁰. Cependant, si ce critère permet d'effectuer un contrôle, il peut également constituer un terrain favorable pour exercer un recours contre un refus d'autorisation de la CNIL.

⁶⁷⁵ Voir par exemple: Tribunal Correctionnel de Nanterre, 4 juin 2004

⁶⁷⁶ Voir en ce sens: CNIL, Délibération n° 02-075 du 24 octobre 2002 portant dénonciation au Parquet d'infractions à la loi du 6 janvier 1978, En ligne: https://www.cnil.fr/sites/default/files/typo/document/delib_spam.pdf (dernière consultation: 5 mars 2018)

⁶⁷⁷ Cass. Soc., Audience publique du mardi 2 octobre 2001, N° de pourvoi n° 99-42942, NIKON, Publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007046161> (dernière consultation: 5 mars 2018)

⁶⁷⁸ Convention STE n°108 du Conseil de l'Europe du 28 janvier 1981 reprise par la directive 95/46/CE

⁶⁷⁹ Article 6.3 de la loi informatique et libertés

⁶⁸⁰ Conseil d'État, 26 juillet 2006, n°285714

243. Dans le but de rendre plus efficaces les obligations précitées, le législateur a mis en place une nouvelle nécessité correspondant au caractère exact et complet des données collectées, avec comme corollaire, celle de les tenir à jour. Dans cette optique, une procédure au sein du traitement doit être établie pour que « *les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées* ». Cela permet d'éviter l'édition d'un fichier dans lequel certaines informations dépasseraient le cadre strict de la finalité du traitement, ou dont la mauvaise saisie aurait des conséquences défavorables pour le sujet du traitement. En dernier lieu, il convient de préciser que la loi informatique et liberté précise que « *il est interdit de collecter ou de traiter des données faisant apparaître directement ou indirectement, les origines raciales ou ethniques, les opinions philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé, ou à la vie sexuelles de celles-ci*⁶⁸¹ ». Enfin, le responsable de traitement doit être vigilant quant à la durée de conservation des données. Celles-ci doivent être conservées « *sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées*⁶⁸² ». Cette durée à appréciation variable est susceptible de générer un certain nombre de questionnements, alors même que la conservation d'une donnée au-delà de la période légale est sanctionnée de cinq ans d'emprisonnement et de 300 000€ d'amende, et jusqu'à 1 500 000€ s'il s'agit d'une personne morale.

B. En aval du traitement de données à caractère personnel

244. A travers l'ensemble des obligations et principes fondamentaux liés à la protection des données personnelles, le législateur a souhaité envisager très tôt une protection élargie des personnes physiques contre les risques induits par l'informatique sur leur vie privée. Ces principes d'application volontairement large tendent à envisager un large panel de situations que le développement de l'informatique a permis. A priori, la surveillance diffuse, par l'utilisation de l'informatique et le traitement de données personnelles, est concernée par le champ d'application de ces dispositions. Il en va de même pour ce qui est des obligations liées aux éléments faisant suite au traitement, en ce compris les droits des sujets du traitement (1) et la responsabilité et les obligations de sécurisation liées aux traitements (2)

⁶⁸¹ Article 8 de la loi informatique et libertés

⁶⁸² Article 6.5 de la loi informatique et libertés

1. Les droits des sujets du traitement : une ambition du législateur à donner aux individus la maîtrise de leurs données personnelles

245. La protection du sujet du traitement, issue de la loi du 6 janvier 1978, va s'appliquer à l'ensemble des traitements de données à caractère personnel et aux responsables de traitement établis sur le territoire Français. Le simple fait d'exercer une activité, de disposer d'une installation ou de recourir à des moyens de traitement sur le sol Français, indépendamment de la forme juridique, suffit à caractériser l'applicabilité du régime. Permettant aux individus concernés par les traitements d'exercer un contrôle sur les données collectées, un certain nombre de droits ont été consacrés par le législateur. Ces droits sont exploitables par les sujets du traitement, mais relèvent en grande partie de la responsabilité du responsable de traitement dans leur mise à disposition. En appui des différentes obligations précitées, une considération particulière doit être portée aux conditions de recueil du consentement préalable du sujet du traitement. Selon l'article 7, seuls « *le respect d'une obligation légale incombant au responsable de traitement, la sauvegarde de la vie de la personne concernée, l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement, l'exécution d'un contrat auquel la personne est partie, ou la réalisation d'un objectif légitime ne méconnaissant pas l'intérêt ou les droits et libertés fondamentales de la personne concernée* » sont susceptibles de passer outre cette étape. Selon la Commission européenne, « *lorsqu'un consentement éclairé est exigé, les règles en vigueur prévoient que l'accord de l'intéressé sur le traitement de données à caractère personnel le concernant devrait consister dans toute manifestation de volonté, libre, spécifique et informée par laquelle il accepte ce traitement*⁶⁸³ ».

246. Le cadre légal de protection de la vie privée impose le respect d'un principe fondamental: le respect des droits de la personne concernée. Il s'agit, d'abord, du droit à l'information de la personne auprès de laquelle sont recueillies les données à caractère personnel la concernant. Celle-ci devra être informée de l'identité du responsable de traitement, de l'objectif de la collecte

⁶⁸³ Commission européenne, *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions - Une approche globale de la protection des données à caractère personnel dans l'union européenne*, Bruxelles, 4 novembre 2010, COM (2010) 609 final, p. 9, En ligne: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:FR:PDF> (dernière consultation: 5 mars 2018). Et, Groupe de travail « article 29 » sur la protection des données, Avis 15/2011 sur la définition du consentement, 13 juillet 2001, 01197/11/FR, WP 187, En ligne: https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp187_fr.pdf (dernière consultation: 5 mars 2018)

d'information, du caractère obligatoire ou facultatif des réponses, des conséquences de l'absence de réponse, des destinataires des informations, des droits reconnus à la personne ainsi que les transferts éventuels vers un pays hors de l'Union Européenne. La loi de transposition en date du 7 août 2004 a ajouté le fait que toute personne a le droit d'interroger le responsable de traitement en vue d'obtenir « *la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement, des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées*⁶⁸⁴ », et ce en vertu du droit d'accès. En justifiant de son identité, la personne concernée aura le droit de prendre connaissance de l'intégralité des données recueillies, ainsi que d'en réclamer une copie, faculté que le responsable peut soumettre à paiement, dans la limite où ce coût ne dépasse pas celui de la reproduction. Cette extension du droit à l'information revêt un caractère crucial pour la défense des droits du citoyen dans la mesure où celle-ci permet un contrôle de la nature du traitement et de son adéquation avec les données collectées. Pour cette raison, le législateur a précisé qu'en cas de risque de dissimulation ou de disparition des données, le juge pourra ordonner, même en référé, toute mesure pour protéger ce droit. Seule une demande manifestement abusive, par sa répétition ou son caractère systématique, pourra permettre au responsable du traitement de ne pas y répondre, sous réserve qu'il apporte la preuve de ce caractère manifeste. Dans le cadre de traitements mis en œuvre aux seules finalités de l'établissement de statistiques, de recherche scientifique ou historique, ces dispositions peuvent être écartées dans les mentions de la demande d'autorisation ou dans les déclarations adressées à la CNIL, mais uniquement lorsque les traitements mis en œuvre excluent manifestement toute atteinte à la vie privée des personnes concernées. Les dispositions entourant la vie privée en droit Français cherchent à donner aux citoyens la maîtrise des informations les concernant.

247. Par la consécration du droit à l'opposition, le législateur a accordé à « *toute personne physique le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement*⁶⁸⁵ ». Seule une obligation légale ou une disposition expresse de l'acte autorisant le traitement peut rendre cette collecte comme étant non susceptible d'opposition. Toute personne pourra refuser, sans avoir à présenter de justification, de donner certaines informations la concernant au moment de la collecte, dans la mesure où ce refus

⁶⁸⁴ Article 39 de la Loi Informatique et Libertés

⁶⁸⁵ Article 38 de la loi Informatique et Libertés

est légitime. Cette légitimité sera appréciée au cas par cas, en fonction de la situation dans laquelle se trouve la personne et de la nécessité juridique de recueillir ses informations. Cette manifestation peut être une simple absence de réponse, ou un refus explicite de signer l'accord écrit obligatoire pour certaines données. Cette maîtrise informationnelle ne s'arrête pas au stade de la collecte. Elle reste attachée aux données. Le citoyen dispose par conséquent d'un droit à l'opposition permanent à l'adresse des traitements basés sur ses données personnelles. Si elle est légitime, cette opposition oblige le responsable de traitement à effectuer la suppression, en prenant toutes mesures de nature à garantir ce droit de manière « *efficace, systématique et immédiate*⁶⁸⁶ ». Le responsable de traitement risque alors jusqu'à cinq ans d'emprisonnement et 300 000€ d'amende s'il continue de procéder au traitement, en application de l'article 226-18-1 du Code Pénal. Il faut préciser également que le sujet du traitement dispose d'un droit de rectification venant compléter le droit à l'opposition. Il peut ainsi exiger du responsable d'un traitement que soient, « *rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel le concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation ou la conservation est interdite*⁶⁸⁷ ». Il pourra demander la preuve des modifications, et de la notification aux tiers lorsque ceux-ci ont eu accès aux informations.

2. La responsabilité liée au traitement et l'obligation de sécurisation

248. Avec l'objectif d'accroître la nécessité de respecter les obligations associées aux traitements de données personnelles, le législateur a créé un régime de sanctions civiles et pénales venant frapper les contrevenants. Le volet pénal est constitué principalement de l'article 226-16 du Code Pénal, qui dispose : « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respecté les formalités préalables à leurs mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000€ d'amende* ». La même peine s'applique au « fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ». De plus, pour éviter tout comportement délétère lors de l'enquête de la CNIL, l'article 51 de la loi du 6 janvier 1978 dispose qu'il « est puni d'un an

⁶⁸⁶ CNIL, Délibération n°2008 - 422 du 6 novembre 2008 portant décision de la formation restreinte à l'égard de la société X, En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000020444356> (dernière consultation: 5 mars 2018)

⁶⁸⁷ Article 40 de la loi Informatique et libertés

d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la Commission Nationale de l'Informatique et des Libertés ».

249. La CNIL assure une mission de veille pour le contrôle des traitements effectués sur le territoire Français. Sa formation restreinte dispose d'un pouvoir d'avertissement et de mise en demeure de faire cesser tout manquement constaté, dans un délai qui peut être ramené à cinq jours en cas d'urgence. Si le responsable de traitement ne se conforme pas à cette mesure, une sanction pécuniaire ne pouvant excéder 150 000€ lors du premier manquement constaté, et 300 000€ lors des suivants constatés dans les cinq années suivantes, sera appliquée. Ces sanctions sont cumulables avec les sanctions pénales évoquées précédemment et représentent donc un fort élément dissuasif, auquel va venir toucher la prochaine réforme de la directive 95/46/CE, en augmentant ces différents montants. Si le responsable de traitement est chargé du contrôle de sa propre activité sur les données, il est également tenu « *de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». La conséquence pénale est sans équivoque : « *le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites [...] est puni de cinq ans d'emprisonnement et de 300 000€ d'amende* ».

250. L'ensemble des droits et obligations issu des dispositions protectrices de la loi informatique et libertés et de la directive de 1995 semble *a priori* pouvoir s'appliquer à la surveillance diffuse. En ce que celle-ci se fonde principalement sur le traitement de données réalisé de manière automatisé, la loi de 78 s'applique. Son champ d'application large confère à la loi Informatique et Libertés une forme d'avance sur le temps technologique. Il permet également de protéger les personnes physiques contre les risques induits par l'informatique sur leur vie privée.

Paragraphe 2: Une protection envisagée en fonction du degré d'intrusivité technologique permettant de couvrir un large panel de situations: l'exemple des technologies biométriques

251. Sans revenir sur la définition du traitement de données à caractère personnel, il est nécessaire d'en préciser l'étendue. Puisque la surveillance diffuse repose essentiellement sur la multiplication de capteurs et d'algorithmes informatiques, il est important, pour caractériser l'applicabilité du régime de protection, de comprendre cette notion. De fait, la distinction entre un

capteur et un système soumis au droit des données personnelles réside dans la capacité à extraire l'information, et dans la nature du programme informatique utilisé. L'analyse du degré d'intrusivité technologique se situe, théoriquement, entre le respect de la neutralité technologique et une approche combinant deux principes fondamentaux de la protection des données personnelles : la finalité et la proportionnalité (A). En réalité, cette approche permet de justifier le choix technologique en fonction d'un usage déterminé. L'exemple des technologies biométriques (B) permet d'illustrer ce propos.

A. Le degré d'intrusivité technologique en théorie

252. Le degré d'intrusivité technologique peut de prime abord rentrer en confrontation avec le principe de neutralité technologique. La polysémie de cette dernière suppose qu'un premier point d'analyse en définisse les contours (1). L'approche combinée de la finalité et de la proportionnalité permet de questionner l'usage technologique et non la technologie (2)

1. La polysémie de la neutralité technologique

253. Dans son ouvrage consacré à la vie privée en péril, Alex Türk évoque la neutralité technologique et écrit que: « *les technologies de l'informatique ne sont ni bonnes ni mauvaises a priori. Il est insensé - comme on l'entend trop souvent - de porter un jugement de valeur à propos de telle ou telle technique, indépendamment du contexte de mise en oeuvre. Seuls les usages qui en sont faits comptent*⁶⁸⁸ ». L'analyse du degré d'intrusivité permet de comprendre de manière effective le contexte de mise en oeuvre technologique. Le principe de neutralité technologique représente dans cette analyse une sorte de garde fou préservant la technologie de tout jugement de valeurs.

254. Bien que sa reconnaissance dans le droit positif soit assez floue, le principe de neutralité technologique est aujourd'hui présenté, ainsi que le rappelle Vincent Gautrais, comme un « *principe fondamental du droit des technologies, sans discussion; en vérité absolue comme « la tarte aux pommes »*⁶⁸⁹ ». Il signifie qu'aucune technologie ne devrait subir de discriminations dans la loi. La loi ne doit pas privilégier l'usage d'une technologie plutôt qu'une autre. Se proposant d'étudier la

⁶⁸⁸ TURK Alex, *La vie privée en péril - Des citoyens sous contrôle*, Op. Cit. p. 20

⁶⁸⁹ GAUTRAIS Vincent, *Neutralité technologique - Rédaction et interprétation des lois face aux changements technologiques*, Les Editions Themis, Montréal, Mai 2012, En ligne: <https://www.gautrais.com/publications/neutralite-technologique/> (dernière consultation: 5 mars 2018)

nature polysémique de la neutralité technologique, Gautrais envisage une triple analyse de la notion. Il déclare que « *d'abord une loi ne réfère pas aux technologies; ensuite une loi ne discrimine pas les technologies et une loi nivèle les effets et les conséquences potentielles des technologies*⁶⁹⁰ ». La neutralité technologique doit se concevoir comme un outil ou comme un résultat à atteindre dans le cadre de la rédaction des lois et de l'interprétation jurisprudentielle⁶⁹¹. Poursuivant son analyse, il écrit ainsi que « *« Outil » versus « censeur ». Deux manières d'envisager le droit, comme le prétendait la professeure Clare Dalton. Deux manières de considérer aussi la neutralité technologique dans la mesure où l'on ne peut traiter de la même manière des champs juridiques qui appréhendent la technologie soit comme un outil, soit comme un domaine à équilibrer*⁶⁹² ». La rédaction de l'article 1er de la loi informatique et libertés est particulièrement éclairante à ce propos. Dire que « *l'informatique doit être au service de chaque citoyen* », c'est avant tout reconnaître ce domaine comme un outil dont l'utilisation ne doit pas être freinée, mais également imposer comme un principe fondamental des nouvelles technologies un équilibre à atteindre entre l'usage des technologies et les droits et libertés des individus.

255. Si ce principe de neutralité technologique n'existait pas lors de l'élaboration de la loi en 1978, il est certain qu'il a fortement inspiré la rédaction de la directive de 1995. S'interrogeant sur l'effectivité de la protection des données issue de la directive de 1995 face aux nouveaux défis technologiques et humain, la Commission européenne déclare: « *les principes essentiels de la directive sont toujours valables et qu'il convient de préserver sa neutralité sous l'angle technologique*⁶⁹³ ». En matière de protection des données personnelles en Europe, il semble même possible d'affirmer que ce principe de neutralité technologique soit envisagé plus particulièrement comme « *un moyen de s'assurer que le droit ne puisse être un empêchement au développement du commerce*⁶⁹⁴ ». Ainsi que le note Vincent Gautrais, il faut alors considérer la neutralité technologique comme « *un facteur de répartition de bénéfices entre des intérêts catégoriels*

⁶⁹⁰ Ibid. p. 32.

⁶⁹¹ Vincent Gautrais écrit: « *Conformément à ce que nous avons pu constater au niveau international, la neutralité technologique se conçoit soit comme un outil, soit comme un résultat. En d'autres termes, elle peut être vue comme un instrument juridique ou comme une finalité d'équivalence vers laquelle tend le législateur. (...). Dans ce que nous qualifions de droit « outil », les dispositions visent principalement à plus d'efficacité ; pour le droit « censeur », c'est plus compliqué. Un rapport de force est généralement présent (...).* ». Ibid. p. 20

⁶⁹² Ibid. p. 21

⁶⁹³ Commission européenne, *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions - Une approche globale de la protection des données à caractère personnel dans l'union européenne*, Op. Cit., p. 3

⁶⁹⁴ GAUTRAIS Vincent, Op. Cit. p. 34

distincts comme c'est par exemple le cas en droit d'auteur (auteur versus utilisateur), en droit de la protection des renseignements personnels (organisation versus individu), en droit de la diffamation (le diffamant de réclamant de la liberté d'expression versus le diffamé de alléguant l'atteinte à sa réputation), et même en droit pénal (protection du public versus protection des droits de l'accusé). Cette distinction n'est pas sans rappeler celle proposée par Clare Dalton quant aux deux fonctions fondamentales du droit: un droit « outil » et un droit « censeur »⁶⁹⁵ ».

2. L'analyse du degré d'intrusivité technologique ou la question des usages technologiques

256. Le Professeur Gautrais voit en la neutralité technologique une sorte de « *boîte à outils permettant de rédiger et d'interpréter des lois*⁶⁹⁶ », qu'il assimile pour partie à la théorie de l'équivalence fonctionnelle⁶⁹⁷, entendue comme l'analyse téléologique guidant l'interprétation et la rédaction des lois. En droit européen et français de la protection des données personnelles, cette dimension du principe de neutralité technologique a contribué fortement à questionner les usages technologiques. L'approche combinée des principes de proportionnalité et de finalité, permettant de jauger du degré d'intrusivité d'une technologie donnée ou d'un traitement donné, en représente l'aboutissement le plus clair.

257. La balance des intérêts en présence, permis par cette approche, est clairement palpable à la lecture de la loi informatique et libertés. Outre le fait de mettre l'informatique au service des individus, son article 1er dispose également que « *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* ». Garantie du développement économique et prise en compte des droits et libertés fondamentaux sont bien les deux intérêts mis en exergue par la loi. Le degré d'intrusivité technologique permet alors une balance entre l'usage technologique et la garantie de protection de la vie privée. Il permet d'évaluer la conformité des usages technologiques avec le cadre légal et protecteur de la vie privée. Pour rappel, la loi impose une feuille de route aux responsables de traitement et aux utilisateurs. Le traitement de données

⁶⁹⁵ GAUTRAIS Vincent, Op. Cit., p. 64

⁶⁹⁶ Ibid. p. 103

⁶⁹⁷ Il écrit ainsi: « *si l'on devait résumer en quelques mots la relation entre neutralité technologique et équivalence fonctionnelle, on pourrait affirmer que la seconde est la cheville ouvrière de la première. Alors que la neutralité technologique est davantage conceptuelle, trop large pour être utilisable dans l'interprétation du droit, l'équivalence fonctionnelle est une « méthode » permettant d'assurer qu'un instrument existant pour le papier puisse être transposé à l'électronique* » (ibid. p. 82).

personnelles doit être envisagé pour des finalités déterminées, explicites et légitimes. Les données collectées doivent être pertinentes, adéquates, non excessives par rapport aux finalités déterminées. Ainsi que le rappelle Alex Türk, « *concrètement, les questions se posent de la manière suivante: (...). Premièrement : quel objectif poursuivez-vous ? Deuxièmement : la solution technique que vous avez retenue pour l'atteindre est-elle adaptée à cet objectif ? On voit ainsi que cette approche finalité/proportionnalité permet de mieux cerner la notion d'usage en couvrant la totalité de l'opération: détermination d'un objectif et d'un choix technologique*⁶⁹⁸ ».

258. Bien que neutre d'un point de vue technologique, le droit à la protection des données personnelles⁶⁹⁹ doit, à l'instar du degré d'intrusivité, ainsi que le rappelle la Commission européenne « *tenir compte des répercussions des nouvelles technologies*⁷⁰⁰ ». Selon la Commission, cela signifie à la fois de « *clarifier et de préciser l'application des principes de la protection des données aux nouvelles technologies, afin de garantir aux personnes une protection réelle et effective des données à caractère personnel les concernant, quelle que soit la technologie utilisée pour traiter ces données, et que les responsables du traitement des données prennent pleinement conscience des répercussions des nouvelles technologies sur la protection des données*⁷⁰¹ ».

B. Le degré d'intrusivité technologique en pratique: l'exemple de la biométrie

259. C'est notamment dans le cadre de la mise en oeuvre de dispositifs biométriques que l'application de la neutralité technologique (2) et de son corollaire le degré d'intrusivité (1) prend tout son sens.

1. Le degré d'intrusivité de la biométrie

⁶⁹⁸ TURK Alex, *La vie privée en péril (...)*, Op. Cit. p. 21.

⁶⁹⁹ Notons ici la position de Vincent Gautrais sur ce point: « *Un autre domaine où la neutralité technologique trouve écho est celui du droit à la protection des renseignements personnels. Ici, l'utilisation qui en est faite est de déclarer que ce domaine du droit, même s'il est sujet à un travail d'adaptation dont on ne sait s'il devrait être de l'ordre de l'évolution ou de la révolution, présente, selon plusieurs, l'avantage d'être neutre sur le plan technologique. Le rapport RAND par exemple, qui n'est pas sans proposer parfois certains bouleversements des concepts pour être en mesure d'intégrer les changements fondamentaux liés notamment aux réseaux sociaux et au «Cloud Computing», se rassure en affirmant qu'heureusement, les lois européennes en vigueur sont techniquement neutres! Lors de consultations relatives à une éventuelle mise à jour de la Loi canadienne sur la protection des renseignements personnels et les documents électroniques il a été plusieurs fois déclaré, parmi les atouts de la loi, qu'heureusement elle était parfaitement neutre sur le plan technologique. Cette neutralité technologique est donc un souhait à suivre* ». Op. Cit. p. 25 - 26.

⁷⁰⁰ Op. Cit. p. 3

⁷⁰¹ Ibid.

260. La biométrie, c'est-à-dire l'identification des personnes à partir de leurs caractéristiques biologiques et morphologiques⁷⁰², est présentée aujourd'hui comme l'une des technologies les plus intéressantes en termes de lutte contre les usurpations d'identités, la criminalité, l'immigration irrégulière. En terme de sécurité, la CNIL voit en la biométrie trois finalités potentiellement admissibles: la protection de l'intégrité physiques des personnes, la protection des biens et des installations⁷⁰³, la protection des informations⁷⁰⁴.

261. En matière de technologies biométriques, et pour caractériser l'applicabilité du régime de protection des données personnelles, il faut d'abord s'intéresser à la notion de capteur. De fait, la distinction entre un capteur et un système soumis au droit des données personnelles réside dans la capacité à extraire l'information, et dans la nature du programme informatique utilisé. Sur le premier point, la CNIL cherche d'abord à identifier si le capteur est en mesure de révéler des caractéristiques physiques de la personne⁷⁰⁵, ou de porter atteinte à sa vie privée en dévoilant certaines informations sur son comportement⁷⁰⁶ selon le caractère intrusif du dispositif. Dans un deuxième temps, il convient de déterminer si l'information, ou la simulation détectée par le capteur est enregistrée ou communiquée selon la définition de l'article 2 de la loi du 6 janvier 1978 modifiée.

262. Cette applicabilité est extrêmement large, car la plupart des systèmes nécessitent une mémoire pour exécuter leurs tâches. En conséquence, le législateur a choisi d'y apporter certaines limites⁷⁰⁷. Malgré son caractère temporaire, l'enregistrement des données personnelles par le capteur peut être soumis au régime protecteur de la vie privée. La distinction issue de la pratique jurisprudentielle s'établit alors sur la capacité d'extraction de cette information. Si un interrupteur automatique à détecteur infrarouge de mouvement peut constituer une immixtion dans la vie privée,

⁷⁰² Empreintes digitales, contour de la main, réseau veineux, iris, voix, traits du visages, ADN...

⁷⁰³ SEVESO, Opérateurs d'importance vitale par exemple

⁷⁰⁴ Par exemple: secret industriel, secret défense. Voir en ce sens: Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, En ligne: <https://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf> (dernière consultation: 5 mars 2018)

⁷⁰⁵ Visage, voix, empreintes,...

⁷⁰⁶ Détecteurs de présence, de toucher, de plaques d'immatriculation, données GPS, ...

⁷⁰⁷ Il existe une exception concernant les copies temporaires, applicable uniquement aux fournisseur de réseaux « dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, [...] à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises ». En restreignant cette exception, le législateur souhaite avant tout protéger le développement des réseaux.

le fait qu'aucune information ne soit enregistrée ni extractible en fait un simple capteur. Si l'information est enregistrée, la CNIL va évaluer le risque pour la personne relativement à la capacité pour l'utilisateur de maîtriser sa donnée, en se référant au cadre de la loi informatique et liberté qui inclut une exception pour les traitements dans le cadre d'activités exclusivement personnelles⁷⁰⁸. Si le stockage s'effectue sur un support individuel, ne pouvant être utilisé pour identifier l'individu à son insu, le capteur et le système associé seront dispensés des autorisations habituelles. Tel est le cas des dispositifs de capture digitale au sein de certains smartphones. L'empreinte étant stockée uniquement sur le terminal et sécurisée par cryptographie, le système entre bien dans la grille d'analyse de la CNIL.

263. L'Autorité administrative évoque un système « d'authentification », dans lequel la donnée biométrique unique contenue dans l'instrument de mesure est comparée à celle présentée par l'utilisateur sur le principe du mode « 1 contre 1 ». Dans ce système, l'identité de l'utilisateur n'est pas indispensablement associée à la donnée biométrique, le caractère intrusif de la technologie s'avère faible (exemple : l'opération qui consisterait à s'assurer de la similitude entre le doigt apposé sur le lecteur et le gabarit stocké sur la carte). Cette méthode est à mettre en opposition à celle dite « d'identification » dans laquelle le dispositif va effectuer une lecture de la donnée présentée par l'utilisateur, et va la comparer à toute celles qui sont stockées dans le système selon le mode « 1 contre N ». Ce système repose nécessairement sur un stockage des données au sein d'un terminal extérieur à celui de l'utilisateur, et implique souvent d'associer la donnée à une identité. Cela révèle le niveau d'intrusion dans la vie privée des personnes concernées par le traitement, générant l'applicabilité du régime de protection des données à caractère personnel et biométrique.

2. Application de la neutralité technologique à la biométrie

264. Ce point technique, nécessaire étant opéré, il importe de comprendre que globalement la CNIL tend à vouloir limiter le recours à la biométrie. Ainsi, elle a pu déclarer, que « *il importe de savoir si le système proposé est bien adapté ou est le mieux adapté à la finalité préalablement définie (...). Il faut rappeler que l'objectif poursuivi par le recours au stockage des empreintes digitales dans une base de données peut presque toujours être atteint par le truchement du système de stockage individualisé sur carte à puce: en l'état actuel de la technique et des informations*

⁷⁰⁸ Voir la Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, Op. Cit.

disponibles, du point de vue de la sécurisation des accès, le dispositif avec base centrale et le dispositif avec support individuel se valent⁷⁰⁹ ». Et d'ajouter que « dans la mesure où il s'agit de situations où l'enjeu de sécurité est majeur, la pertinence, l'adéquation et le caractère non excessif d'un système avec une base d'empreintes digitales doivent aussi être examinés au regard du nombre des personnes concernées: plus la zone est circonscrite et le nombre des personnes concernées réduit, plus les inconvénients d'une base d'empreintes digitales diminuent⁷¹⁰ ».

265. Dans une délibération rendu en 2000, la CNIL a également pu juger que la mise en oeuvre d'un projet de contrôle d'accès biométrique du personnel de l'Académie de Lille ne paraissait pas, au vu de sa finalité d'assurer la fluidité de l'entrée du personnel, « justifier dans sa généralité, la constitution d'une base de données d'empreintes digitales de l'ensemble du personnel de la cité académique⁷¹¹ ». Par ailleurs, s'appuyant sur le respect de la proportionnalité, le juge judiciaire a pu quant à lui interdire la mise en oeuvre d'un système de gestion et de contrôle des temps des salariés d'une entreprise par empreintes digitales en déclarant que: « l'objectif poursuivi n'est pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels travaillant dans les espaces publics des gares de la SNCF, le traitement pris dans son ensemble n'apparaissant ni adapté ni proportionné au but recherché⁷¹² ».

266. L'ensemble de ces exemples et des règles décrites précédemment se réfère globalement à la neutralité technologique entendu par Vincent Gautrais comme permettant une aide à l'interprétation du droit positif⁷¹³, et plus particulièrement au principe de proportionnalité posé par l'article 6 de la loi informatique et libertés qui dispose que les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ». C'est d'ailleurs ce que rappelle les juges de la CEDH dans le cadre de l'arrêt Marper⁷¹⁴

⁷⁰⁹ Ibid. p. 9

⁷¹⁰ Ibid.

⁷¹¹ CNIL, Délibération n° 00-056 du 16 novembre 2000, portant avis sur un projet d'arrêté présenté par le ministre de l'éducation nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès par la reconnaissance des empreintes digitales de certains personnels de l'éducation nationale, pour certains locaux de la cité académique de Lille, En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653132> (dernière consultation: 5 mars 2018)

⁷¹² TGI de Paris, 1ère Chambre, Section sociale, du 19 avril 2005, En ligne: <https://www.cnil.fr/sites/default/files/typo/document/JgfTGIParis19-4-2005Biometrie.pdf> (dernière consultation: 5 mars 2018)

⁷¹³ Le principe de neutralité technologique vu comme participant à une analyse téléologique dans le cadre de l'interprétation des textes de loi.

⁷¹⁴ CEDH (Grande Chambre), Affaire S. et Marper contre Royaume-Uni, Requêtes n° 30562/04 et 30566/04, Strasbourg, 4 décembre 2008, En ligne: <https://rm.coe.int/16806ae19a> (dernière consultation: 5 mars 2018)

par exemple: « *Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (préambule et article 5 de la Convention sur la protection des données et principe 7 de la recommandation R(87)15 du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police). Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (voir notamment l'article 7 de la Convention sur la protection des données). Les considérations qui précèdent valent tout spécialement lorsqu'est en jeu la protection de catégories particulières de données plus sensibles (article 6 de la Convention sur la protection des données), notamment des données ADN, qui, dans la mesure où elles contiennent le patrimoine génétique de la personne, revêtent une grande importance tant pour elle-même que pour sa famille⁷¹⁵ ».*

267. Bien que la loi Informatique et Libertés et la directive de 1995 ont joué un rôle précurseur dans l'appréhension des nouvelles technologies en terme de protection de la vie privée, ces deux textes semblent aujourd'hui souffrir d'un déficit d'effectivité du fait de la surveillance diffuse. Alors qu'il s'interrogeait sur l'évolution possible de la loi de 1978, à l'occasion de la transposition de la directive de 1995, Alex Türk⁷¹⁶ déclarait: « *la France a été l'un des premiers Etats à introduire dans sa législation des dispositions protégeant les personnes physiques contre les risques induits par l'informatique sur leur vie privée⁷¹⁷ »*. Et de poursuivre en indiquant que « *tout d'abord cette menace a été perçue comme susceptible de provenir d'un Etat-Léviathan. La loi du 6 janvier 1978 a donc distingué les traitements publics réputés plus dangereux et les traitements privés bénéficiant d'une présomption d'innocuité. (...). Cette perspective a désormais évolué. Le développement de l'informatique dans les entreprises a conduit à une diversification des risques, encore décuplée par*

⁷¹⁵ CEDH, Marper, Op. Cit. Point 103.

⁷¹⁶ TURK Alex, *Rapport n°218 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif 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*, Op. Cit.

⁷¹⁷ Ibid. p. 11

le développement d'Internet. (...). Entre temps, l'approche normative a évolué, notamment sous l'influence des organisations internationales, conscientes de la valeur marchande de ces données. Elle est ainsi passée de la protection de la vie privée à la promotion de la libre-circulation et de la commercialisation des informations nominatives⁷¹⁸ ». Bien qu'écrit il y a approximativement 15 ans, ces mots sont encore très pertinents et trouvent à la surveillance diffuse. La situation contemporaine est encore partagée entre la menace de l'Etat-Léviathan décrit par Alex Türk et la commercialisation d'informations personnelles, techniques, mais également et surtout d'information non personnelles, de data. Aujourd'hui, la protection des données personnelles se trouvent confrontées à la totalisation numérique et à l'ambition propre à la surveillance d'envisager un panoptique d'un nouveau genre: le data-panoptisme.

Section 2: Un déficit de conscience des enjeux de la surveillance diffuse: l'érection d'un data-panoptisme permis par la totalisation numérique

268. Evoquer le data-panoptisme suppose de comprendre le panoptique de Bentham et l'étude réalisée par Michel Foucault de ce dernier (paragraphe 1). Les conclusions qu'opèrent Foucault concernant la surveillance sont certes d'actualité. Les principaux effets qu'il a dégagé concernant cette notion sont toujours présents dans notre société. Pourtant, elles doivent être enrichies d'un versant numérique. Appréhender la surveillance diffuse comme « un data-panoptisme » permet en effet le constat suivant: la surveillance diffuse permet la collecte de toujours plus de données engendrant ainsi la traçabilité des individus (paragraphe 2).

Paragraphe 1: Le panoptique de Bentham: une grille d'analyse nécessaire pour comprendre le data-panoptisme

269. Evoquer la surveillance diffuse revient souvent à opérer par renvoi à Michel Foucault et à son analyse du Panoptique de Bentham (A). Cette référence permettait jusqu'alors de comprendre la surveillance diffuse comme un dispositif de contrôle. Les études de Foucault et de Deleuze concernant le lien qu'entretient la surveillance et le contrôle social doivent ainsi être activées. Elles représentent en effet des grilles d'analyses nécessaires pour la bonne interprétation de la surveillance. Ainsi que le notait Ariel Kyrou, elles permettent « *d'éclairer les prémices d'une*

⁷¹⁸ Ibid.

*réflexion (...) dans la nuit de nos temps numérisés*⁷¹⁹ ». Elles doivent néanmoins être enrichies pour permettre d'appréhender pleinement la surveillance diffuse. Cette dernière représente la consécration de la totalisation numérique : un data-panoptisme (B).

A. Du panoptique de Bentham...

270. Deux éléments doivent être analysés: le principe d'inspection dégagé par Bentham (1) et l'importance du regard que Foucault (re)met en lumière à travers son étude du Panoptique (2).

1. Le principe d'inspection de Bentham à l'épreuve de la surveillance diffuse

271. « *Si l'on trouvait un moyen de se rendre maître de tout ce qui peut arriver à un certain nombre d'hommes, de disposer tout ce qui les environne, de manière à opérer sur eux l'impression que l'on veut produire, de s'assurer de leurs actions, de leurs liaisons, de toutes les circonstances de leur vie, en sorte que rien ne pût échapper ni contrarier l'effet désiré, on ne peut pas douter qu'un moyen de cette espèce ne fût un instrument très énergique et très utile que les gouvernements pourraient appliquer à différents objets de la plus haute importance* ⁷²⁰ ». C'est par ces mots que le juriste et philosophe de l'utilitarisme, Jérémy Bentham, introduit son *Mémoire sur un nouveau principe pour construire des maisons d'inspection, et nommément des maisons de force*, autrement appelé le Panoptique. La méthode de contrôle pensée par Bentham, redécouvert par Foucault, doit nécessairement être approfondi pour en vérifier sa concordance avec les événements récents.

272. Au-delà de l'édifice architectural repris dans le cadre de l'analyse de Bentham, ce dernier établit avec acuité le principe de fonctionnement de l'économie du regard et de la visibilité. Le questionnement de son analyse est assez simple. Après avoir décrit les prisons de son époque comme des « *séjours infects et horribles, une école de tous les crimes et entassement de toutes les misères*⁷²¹ », l'auteur se demande « *comment établir un nouvel ordre de choses ? Comment s'assurer, en l'établissant, qu'il ne dégènera pas ?*⁷²² ». Il répond à ces interrogations par ces

⁷¹⁹ Op. Cit. p. 115

⁷²⁰ BENTHAM Jérémy, *Panoptique*, Mille et une nuits, département de la librairie Arthème Fayard, Septembre 2002, p. 7

⁷²¹ Op. Cit p. 9

⁷²² Ibid.

mots: « *l'inspection: voilà le principe unique pour établir l'ordre et pour le conserver; mais une inspection d'un genre nouveau, qui frappe l'imagination plutôt que les sens, qui mette des centaines d'hommes dans la dépendance d'un seul, en donnant à ce seul homme une sorte de présence universelle dans l'enceinte de son domaine*⁷²³ ». Et poursuit son analyse en déclarant: « *cette maison de pénitence serait appelée panoptique, pour exprimer d'un seul mot son avantage essentiel, la faculté de voir d'un coup d'oeil tout ce qui s'y passe*⁷²⁴ ». Ce principe d'inspection décrit par Bentham doit donc bien être compris comme une économie du regard et de la visibilité.

273. La surveillance contemporaine, dans sa double dimension (imposée et banale), porte les stigmates de cette économie du regard: l'oeil des caméras installées sur les bâtiments publics ou privés en est le parfait exemple. Toutefois, ce regard est d'un genre nouveau: il scrute, analyse les comportements des individus, leurs informations non plus pour « *assurer à un seul homme une sorte de présence* » pour reprendre les termes du juriste anglais, mais bien pour élaborer une sorte de prédiction. Cette prédiction s'assimile alors beaucoup plus à une sorte de voyance qu'à une tyrannie de la visibilité. Enfin, la surveillance contemporaine frappe toujours « *l'imagination plutôt que les sens* », mais là encore une actualisation de ces propos est nécessaire. Pour plus de clarté, il faudrait écrire plutôt, qu'elle frappe l'imaginaire plutôt que les sens. La surveillance contemporaine s'exerce sur des individus conscientisés, qui n'hésitent pas à arguer du fait de n'avoir rien à cacher, rien à se reprocher, pour se placer d'eux-mêmes dans le champ d'observation de la surveillance. Ainsi, le sentiment conscient, voire anxieux de visibilité semble avoir fait place à une forme de consentement à la surveillance, ou à tout le moins, à une acceptation.

2. L'importance du regard dans l'étude du panoptique par Foucault

274. Lorsque Foucault redécouvre le panoptique, il reprend l'analyse de Bentham quant à son principe d'inspection. Il décrit alors « *l'effet majeur du Panoptique : induire chez le détenu un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir. Faire que la surveillance soit permanente dans ses effets, même si elle est discontinuée dans son action ; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice [...] Bentham a posé le principe que le pouvoir devait être visible et invérifiable. Visible : sans cesse le détenu aura devant les yeux la haute silhouette de la tour centrale d'où il est épié. Invérifiable : le détenu ne doit jamais*

⁷²³ Ibid.

⁷²⁴ Ibid. p. 11

*savoir s'il est actuellement regardé ; mais il doit être sûr qu'il peut toujours l'être*⁷²⁵ ».

275. La surveillance contemporaine se fonde sur ces éléments et emporte des conséquences similaires. On ne peut, en effet, qu'être en accord, avec l'idée de Foucault selon laquelle le pouvoir s'exerce de façon automatique. Il voit, il contrôle, il maîtrise, il établit des prévisions, et conditionne, de manière sans cesse renouvelée, à l'acceptation de la surveillance. Elle est, comme le souligne Foucault, permanente dans ses effets. Les mémoires des outils informatiques rendent cette caractéristique endémique de la surveillance, puisque quasiment irréversible. Bien qu'il soit possible, de nos jours, d'arguer d'un droit à l'oubli pour obtenir le retrait de certaines informations contenu sur des sites internet, ce droit n'est en rien une garantie d'effacement des données personnelles ou des informations concernant un individu des serveurs d'une entreprise. Il s'agit d'un droit au déréférencement, ou d'un droit à l'effacement d'une mention publiée sur un site. Ainsi, l'information apparaît toujours dans les serveurs d'une entreprise. D'où le constat suivant: la surveillance contemporaine tend à être encore plus invérifiable qu'à l'époque des prisons de Bentham. Bien que les données collectées en Europe doivent répondre à une finalité précise, la quantité d'informations que nous laissons via les outils numériques ne permettent plus réellement de connaître clairement des finalités correspondantes, et des possibles détournements de finalités.

276. Néanmoins, l'analyse de Foucault quant à la visibilité du pouvoir et son assimilation à « *la haute silhouette de la tour centrale* » appelle quelques éléments de précisions et de nuances. Cette haute silhouette n'est plus d'actualité aujourd'hui. Elle a été remplacée par les technologies de l'information, de la communication et de la sécurité. Ainsi, le pouvoir décrit par Foucault n'est plus seulement cet « *oeil du gouvernement incessamment ouvert et veillant indistinctement sur tous les citoyens sans pour cela les soumettre à aucune mesure de coercition quelconque*⁷²⁶ ». Et c'est à travers la lecture de l'ensemble de son oeuvre que l'on comprend que le pouvoir de contrôle ne s'exerce pas exclusivement par un gouvernement, ou une classe sociale dominante. Le pouvoir ne doit pas être entendu comme le titulaire légitime de ce dernier. Pour rappel, la surveillance contemporaine est permise par la convergence des intérêts du secteur public et du secteur privé, mais également par la fascination de l'individu envers les technologies du numérique.

⁷²⁵ FOUCAULT Michel, *Surveiller et punir - Naissance de la prison*, Op. Cit., p. 360 - 361

⁷²⁶ Ibid. p. 503. Ici Foucault décrit la surveillance générale de la population en ces termes: « *Surveillance générale de la population, vigilance muette, mystérieuse, inaperçue... C'est l'oeil du gouvernement incessamment ouvert et veillant indistinctement sur tous les citoyens sans pour cela les soumettre à aucune mesure de coercition quelconque...* ».

277. De fait, la surveillance contemporaine établit ses fondations des analyses du Panoptique de Bentham, reprise par Foucault. Elle est, d'une part, la consécration d'un principe de visibilité devenue aujourd'hui intégrale. Elle représente, d'autre part, l'aboutissement des méthodes de contrôle du panoptique. Mais, elle se détache également de ces analyses. Elle les surpasse au plus haut degré en ce qu'elle est de plus en plus invérifiable, et amasse une quantité d'informations sur les individus qui les rend traçable. Qui plus est elle tend à réduire l'individu à sa trace numérique, qui peut devenir sa principale ressource économique et de pouvoir. Bentham et Foucault ont ainsi posé les bases d'une méthode de contrôle social nouvelle; les technologies de l'information et de la communication ont affiné ces éléments pour rendre la surveillance diffuse invisible dans ses effets et ses conséquences pour les libertés individuelles.

B. ... Au Data-panoptisme: totalisation numérique et datafication de la vie même

278. Le Data-panoptisme prôné par la surveillance diffuse doit avant tout être analysé à la lumière des analyses de Deleuze concernant les sociétés de contrôle. Dès la fin des années 1980, ce dernier présentait déjà l'apparition d'un data-panoptisme lorsqu'il rapprochait la notion même d'information au système contrôle (1). Son étude doit être enrichie par l'étude de la situation actuelle dominée par la totalisation numérique et la datafication de la vie même (2).

1. L'information: un système de contrôle selon Deleuze

279. Lorsque Gilles Deleuze écrit son post-scriptum sur les sociétés de contrôle⁷²⁷, l'informatique débute sa diffusion massive avec, entre autre, l'ère du Personal Computer. Nulle question à cette époque de traitement généralisé de données, nul phénomène d'interconnexion généralisé des bases de données, de géolocalisation, de vidéosurveillance, de vidéoprotection, d'analyses comportementales, ou encore d'analyses prédictives. Pourtant, dès 1990, Deleuze écrit: « *dans les sociétés de contrôle, au contraire, l'essentiel n'est plus une signature ni un nombre, mais un chiffre: le chiffre est un mot de passe, tandis que les sociétés disciplinaires sont réglées par des mots d'ordre (aussi bien du point de vue de l'intégration que de la résistance). Le langage numérique du contrôle est fait de chiffres, qui marquent l'accès à l'information, ou le rejet. (...). L'homme des disciplines était un producteur discontinu d'énergie, mais l'homme du contrôle est plutôt*

⁷²⁷ DELEUZE Gilles, « Post-scriptum sur les sociétés de contrôle », in. *L'autre journal* n° 1, mai 1990

*ondulatoire, mis en orbite, sur faisceau continu. Partout le surf a déjà remplacé les vieux sports*⁷²⁸ ». Ces conclusions sont d'ordre quasi-prophétiques. La société de contrôle aidée par l'informatique devient une société numérique du contrôle. Cette dernière dispose effectivement de son propre langage - le langage numérique. Les données collectées, les masses de données, sont stockées dans des bases de données, dans des usines à données que nous remplissons consciemment ou non, quotidiennement, gratuitement, continuellement et quasi-volontairement. Le surf, comme le notait Deleuze, a remplacé les vieux sports, et plus loin l'internet des objets, le big data, ou encore les pratiques de quantified self ont remplacé des activités permettant un rapport aux autres. Qu'il s'agisse de la santé, du marketing, de notre vie sociale, aucune activité n'est épargnée par le langage numérique, l'ambition à la collecte de données et à la production d'informations.

280. Dans ses analyses, Deleuze rapproche très tôt l'information au système de contrôle en déclarant que : « *on pourrait dire que la communication, c'est la transmission et la propagation d'une information. Or une information, c'est quoi ? C'est pas très compliqué, tout le monde le sait : une information, c'est un ensemble de mots d'ordre. Quand on vous informe, on vous dit ce que vous êtes sensés devoir croire. En d'autres termes : informer c'est faire circuler un mot d'ordre. Les déclarations de police sont dites, à juste titre, des communiqués; on nous communique de l'information, c'est à dire, on nous dit ce que nous sommes censés être en état ou devoir croire, ce que nous sommes tenus de croire. Ou même pas de croire, mais de faire comme si l'on croyait, on ne nous demande pas de croire, on nous demande de nous comporter comme si nous le croyions. C'est ça l'information, la communication, et, indépendamment de ces mots d'ordre, et de la transmission de ces mots d'ordre, il n'y a pas de communication, il n'y a pas d'information. Ce qui revient à dire : que l'information, c'est exactement le système du contrôle*⁷²⁹ ». L'information - système de contrôle - est produite par l'individu, collectée par les entreprises et l'Etat. Cette donnée collectée est aujourd'hui devenue la matière essentielle d'un marché économique, mais également la matière du contrôle. En 1990, Deleuze souligne aussi ce propos, lorsque citant Guattari il écrit: « *il n'y a pas besoin de science-fiction pour concevoir un mécanisme de contrôle qui donne à chaque instant la position d'un élément en milieu ouvert, animal dans une réserve, homme dans une entreprise (collier électronique). Félix Guattari imaginait une ville où chacun pouvait quitter son appartement, sa rue, son quartier, grâce à sa carte électronique (dividuelle) qui faisait lever telle ou*

⁷²⁸ DELEUZE Gilles, Op. Cit., p 4 - 5.

⁷²⁹ DELEUZE Gilles, *Qu'est ce que l'acte de création ?*, Conférence donnée dans le cadre des mardis de la fondation Femis, 17 mai 1987, En ligne: <https://www.webdeleuze.com/textes/134> (dernière consultation: 5 mars 2018)

*telle barrière; mais aussi bien la carte pouvait être recrachée tel jour, ou entre telles heures; ce qui compte n'est pas la barrière, mais l'ordinateur qui repère la position de chacun, licite ou illicite, et opère une modulation universelle*⁷³⁰ ». Quelques trente années plus tard, la Smart City réalise la prophétie de Guattari, les colliers électroniques de Deleuze sont parfaitement représentés par les smartphones, les montres connectées, les réseaux sociaux qui alimentent de manière permanente et implacable les bases de données et data-center d'entreprises du secteur privé.

281. Ces premiers éléments d'analyse ne sont pas sans rappeler les mots de Bernard Stiegler lorsqu'il décrivait la « *société computationnelle devenant automatique*⁷³¹ ». Poursuivant l'analyse de Deleuze, Stiegler démontre le nouveau paradigme à l'oeuvre et évoque le passage « *des sociétés de contrôle à l'automatisation intégrale*⁷³² ». Il écrit ainsi que: « *dans la société automatique que Deleuze n'a pas connue, mais qu'il a anticipée avec Félix Guattari, en particulier lorsqu'ils parlèrent de individuels, le contrôle passe par la liquidation machiniste du discernement (...). Deleuze envisage dans un dialogue avec Serge Daney que l'époque des sociétés de contrôle puisse donner naissance à un « art du contrôle » (...). Un « art de l'hypercontrôle » serait-il semblablement concevable dans l'économie de la traçabilité ? (...). La société automatique de l'hypercontrôle est la société fondée sur l'exploitation industrielle, systémique et systématique des rétentions tertiaires numérique par où tous les comportements sont générateurs de traces et toutes les traces sont devenues des objets de calculs - d'Angela Merkel au « clodo du coin »*⁷³³ ».

2. Le data-panoptisme ou la mise en données du monde pour un contrôle social invisible et invérifiable

282. Bien que l'analyse de Sadin dans ses différents ouvrages s'assimile souvent à la re-

⁷³⁰ DELEUZE Gilles, Op. Cit., p. 6

⁷³¹ Op. Cit.

⁷³² STIEGLER Bernard, Op. Cit., p. 78 et suivants

⁷³³ Ibid. p. 79 - 80 Les rétentions tertiaires qu'évoquent Stiegler doivent être comprises comme « *les traces numériques, analogiques et mécaniques* », donc, toutes informations, données personnelle ou non.

formulation de concept empirique⁷³⁴, cette dernière a d'une part le mérite de dénoncer la normalisation d'un régime pourtant historiquement spécial qu'est la surveillance contemporaine. D'autre part, cette actualisation de la figure du panoptique liée à la surveillance diffuse, le « Data-panoptisme », reflète parfaitement de la réalité de la situation contemporaine.

283. Le principe de visibilité, que la surveillance diffuse porte en son sein, est devenu invisible et invérifiable du fait de la manipulation d'un ensemble de données personnelles ou non. Aussi, et bien que Sadin procède par renvoi et actualisation de la pensée de Jacques Ellul concernant la technique et le progrès, le concept de « *totalisation numérique* » décrite par Eric Sadin en 2015 rend compte de l'évolution de la surveillance diffuse poussée par les objectifs du marché du numérique et l'idéologie de la sécurité. Dans ses trois ouvrages de référence, Ellul a défini la technique comme la recherche du moyen le plus efficace dans tous les domaines, et en a tiré la conclusion que: la technique est l'enjeu du siècle. Ces mots devraient être complétés aujourd'hui car c'est bien le produit de la technique, c'est-à-dire la donnée, l'information, la data qui devient l'enjeu du siècle de la surveillance diffuse. Par la numérisation de toutes formes de signal intentionnel ou non, individuel ou collectif, plus globalement par l'échantillonnage⁷³⁵ des activités humaines, la surveillance diffuse développe, en les enrichissant, les figures utopiques du progrès. Ainsi que le soulignait Ellul à l'égard de la Technique, elle contribue alors à neutraliser toute forme de frein⁷³⁶ au progrès, à la numérisation. Ellul a également dénoncé l'omniprésence des techniques industrielles, informationnelles, économiques et politiques, qui a permis au pouvoir de rationaliser son action, ainsi que de la rendre acceptable. La mobilisation de la technique par le pouvoir

⁷³⁴ Cf. un article de Thibault Le Texier concernant la lecture croisée des trois ouvrages de Sadin. Le Texier écrit: « *la prémonition de cette nouvelle condition humaine et de son milieu entièrement artificiel et de plus en plus numérisé ne manque pas d'intérêt et sonne souvent juste.(...).* Toutefois, pour intellectuellement stimulants et séduisants qu'ils soient, ces trois essais sur les sociétés de contrôle à l'heure du numérique posent plusieurs problèmes. pour le dire d'un mot, leur auteur privilégie souvent la prédiction et le concept dropping à l'analyse empirique et à la théorisation ». in. LE TEXIER Thibault, « Éric Sadin et le coup d'État technologique permanent », *Quaderni*, 86, Hiver 2014-2015, En ligne: <http://journals.openedition.org/quaderni/868>, p.80 (dernière consultation: 5 mars 2018). Nous rejoignons les conclusions de Le Texier: qu'il s'agisse de son étude concernant la datafication - qui correspond ni plus ni moins au phénomène de mise en données du monde décrit par nombre d'auteurs dont Emmanuel Kessous -, de son unique paragraphe concernant la « gamification de l'existence » - qui reprend des théories de l'application des principes du jeu à la vie quotidienne tel que décrit par François Ost par exemple -, ou encore de son invocation de la totalisation numérique - où Sadin n'opère que peu de référence à Jacques Ellul (mis à part dans son introduction générale).

⁷³⁵ En informatique l'échantillonnage est le procédé de transformation d'un signal analogique en valeurs numériques.

⁷³⁶ C'est ce que Ellul entendait par l'automatisme du choix technique, l'auto-accroissement de la Technique, mais également par ce qu'il « voyait » dans le « *terrorisme feutré de la technologie* ». A partir du moment où le choix de l'individu s'oriente vers le choix technique, du progrès, il y aurait une forme de neutralité de l'acte de décision, plaçant l'individu dans une « *situation de double dépendance irréversible, si bien qu'il est subjugué* » face à la technique. « *Tout ce discours terroriste se fonde sur la représentation de la société de demain* » écrivait Ellul. Ces mêmes mots pourraient entièrement trouver application à la société contemporaine, si dominée par les objets connectés, la sécurité et le marché économique de la donnée, que l'individu ne questionne plus l'idéologie de la surveillance qui se joue en trame de fond. (ELLUL Jacques, *Le bluff technologique*, Op. Cit., p. 685 - 686)

(économique, politique, juridique et réglementaire) possède une ambivalence dans ses effets. D'une part, elle est un facteur décisif d'une forme d'amélioration des conditions de vie des individus; d'autre part elle est un moyen de domination du pouvoir, qui s'introduit dans la sphère privée et publique des individus. Selon l'auteur, la technique est alors totalisante et porte en son sein un totalitarisme technologique⁷³⁷. Plus la société s'organise autour de la technique et du progrès, moins les individus ont de pouvoirs et de libertés. A la suite de Jacques Ellul, Eric Sadin décrit le processus de totalisation numérique à la lumière de cinq éléments: « *la puissance rationalisante des nombres*⁷³⁸ », « *l'ère des capteurs*⁷³⁹ », « *l'interopérabilité universelle, la perception intégrale de la vie*⁷⁴⁰ », « *la datafication*⁷⁴¹ *et la dimension performative des data*⁷⁴² ».

284. Mise en données du monde par des capteurs de plus en plus nombreux qui numérisent, analysent et décryptent les activités humaines; perception et prédiction par le nombre, par l'information et la donnée; rapport quantitatif voire qualitatif au réel, menant à une rationalisation maximale de l'ensemble de la vie en société: voilà ce qu'est, selon Sadin, la totalisation numérique.

⁷³⁷ Ellul écrit: « *A l'époque de l'ordinateur et de la synthèse des sciences de l'homme qui débute, il ne peut plus être question de fascisme: celui-ci paraît merveilleusement démodé (...). Mais la dictature technicienne abstraite et bienfaitrice sera beaucoup plus totalitaire que les précédentes. (...). Cette totalisation de la Technique (...) recouvre en fait tous les éléments composant le corps social et que progressivement toutes les expressions de la vie humaine deviennent techniques: ceci veut dire que la technique a, envers la société et l'existence humaine, un double effet (...). C'est non pas la subordination de l'homme à la technique, etc, mais bien plus profondément une nouvelle totalité qui se constitue* ». (in. ELLUL Jacques, *Le système technicien*, Op. Cit., p. 210 - 211). N'est-ce pas là ce qui caractérise le mieux la situation actuelle - « *une totalisation qui produit une véritable intégration de tous les facteurs humains, sociaux, économiques, politiques* » ? La « *dictature technicienne abstraite et bienfaitrice* » et le « *terrorisme feutré de la technologie* » ne sont-ils pas des phénomènes amplifiés par la surveillance diffuse, la numérisation de la vie des individus ? Par ses motivations, ses rationalités fondées sur la sécurité et le marché du numérique, la surveillance diffuse « *abstraite et bienfaitrice* » ne recouvre-t-elle pas un sens totalisant et totalitaire ?

⁷³⁸ SADIN Eric, *La vie algorithmique*, Op. cit., p. 45 - 50. « *Le principe de numération témoigne dès son origine de la volonté d'entretenir un rapport quantitatif au réel* » (p. 45). Et d'ajouter: « *mouvement graduel de numérisation qui s'est accru ou radicalisé depuis le début du nouveau millénaire* » (p. 50).

⁷³⁹ Pour Sadin, « *notre période est caractérisée par un mouvement massif d'incorporation de capteurs au sein de surfaces toujours plus étendues du réel* ». Ibid. p. 51. Plus globalement, voir p. 51 à 55.

⁷⁴⁰ Selon l'auteur, « *le processus historique de numérisation progressive à visée désormais intégrale a institué un régime d'interopérabilité universelle* ». Ibid. p. 56, et plus globalement voir, p. 56 à 58

⁷⁴¹ Qu'il définit comme suit: « *Désormais, chaque événement peut être capté en tant que tel et témoigner de sa qualité propre, autant qu'être virtuellement mis en lien avec tout autre. C'est cela la mise en données du monde, sa datafication, ne s'éprouvant plus comme un horizon infini de faits épars, mais comme un registre intarissable d'équations évolutives, exposant ou révélant en temps réel l'état général et singulier des choses grâce à la réduction numérique universelle relayée par la puissance de systèmes corrélatifs et d'algorithmes interprétatifs.* ». Ibid. p. 58 - 59

⁷⁴² Sadin évoque ici la temporalité de la vie algorithmique: « *Tableaux perpétuellement dynamiques de la réalité qui ne revêtent pas une seule dimension informationnelle, mais qui opèrent des effets de rétroaction sur les gestes, peu à peu délivrés de l'imprécision ou du « bruit » jusque-là tenus comme consubstantiels à l'expérience. C'est une « compression » dans le processus de la décision qui se constitue, se déterminant suivant des délais toujours plus resserrés Le sursis se réduit entre une perception toujours plus informée et les modes d'agissement en retour. Récente rythmique qui correspond à une nouvelle forme d'efficacité en acte établie sur la dissolution progressive de toute latence, conduisant à un surcroît d'économie rationnelle du temps. C'est la notion de « temps réel » qui subit une modification* ». Ibid. p. 62 (et, pour aller plus loin, voir p. 62 à 65).

Cette dernière reprend bien les traits de la totalisation technique, et la surpasse par la notion même de donnée. Ainsi que Jacques Ellul le notait à propos de la technique : « *cette société, cet homme (...) reçoivent désormais leur unité de la technique totalisante. Mais celle-ci ne peut donner un sens: c'est sa grande lacune. La totalité reconstituée est vide de signification*⁷⁴³ ». Reprenant les traits de la totalisation numérique et fonctionnant sur la mise en donnée du monde et l'analyse, la perception, la prévision du présent et du moment à venir, la surveillance diffuse donne quant à elle une signification, ou du moins, l'illusion d'une signification. Cette illusion de signification est parfaitement illustrée par Eric Sadin lorsqu'il conclut: « *les flux de code ne se situent plus seulement après les choses, mais structurent et conditionnent de part en part notre rapport au réel. C'est cela qu'aura produit in fine le mouvement historique de numérisation, non pas un strict équivalent chiffré, mais l'avènement d'une nouvelle anthropologie déterminée, guidée, « drivée » par des logiques littéralement binaires, qui ordonnent sans ambiguïté ou sous une rationalité apodictique la marche de plus en plus globale du monde*⁷⁴⁴ ». Cette conclusion pousse l'auteur à voir en la vie algorithmique une sorte de « *panopticum électronique*⁷⁴⁵ », et plus précisément, à détecter le passage du « *régime de la surveillance numérique qui aura caractérisé les années 1995 - 2015, à un DATA -PANOPTISME, non pas détenu par quelques figures omnipotentes, la NSA ou d'autres entités, mais entretenu et exploité de partout, avec pour objectif prioritaire d'offrir des services et d'assurer le plus grand « confort de tous »*⁷⁴⁶ ».

Paragraphe 2: Le data-panoptisme et l'injonction de transparence pesant sur les individus

285. « *Comment un homme seul peut-il suffire à veiller parfaitement sur un grand nombre d'individus? Comment même un grand nombre d'individus pourrait-il veiller parfaitement sur un seul ? (...). On conviendra donc facilement qu'une idée aussi utile que neuve, serait celle qui donnerait à un seul homme un pouvoir de surveillance qui, jusqu'à présent, a surpassé les forces réunies d'un grand nombre*⁷⁴⁷ ». Ces interrogations contenues dès les premières pages du panoptique de Bentham sont également au centre des préoccupations des études concernant la surveillance contemporaine. La surveillance diffuse, dans sa double nature (imposée et banale),

⁷⁴³ Op. Cit.

⁷⁴⁴ SADIN Eric, *La vie algorithmique - Critique de la raison numérique*, Op. Cit. p. 65.

⁷⁴⁵ Ibid. p. 50

⁷⁴⁶ Ibid. p. 169 (Voir également p. 165 à 190).

⁷⁴⁷ Ibid. p.7 - 8

n'est en aucun cas exercé par un seul homme sur un grand nombre. La surveillance diffuse n'implique généralement pas des personnes incarnées qui exerceraient une sorte de veille sur d'autres. La surveillance actuelle cherche plutôt à obtenir des fragments de vie, des informations abstraites, des faits sur les individus, ou comme l'écrivait Ariel Kyrou: « *le suivi de nos traces digitales et le calcul de nos probabilités d'actions*⁷⁴⁸ ».

286. S'il est vrai que la surveillance diffuse permet la traçabilité des activités humaines et la réduction des individus à une sorte de trace numérique (A), il semble également qu'il faille enrichir le principe d'inspection de Bentham. La surveillance diffuse impose, par le data-panoptisme et la traçabilité des activités humaines, une véritable injonction de transparence aux individus (B).

A. De la traçabilité des activités humaines au suivi de nos traces digitales...

287. Confrontée à la surveillance diffuse, la reconnaissance de la notion de traçabilité, de son utilisation dans le langage juridique, n'est pas anodine, et ce, d'autant plus que cette notion technique n'a pas de définition juridique précise. Elle soulève également des interrogations tant au titre de la protection offerte par le droit des données personnelles, qu'au titre de la protection de la vie privée. La surveillance diffuse réduit aujourd'hui l'individu à une trace numérique (1). L'évocation des concepts de traces et de traçabilité permettent également d'actualiser les principes dégagés par Bentham et Foucault. Le principe d'inspection et l'importance du regard dégagés par ces deux auteurs obtiennent de nos jours une teinte sécuritaire du fait même de la reconnaissance dans le droit positif de la traçabilité. Sa force juridique est en effet liée au principe de précaution (2) permettant de prévenir des risques et menaces dans la société humaine.

1. De la traçabilité de l'individu et de sa réduction à une trace numérique...

288. C'est avec la fin du 20ème siècle que le concept de traçabilité a émergé. Il s'est développé en France et en Europe à la suite des crises du sang contaminé, de la vache folle et des premières études liées aux organismes génétiquement modifiés. Son développement a touché l'ensemble des activités humaines : agro-alimentaire, santé, télécommunications, informatique, travail, vente, envois postaux ; et a profité des avancées techniques majeures de ces dernières années dans le

⁷⁴⁸ Op. Cit.

domaine de l'informatique : entre miniaturisation de l'informatique (codes-barres, puces RFID, nanotechnologies...) et augmentation des mémoires informatiques (bases de données, interconnexion). Au niveau juridique, ce vocable se rencontre d'abord en droit européen à travers plusieurs règlements et décisions de la Commission européenne liés à la sécurité alimentaire⁷⁴⁹ ; puis en droit interne, dans la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles⁷⁵⁰, ou encore dans la loi d'orientation agricole du 9 juillet 1999⁷⁵¹. Par la suite, de nombreuses décisions jurisprudentielles des juridictions administratives et civiles évoquent la traçabilité en droit interne⁷⁵². Progressivement, la notion de traçabilité a touché l'ensemble des pans du Droit, qu'il soit public ou privé, passant par le droit du numérique au droit de la santé, du droit pénal au droit civil, du droit du travail au droit des contrats et marchés publics.

⁷⁴⁹ Règlement (CE) n°1760/2000 du Parlement européen et du Conseil du 17 juillet 2000 *établissant un système d'identification et d'enregistrement des bovins et concernant l'étiquetage de la viande bovine et des produits à base de viande bovine et abrogeant le règlement (CE) n° 820/97 du Conseil*, JOCE 11 août 2000, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32000R1760&from=FR> (dernière consultation: 5 mars 2018); ou encore, Commission des Communautés Européennes, COM (1999) 719 final, Livre blanc sur la sécurité alimentaire, 12 janvier 2000, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:51999DC0719&from=FR> (dernière consultation: 5 mars 2018)

⁷⁵⁰ Loi 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, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000556901&dateTexte=19980618> (dernière consultation: 5 mars 2018). Le titre XIX de cette loi fait mention de la création du « *fichier national automatisé destiné à centraliser les traces génétiques ainsi que les empreintes génétiques* » (FNAEG).

⁷⁵¹ Loi n°99-574 du 9 juillet 1999 d'orientation agricole, JORF n°158 du 10 juillet 1999, p. 10231, texte n°1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000395813> (dernière consultation: 5 mars 2018). L'article 59 de cette loi évoque clairement la notion de traçabilité, plus précisément, sa mise en œuvre.

⁷⁵² On peut notamment citer le premier arrêt rendu par le Conseil d'État mentionnant la traçabilité : Conseil d'État, 29 décembre 1999, n° 206945, Publié au recueil Lebon (absence de traçabilité de produits de consommation importés), En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000007996586> (dernière consultation: 5 mars 2018); ainsi qu'un arrêt plus récent, Conseil d'État, 16 mars 2015, n° 370072, Société Gatpharm, Inédit au recueil Lebon, (concernant la traçabilité des médicaments), En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000030642893> (dernière consultation: 5 mars 2018). Et, pour les juridictions civiles : Cass. Crim., 7 avril 1999, n° de pourvoi: 98-83770, Publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007070450> (dernière consultation: 5 mars 2018); ou plus récemment, Cass. Crim., 17 mai 2011, n° de pourvoi: 10-87646, Non publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000024252814> (dernière consultation: 5 mars 2018). Ces deux arrêts concernent la justification de la traçabilité de produits de consommation chez des commerçants et dans un hypermarché par le non-respect de normes de sécurité essentielles. Enfin, au niveau européen, Voir: CJCE, Affaire C-1/00, Arrêt de la Cour du 13 décembre 2001, Commission des communautés européennes contre République française, Recueil de la jurisprudence 2001 I-09989, Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/showPdf.jsf?jsessionid=9ea7d2dc30dd84f84dc8e3b64819a74cddb69833368e.e34KaxiLc3qMb40Rch0SaxyNaNn0?text=&docid=46950&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=66877> (dernière consultation: 5 mars 2018). La Cour condamne la France pour avoir refusé de lever l'embargo sur les importations de viandes bovines britanniques tout en soulignant l'importance d'un système de traçabilité fiable pour la protection de la santé publique.

289. Définie dans le domaine industriel, par une première norme ISO⁷⁵³ en 1994 comme la « *possibilité à retrouver l'historique, l'utilisation ou la localisation d'une entité au moyen d'identifications enregistrées*⁷⁵⁴ », la traçabilité est venue progressivement, au travers du contrôle social et des outils de surveillance, s'appliquer à l'individu. A travers cette définition, il est possible d'esquisser une explication de la notion de traçabilité. Elle doit s'analyser comme un ensemble de techniques mises en œuvre afin de prévenir et de limiter les risques tout en garantissant la qualité des produits de leurs origines à leurs destructions et, par là, leurs flux de circulation. Il s'agit alors de codifier, archiver, collecter, surveiller les origines et le devenir des produits. En suivant un bien de sa fabrication à sa destruction, en passant par sa distribution et son utilisation, on peut alors détecter des failles, des risques potentiels et y remédier. On comprend ici l'efficacité de ce procédé technique et la dangerosité de son application à l'individu, tant en termes de protection de sa vie privée, qu'en termes de protection des données à caractère personnel.

290. L'une des premières évocations de la trace, de la traçabilité, de son importance au niveau juridique, et de son application à l'individu remonte au 18^{ème} siècle. Jean-Guillaume Locré de Roissy écrit ainsi que « *si tous les hommes étaient justes et sincères, on n'aurait pas besoin sans doute de tant de règles. Mais outre que l'expérience n'a que trop appris tout ce que l'on doit redouter du vice ou de la faiblesse, ce qui seul justifierait les mesures que la loi prend pour constater les conventions, nous devons aussi reconnaître que les hommes se succédant sur la terre et les obligations se transmettant d'âge en âge, il est indispensable de fixer les formes qui seules peuvent faire retrouver les traces des obligations et des preuves de la libération*⁷⁵⁵ ». A travers cette citation, on comprend tout l'enjeu de l'application de cette notion, de ces implications en Droit. La traçabilité répond à une recherche de sécurité, et correspond au rejet de tout aléa possible. Elle

⁷⁵³ Norme ISO 8402, en 1994, En ligne: http://www.iso.org/iso/fr/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=29280 (dernière consultation: 5 mars 2018). Cette norme n'a eu de cesse d'évoluer depuis puisqu'elle a été remplacée par la norme ISO 9000:2000, puis la norme ISO:9000:2005, et enfin la norme ISO 9000:2015 qui spécifie les termes et définitions s'appliquant à toutes les normes relatives au management de la qualité et aux systèmes de managements de la qualité élaboré par l'ISO / TC 176, voir: <https://www.iso.org/fr/standard/45481.html> (dernière consultation: 5 mars 2018)

⁷⁵⁴ Des notes apparaissent à la suite de cette définition. « *1. Le terme traçabilité peut être utilisé dans trois acceptions principales : a) lorsqu'il se rapporte à un produit, le terme peut se référer à l'origine des matériaux et des pièces, l'historique des processus appliqués au produit, la distribution et l'emplacement du produit après livraison ; b) lorsqu'il se rapporte à l'étalonnage, il s'applique au raccordement des équipements de mesure aux étalons nationaux ou internationaux, aux étalons primaires, aux constantes et propriétés physiques de base ou matériaux de référence ; c) lorsqu'il se rapporte à la collecte de données, il relie les calculs et les données générales tout au long de la boucle de qualité, en remontant parfois aux exigences pour la qualité pour une entité. 2. Il convient que tous les aspects concernant les éventuelles exigences de traçabilité soient clairement spécifiés, par exemple en termes de période couverte, point d'origine ou identification.* »

⁷⁵⁵ in. GAUTIER Pierre-Yves, LINANT DE BELLEFONDS Xavier, *De l'écrit électronique et des signatures qui s'y attachent*, JCP éd. G 2000, I, n°236, v. n°31 ; Locré, t. XII, p.505

correspond par là à ce que les technophobes envisageaient sous couvert de l'expression de « recherche d'efficacité » que permet la technologie. Appliquée à l'individu, la volonté de réduire ce dernier à une trace numérique est permise grâce à la datafication, à la totalisation numérique, mais également à la croyance en la toute puissance libératrice des technologies. La traçabilité correspond en réalité à l'effet réel produit par le solutionnisme technologique que prône nos société.

291. Le concept de traçabilité a pris place dans un contexte social de crise de confiance dans la filière alimentaire, et donc d'un risque sanitaire. Face à ce nouveau risque, elle se présentait comme une solution adéquate. Est-ce à dire aujourd'hui que la société actuelle, dominée par la peur et le narcissisme, est en crise de confiance dans la capacité des individus à suivre des règles de vie sociale, ou pour reprendre les termes de Lochré à être « *justes et sincères* » ? Plus clairement, est-ce à dire que l'individu aujourd'hui représente lui-même un risque, un danger, une menace ?

2. ... Par l'avènement en droit positif de la reconnaissance du principe de précaution

292. L'utilisation de la notion de traçabilité dans le langage juridique a été facilitée par l'avènement du principe de précaution tant au niveau international⁷⁵⁶, qu'au niveau européen⁷⁵⁷ et interne⁷⁵⁸. Tout comme la traçabilité, le principe de précaution tend à s'appliquer à tous les

⁷⁵⁶ C'est dans les années 1980 que le principe de précaution a été dégagé au niveau international en matière de protection de l'environnement. A titre d'exemple, on citera notamment l'adoption de la Convention de Vienne sur la protection de la couche d'ozone de 1985 avec laquelle « *les nations du monde entier ont accepté le principe de s'attaquer à un problème écologique mondial avant que ses effets ne se fassent sentir et avant même que son existence ne soit scientifiquement prouvée, ceci étant probablement le premier exemple de l'application du « principe de précaution » dans le cadre d'importantes négociations internationales* ». Programme des Nations Unies pour l'environnement, Secrétariat de l'ozone, *Convention de Vienne pour la protection de la couche d'ozone*, 22 mars 1985, En ligne: https://www.diplomatie.gouv.fr/sites/odyssee-developpement-durable/files/4/Convention_Vienne_1985.pdf (dernière consultation: 5 mars 2018)

⁷⁵⁷ L'Union européenne accorde au principe de précaution une place importante : article 174 du traité instituant les Communautés européennes, la résolution du Conseil des ministres du sommet européen de Nice du 7 décembre 2000 faisant suite à la communication de la Commission du mois de février de la même année. Il faut également noter ici que de nombreux règlements et directives en font mention ; notamment : la directive CE n° 2001/95 du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits et le règlement n° 178-2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires.

⁷⁵⁸ En droit interne, le principe de précaution est inscrit à l'article L.110-1, II, 1° du code de l'environnement (loi Barnier, n°95-101 du 2 février 1995). Il est également directement introduit à l'article 5 de la loi constitutionnelle n° 2005-205 du 1er mars 2005 relative à la Charte de l'environnement, JORF n°51 du 2 mars 2005, page 3697, texte n°2, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000790249&categorieLien=id> (dernière consultation: 5 mars 2018).

domaines représentant un risque potentiel⁷⁵⁹ pour la société, pour l'individu. Il a trouvé sa première application dans le domaine environnemental, puis comme pour la traçabilité, il a eu vocation à s'étendre aux produits alimentaires et sanitaires (vache folle, OGM, sang contaminé), aux constructions de bâtiments (amiante), ainsi que plus récemment pour les ondes électromagnétiques (téléphonie mobile), et bientôt pour les nanotechnologies. A l'instar de la traçabilité, le principe de précaution n'a pas de définition précise. Ainsi que l'ont rappelé Philippe Kourilsky et Geneviève Viney en 1999, le principe de précaution *« doit être entendu comme une incitation à l'action. Au dicton « dans le doute abstiens-toi », le principe de précaution substitue l'impératif : « dans le doute, mets tout en œuvre pour agir au mieux ». Cette attitude positive, d'action plutôt que d'inaction, de gestion active du risque plutôt que de démission devant le risque, correspond à l'objectif unanimement partagé de réduction des risques pour l'homme et l'environnement sans que celle-ci passe obligatoirement par une accumulation de moratoires et un gel des innovations⁷⁶⁰ ».*

293. Décrit en ces termes, le principe de précaution doit alors être entendu bien plus comme une règle de comportement face aux risques qu'une norme de droit *stricto sensu*. Le contenu normatif du principe de précaution⁷⁶¹, précisé par Geneviève Viney et Philippe Kourilsky en 1999, tend à confirmer ce propos : *« la position qui semble la plus répandue aujourd'hui subordonne la mise en œuvre du principe de précaution à l'énoncé d'une hypothèse de risque scientifiquement crédible, qui soit admise comme plausible par une partie significative de la communauté scientifique au moment où la décision est prise. (...) Elle privilégie en principe les mesures positives, notamment les recherches qui permettent une évaluation de plus en plus précise du risque, mais elle n'exclut pas le*

⁷⁵⁹ Pour preuve de cette applicabilité du principe de précaution aux risques, Voir: KOURILSKY Philippe, VINEY Geneviève, *Rapport au premier ministre - Le principe de précaution*, Odile Jacob: La Documentation française, 1999, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/004000402.pdf> (dernière consultation: 5 mars 2018). Dès l'introduction de ce rapport, les auteurs s'attardent sur le contenu conceptuel de ce principe, notamment sur le sens des mots : risque, danger, aléa, précaution et prévention. On notera que selon l'introduction de ce rapport (p. 11), *« la précaution est relative à des risques potentiels et la prévention à des risques avérés. (...) La précaution n'est ni l'inaction, ni une délibération sans fin. C'est un mode d'action d'un type particulier, requis par le contexte d'incertitude dans lequel la décision doit être prise. Le principe de précaution exige de la vigilance et la mise en œuvre de mesures proportionnées à la gravité du risque, bien que celui-ci ne soit que potentiel. Il impose la souplesse, puisque l'incertitude peut être dissipée avec l'évolution des connaissances, de sorte que les mesures prises seront généralement révisables et pourront être alourdies ou allégées, avec l'appréciation du risque, voire annulées si ce dernier est finalement jugé insignifiant. »*

⁷⁶⁰ KOURILSKY Philippe, VINEY Geneviève, *Rapport au premier ministre - Le principe de précaution*, Op. Cit. , p.8,

⁷⁶¹ Bien que le principe de précaution ne réponde pas d'une définition précise, trois conceptions semblent pouvoir se dégager : une conception minimaliste qui assimile la précaution à la notion de prévention en ne retenant son application qu'en présence d'un risque à la fois probable et de nature à provoquer de graves dommages ; une conception radicale qui conduit à garantir le risque zéro et à privilégier *« systématiquement, dans la représentation des dangers possibles, le « scénario du pire »*. » (rapport précité p. 63). Cette conception radicale conduit les décideurs publics ou privés à apporter la preuve de l'innocuité de leur action, en rejetant toute notion de proportionnalité liée notamment aux coûts économiques de la démarche de précaution. Enfin, il faut citer la conception médiane, intermédiaire explicitée ci-dessus.

*moratoire lorsque celui-ci s'avère nécessaire pour éviter des conséquences graves ou irréversibles. Enfin, dans l'établissement du bilan coût/avantage, elle permet de tenir compte non seulement des coûts économiques appréciés avec souplesse, mais également d'autres facteurs (sociaux, culturels, éthiques...)*⁷⁶² ». Ainsi, le principe de précaution ne vise pas à affirmer de nouvelles règles de droit fixant un régime particulier dans tel ou tel domaine, mais se traduit plutôt par la mise en place de pratiques et de procédures à suivre afin de rendre son introduction et la gestion du risque concrète et opérationnelle. « *Dix commandements*⁷⁶³ » doivent être envisagés pour l'application de principe : « *tout risque doit être défini, évalué et gradué ; l'analyse des risques doit être comparative ; préalablement à la décision, toute analyse de risque doit comporter une analyse économique ; les structures d'évaluation des risques doivent être indépendantes ; les décisions doivent, autant qu'il est possible, être révisables et les solutions adoptées réversibles et proportionnées ; sortir de l'incertitude impose une obligation de recherche ; les circuits de décisions sécuritaires doivent être efficaces, cohérents et fiables ; les évaluations, les décisions et leur suivi, ainsi que les dispositifs qui y contribuent, doivent être transparents, ce qui impose l'étiquetage et la traçabilité ; le public doit être informé au mieux et son degré de participation ajusté par le pouvoir politique*⁷⁶⁴ ». A la lecture de ce rapport, on constate bien que le principe de précaution s'appuie sur les notions de sécurité, de risque, de contrôle, d'expertise ; mais aussi et surtout de transparence permise grâce à la traçabilité.

294. En s'appuyant par exemple sur le domaine de la sécurité alimentaire, on voit bien depuis les années 80 – 90 une augmentation des exigences procédurales préalables à la mise sur le marché d'un produit, que l'on pense à l'étiquetage des produits OGM, ou encore aux récents débats concernant l'huile de palme, le recours au Bisphénol-A. S'agissant des décideurs publics, ces exigences permettent un renforcement des pouvoirs de police tel que définit par le droit administratif. Le code de la santé publique évoque d'ailleurs la notion de police sanitaire. A côté de ces éléments strictement procéduraux, on assiste à la création de plus en plus d'autorité, d'institutions indépendantes en charge de contrôler les décisions prises en amont et en aval⁷⁶⁵. Ces dispositifs institutionnels sont complétés par des pratiques destinées à assurer plus de transparence

⁷⁶² Ibid, p. 63

⁷⁶³ Ibid, p. 48

⁷⁶⁴ Ibid, p. 48 - 50

⁷⁶⁵ On pense ici à l'Agence Nationale de Sécurité Sanitaire de l'alimentation, de l'environnement et du travail (ANSES), résultat de la fusion de l'Agence Française de Sécurité Sanitaire des Aliments (AFSSA) et de l'Agence Française de sécurité sanitaire de l'environnement et du travail (AFSSET).

concernant certaines activités, certains domaines, ainsi qu'à écarter les craintes de dangerosité liées à ces dernières. On pense ici aux recours à des experts pour expliquer la nature du risque potentiel, et limiter la perception de la dangerosité de ce dernier ; mais aussi et surtout, à la généralisation du recours à la traçabilité. Appliqués aux individus, la traçabilité et le data-panoptisme permis par la totalisation numérique engendrent une véritable injonction de transparence.

B. ... A l'injonction de transparence des individus posée par la surveillance diffuse

295. La data-panoptisme, la traçabilité aidée par le principe de précaution ont permis progressivement de faire des individus des êtres transparents, des « citoyens de verre » pour reprendre l'expression de Wolfgang Sofsky (1). Cette injonction de transparence engendre des effets palpables dans la société contemporaine (2).

1. Traçabilité, principe de précaution et data-panoptisme ou l'injonction de transparence

296. Pour Gaspard Koenig, « *la clé du principe de précaution, et son plus grand danger, réside dans le refus de l'incertitude. (...). Ce que le principe de précaution dessine en filigrane, c'est le rêve cartésien d'un monde intégralement maîtrisé par la raison humaine, où causes et conséquences s'enchaînent de manière ordonnée et prévisible*⁷⁶⁶ ». Passant quasiment de la conception intermédiaire de ce principe à une conception radicale, conduisant à rechercher le risque zéro en se fondant sur l'hypothèse du scénario du pire, l'invocation⁷⁶⁷ et l'application du principe de

⁷⁶⁶ KOENIG Gaspard, *Quand Ebola relance le débat sur le principe de précaution*, Figaro Vox, Vox Monde, 11 août 2014, En ligne: <http://www.lefigaro.fr/vox/monde/2014/08/11/31002-20140811ARTFIG00111-quand-ebola-relance-le-debat-sur-le-principe-de-precaution.php> (dernière consultation: 5 mars 2018)

⁷⁶⁷ Il est important de souligner ce terme d'invocation du principe de précaution, qui frise parfois une logique d'incantation politique. Pour preuve de cette affirmation, on citera un extrait du livre de Didier Tabuteau, *Les contes de Ségur : les coulisses de la politique de santé (1988 – 2006)*, Ophrys, 2006 : « *la notion de précaution symbolise aujourd'hui une sorte de bouleversements des règles de la décision publique, des principes d'actions et des régimes de responsabilité. Prion, effet de serre, OGM, gaucho, légionellose, canicule, Vioxx, ... Le discours sur les risques s'est imprégné, peut-être devrait-on dire emparé, du principe de précaution. Norme juridique, principe moral d'action, incantation politique, standard de comportement, obligation d'État. Chacun paraît mettre derrière ce principe l'instrument qui sert sa cause.* » (p. 44). Cette incantation du principe de précaution par le politique a d'ailleurs des conséquences claires : le principe de précaution devient une rhétorique de l'action des politiques publiques. La frontière entre précaution et prévention est de plus en plus brouillée par ces incantations. Cette situation emporte parfois blocage de l'innovation et de la recherche ; à tel point qu'une *proposition de loi constitutionnelle visant à retirer le principe de précaution du bloc de constitutionnalité* a été enregistrée à la Présidence de l'Assemblée nationale le 13 juin 2014. Sur ces derniers points, voir : ATTALI Jacques, *Rapport de la Commission pour la libération de la croissance française*, XO Editions, La Documentation française, 2008, p. 91-92, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000041.pdf> (dernière consultation: 5 mars 2018), ainsi que HUNYADI Mark, « La logique du raisonnement de précaution », *Revue européenne des sciences sociales*, XLII-130|2004, En ligne <http://ress.revues.org/341> (dernière consultation: 5 mars 2018).

précaution à toutes les activités humaines⁷⁶⁸ ont permis d'appliquer la traçabilité à l'humain. N'est-ce pas là la réalisation du « *rêve cartésien d'un monde intégralement maîtrisé par la raison humaine* » décrit par Gaspard Koenig et pressenti par Weber ? En 1890 déjà, Gabriel Tarde écrivait que « *si la statistique continue à faire les progrès qu'elle a fait depuis plusieurs années, si les informations qu'elle nous fournit vont se perfectionnant, s'accélégrant, se régularisant, se multipliant toujours, il pourra venir un moment où, de chaque fait social en train de s'accomplir, il s'échappera pour ainsi dire automatiquement un chiffre, lequel ira immédiatement prendre son rang sur les registres de la statistique*⁷⁶⁹ ».

297. Par application du principe de précaution, l'individu, représentant un risque potentiel pour lui et les autres, doit être tracé. La surveillance diffuse, par le déploiement d'une ensemble technologique, a permis de réduire l'individu à son plus petit dénominateur: ses données personnelles et non personnelles. L'organisation de sa granularité par la numérisation de nos sociétés, la possibilité de voir l'ensemble de ses activités quotidiennes a permis la production de « chiffres statistiques », de traces. Que ce soit dans l'espace numérique - requête sur un moteur de recherche, conversation en ligne, statut des réseaux sociaux – ou dans les espaces publics et privés – vidéosurveillance, domotique, carte de fidélité, retrait bancaire – l'ensemble des faits et gestes d'un individu peut être envisagé, capté, enregistré, analysé par des outils statistiques et de plus en plus par des algorithmes informatiques. L'ensemble des activités sociales, ainsi numérisées, a permis pour des acteurs différents (État, entreprises) et dans des buts variés (sécurité, analyse des marchés) de penser une véritable observation totale et technicisée des individus. Cette observation totale des sociétés passe par l'analyse des traces que chaque individu laisse au quotidien dans ses pratiques sociales, et donc par la traçabilité humaine. Ainsi mis à nu, l'individu, tel un « *Petit-Poucet*⁷⁷⁰ » sème des traces de sa naissance à sa mort. Il organise sa propre transparence du fait de ses usages technologiques.

⁷⁶⁸ Récemment, on pourra citer l'invocation du principe de précaution concernant les biotechnologies et les nanotechnologies, concernant la menace du virus Ebola et la mise en quarantaine envisagée de tous les passagers en provenance des pays contaminés. On pourra également citer, au lendemain des attentats du 7 janvier 2015 à Charlie Hebdo, l'application extrême du principe de précaution par le Ministère de l'Intérieur avec le déclenchement de l'alerte attentat du plan Vigipirate, l'omniprésence des services de police, et les premières bases jetées du futur projet de loi sur le renseignement; mais également, l'invocation du principe de précaution avant toute implantation d'une nouvelle mosquée en France par M. Christian Estrosi sur son compte Facebook (<https://www.facebook.com/estrosi.christian/posts/10153390288830579> (dernière consultation: 5 mars 2018))

⁷⁶⁹ TARDE Gabriel, *Les lois de l'imitation*, Paris, Seuil, p. 151 – 152, 1890

⁷⁷⁰ FRAYSSINET Jean, « La traçabilité des personnes sur l'internet, une possible menace pour les droits et libertés », in. PEDROT Philippe (sous la direction de), *Traçabilité et responsabilité*, Paris, Economica, 2003, p. 88 - 113.

298. De nos jours, la traçabilité n'est donc plus simplement un outil, une technique permettant la gestion du risque. Comme le rappelle Philippe Pédrot, « à un moment où l'on assiste à une montée en puissance du droit, à une juridicisation des relations sociales, ce terme technique est désormais intégré dans le langage juridique. Instrument de pouvoir et de maîtrise, la traçabilité correspond à un arsenal de techniques visant à prévenir et à limiter les risques. Fil d'Ariane de la responsabilité, elle permet aussi d'assurer le suivi d'un produit à toutes les étapes de sa préparation et de sa distribution. Mécanisme de recherche de la sécurité, la traçabilité est également un procédé visant à promouvoir la qualité et la fiabilité technique des produits. Instrument de contrôle, elle permet enfin d'exercer une vigilance et une surveillance des personnes et des activités⁷⁷¹ ». La traçabilité et la précaution prennent place aujourd'hui dans un contexte de juridicisation⁷⁷² de l'ensemble des relations et activités sociales, et visent à une recherche de sécurité permanente, à un rejet de tout aléa. Ces notions semblent fondées non plus seulement sur les risques mais également et surtout sur les peurs collectives ou individuelles. La prise en compte de ces dernières semblent justifiées lorsqu'elles sont liées à des risques individuels ou collectifs, c'est-à-dire l'importante probabilité de vivre un drame ou de subir un dommage du fait d'un comportement ou d'une situation. Elle l'est moins lorsque le risque est imaginaire. Or, rappelons-le ici « *la France a peur*⁷⁷³ », et la peur est devenue aujourd'hui une réalité sociale sur laquelle les responsables politiques et les médias s'évertuent à agir⁷⁷⁴, parfois même en jouant sur cette peur. Pour preuve, la récupération politique et médiatique suite aux attentats du 7 au 11 janvier 2015 : en jouant sur les peurs du terrorisme, sur la crainte de la réalisation du scénario du pire, la traçabilité des individus, de leurs activités a été envisagée, et la surveillance a trouvé une nouvelle assise: l'injonction de transparence.

299. En deçà de la surveillance diffuse se profile un besoin d'informations sur les individus afin de gérer les risques et les dangers d'une société alimentée, volontairement ou non, par une certaine insécurité. Cette société du risque et de la peur est caractérisée par le besoin d'information de ses

⁷⁷¹ PEDROT Philippe, « Avant Propos. De la trace à la traçabilité : des enjeux nouveaux pour des risques nouveaux », p. VII – VIII, in. PEDROT Philippe (sous la direction de), *Traçabilité et responsabilité*, Paris, Economica, 2003

⁷⁷² Ce mot désigne le phénomène de propagation du droit et des solutions juridiques à un plus grand nombre de domaines de la vie sociale et économique, et conduit notamment, à la judiciarisation. Pour une étude de la notion de juridicisation dans le domaine du travail, voir : PELISSE Jérôme, « Juridicisation ou judiciarisation : usages et réappropriations du droit dans les conflits du travail », *Politix* 2/2009 (n° 86) , p. 73-96, En ligne: www.cairn.info/revue-politix-2009-2-page-73.htm (dernière consultation: 5 mars 2018)

⁷⁷³ C'est avec cette phrase que Roger Gicquel ouvre son journal télévisé sur TF1, le 18 février 1976. La vidéo de ce journal est disponible en ligne à l'adresse suivante : <http://www.ina.fr/video/CAA87014358> (dernière consultation: 5 mars 2018)

⁷⁷⁴ Nous renvoyons aux analyses développées précédemment. Voir également: FEDERBUSCH Serge, *La marche des lemmings. La deuxième mort de Charlie Hebdo*, Ixelles Editions, 2015

gestionnaires publiques ou privés et des citoyens. Plus l'information dont les personnes disposent est grande, plus ils sont en mesure de calculer les risques dans l'espoir de les réduire, de les éliminer. Ce besoin d'informations constitue aujourd'hui un puissant moyen de collecte d'informations destiné à atténuer les menaces à la sécurité, à réduire la criminalité, et à assurer la pérennité d'un marché économique. Il porte en son sein l'injonction de transparence des individus.

2. Des effets de la transparence imposée

300. Le nouvel enjeu politique de nos sociétés contemporaines réside dans la maîtrise des risques, des menaces, des peurs. Au delà de ces mots et expressions, le politique cherche à maîtriser les conséquences indésirables de la vie en société. Cette affirmation engendre un travail d'objectivation des peurs et de discours sur les représentations des menaces, des risques; permettant la mise en place de logiques narratives et discursives. Légitimation des interventions institutionnelles par la gouvernementalité par la peur, traçabilité des individus, précaution et prévention, encouragements à l'adaptation des individus aux nouvelles technologies, acceptabilité de ces dernières, logique du feedback par la datafication sont autant d'effets insidieux de l'organisation et de la prise en charge de la transparence des individus. La situation actuelle s'inscrit alors dans une logique anticipative visant à obtenir des connaissances sur l'individu devenu dangereux, encourageant ainsi la culture de la surveillance. L'intériorisation de cette culture a fait de l'injonction de transparence une forme d'auto-contrôle promue par des « entrepreneurs de morale⁷⁷⁵ », produit par une idéologie dominante⁷⁷⁶, par une forme ingénieuse de propagande⁷⁷⁷ dans la société de consommation. Nicole Aubert et Claudine Haroche sous-entendent ces interrogations dès l'introduction de leur ouvrage en écrivant: « *au XIX^{ème} siècle, dans les sociétés occidentales, il fallait taire l'intime: un renversement de valeurs, dans ces mêmes sociétés, conduit aujourd'hui à se livrer à une exhibition de l'intime pour exister. L'invisible tendant dans notre société à signifier l'insignifiant, et au-delà l'inexistant. (...). Pourquoi et comment l'exigence de visibilité a-t-elle pris une telle ampleur aujourd'hui dans notre société? Est-ce en raison de l'extension des exigences bureaucratiques? Du développement de formes de pouvoir, de domination*

⁷⁷⁵ Voir en ce sens: BECKER Howard, *Outsiders: Etudes de sociologie de la déviance*, Editions Métailié, 2012

⁷⁷⁶ Voir en ce sens: BOURDIEU Pierre, BOLTANSKI Luc, « La production de l'idéologie dominante », in. *Actes de la recherche en sciences sociales*, 1976, Volume 2, numéro pp. 3 - 73, En ligne: http://www.persee.fr/doc/AsPDF/arss_0335-5322_1976_num_2_2_3443.pdf (dernière consultation: 5 mars 2018)

⁷⁷⁷ Voir en ce sens: CHOMSKY Noam, HERMAN Edward, *La fabrication du consentement - De la propagande médiatique en démocratie*, Editions Agone, Collection Contre-feux, 2008. Mais aussi: HAZAN Eric, *Lingua Quintae Republicae - La propagande au quotidien*, Editions Raisons d'agir, 2006.

et de servitude liées en particulier à la globalisation et aux évolutions de la technologie et des moyens de communication omniprésents et continus ?⁷⁷⁸ ».

301. L'exigence de transparence, renforcée par la surveillance diffuse dans nos sociétés, répond au désir de reconnaissance quasi instantané des individus. La transparence permet d'une part, d'évaluer, selon des rationalités différentes, la qualité d'un travail, notre rapport aux autres, à notre consommation, de « *juger de son utilité pour la collectivité, la société, le bien commun, de juger de son coût et de justifier alors la dépense, l'emploi des deniers publics⁷⁷⁹ »*. D'autre part, la transparence induit des mécanismes de contrôles de plus en plus insidieux pouvant parfois relever des analyses du panoptique de Foucault et des sociétés de contrôle de Deleuze. Toutefois, cette exigence de transparence liée à la surveillance diffuse semble revêtir un sens plus profond que la référence au contrôle, à la société de contrôle. Certes, la surveillance diffuse s'inscrit dans la lignée de ces analyses. Elle renforce le contrôle social, les sociétés de contrôle, ainsi qu'une visibilité intégrale, une transparence. Mais, par l'incitation à l'auto-contrôle et l'auto-contrainte qu'elle porte en son sein, aujourd'hui l'individu participe clairement de cette transparence. Et c'est dans ce rapport des individus à la transparence induite par la surveillance diffuse, que le principe de visibilité dégagé par Foucault prend tout son sens. Jean-Philippe Bouilloud dresse, en 2011, une présentation efficace du sens de l'exigence de visibilité contemporaine. Il écrit ainsi que: « *la visibilité s'est instituée comme projet: être vu de soi et des autres, être reconnu (pour soi-même, pour ce que l'on est, pour ce que l'on représente, peu importe...) devient l'horizon du désir de l'individu en société. Dès lors, il y a une injonction sous-jacente à la visibilité dans nos sociétés contemporaines. Celle-ci porte en elle-même un double problème: d'un côté, un « trop » (d'exigence de visibilité...), de l'autre côté un « trop peu » (une négligence sociale). La problématique de la visibilité se situe ainsi à la jonction de différentes forces antinomiques: injonction à voir (le citoyen est transformé en spectateur permanent) et à être vu dans la « médiatisation généralisée », mais aussi désir de liberté, c'est-à-dire de s'en échapper; désir d'être vu et reconnu, mais sans être « épié »; réalité panoptique (Bentham-Foucault), mais aussi impossibilité de rendre compte de la totalité du réel (H. Simon)⁷⁸⁰ »*. Dans cette représentation de la

⁷⁷⁸ AUBERT Nicole, HAROCHE Claudine (sous la direction de), *Les tyrannies de la visibilité - Etre visible pour exister?*, Editions Eres, Collection Sociologie clinique, 2011, p. 7 - 8.

⁷⁷⁹ Ibid

⁷⁸⁰ BOUILLOUD Jean-Philippe, « Du monde de la parole au règne du visible » p. 72 - 73, in. AUBERT Nicole, HAROCHE Claudine (sous la direction de), *Les tyrannies de la visibilité - Etre visible pour exister?*, Editions Eres, Collection Sociologie clinique, 2011, pp. 55 - 76.

totalité du réel, l'individu contraint à la transparence est incité à devenir responsable.

302. Par la traçabilité, la précaution, il s'agit, ainsi que le souligne Mark Hunyadi: « *d'imposer – si possible par le droit, mais à tous le moins dans les intentions – une limite de principe aux activités instrumentales, qui, livrées à elles-mêmes, suivent une logique simplement cumulative et orientée en fonction d'une fin qu'elles établissent elles-mêmes ; alors qu'elles sont par leur nature même rationnelles en fonction d'une fin, elles sont à présent en quelque sorte sommées de devenir responsables à l'égard des conséquences provoquées en dehors de leur sphère d'action particulière*⁷⁸¹ ». Rappelons ici les mots de Michel Foucault lorsqu'il analysait le pouvoir disciplinaire: « *Le pouvoir disciplinaire, lui, s'exerce en se rendant invisible; en revanche il impose à ceux qu'il soumet un principe de visibilité obligatoire. Dans la discipline, ce sont les sujets qui ont à être vus. Leur éclairage assure l'emprise du pouvoir qui s'exerce sur eux. C'est le fait d'être vu sans cesse, de pouvoir toujours être vu, qui maintient dans son assujettissement l'individu disciplinaire*⁷⁸² ». Pour reprendre les termes de Nicole Aubert et Claudine Haroche, tout se passe aujourd'hui comme si nous vivions sous des « *tyrannies de la visibilité*⁷⁸³ »; comme si, pour exister nous nous devons à la fois d'être visible et évaluable⁷⁸⁴ et que pour vivre en société nous nous devons d'être transparent.

⁷⁸¹ HUNYADI Mark, *Op. Cit.*

⁷⁸² FOUCAULT Michel, *Surveiller et punir (Op. Cit)*, p. 334.

⁷⁸³ AUBERT Nicole, HAROCHE Claudine (sous la direction de), *Les tyrannies de la visibilité - Etre visible pour exister?*, Editions Eres, Collection Sociologie clinique, 2011

⁷⁸⁴ La Chine souhaite attribuer une note de confiance à chaque citoyen en fonction de son comportement, directement évalué au travers des données qu'il laisse sur lui. Voir en ce sens: ARSENE Séverine, *La Chine nouveau laboratoire du contrôle social de la population*, Le Monde, 26 octobre 2017, p. 2

Chapitre 2: Un déficit d'effectivité globale des premières législations informatiques et libertés face à la surveillance diffuse

303. La surveillance diffuse doit être analysée comme une attention des Etats, des entreprises et des individus qui, par la datafication et la totalisation numérique, réduit l'individu à son plus petit dénominateur commun: la data, l'information, la donnée. Ces éléments engendrent normalisation des comportements et organisation d'une plasticité sociale. Si la surveillance diffuse n'a aucune définition juridique, le législateur est intervenu afin d'en réglementer certains aspects. Très tôt, le traitement des données à caractère personnel a été réglementé, puis amendé, et modifié. Plus récemment, ce sont les technologies de l'information et de la communication et les technologies de sécurité qui ont vu leur domaine être saisi par le Droit. On pense notamment à la vidéosurveillance qui a vu son régime naître, puis être amendé, et modifié pour parvenir à un double régime, d'un côté la vidéosurveillance pour les lieux privés et la vidéoprotection, de l'autre, pour les lieux publics.

304. Pour le juriste, la réponse de la loi aux défis de la société de l'information et de la communication, plus généralement aux défis posés par la surveillance diffuse, semble se développer dans un désordre absolu. En effet, cette dernière s'élabore sous forme de réglementations mal coordonnées et sans cesse remise en question. Alors qu'il tentait d'élaborer une ébauche d'une théorie juridique de l'information, en 1982, Pierre Catala se demandait: « *comment éviter, en effet, que la réponse de la loi au défi électronique ne s'élabore dans le désordre, sous forme de réglementations mal coordonnées, minutieuses à l'excès et cependant parcellaires, attelées au progrès scientifique et, comme lui, sans cesse remises en question, oubliées enfin de quelques vérités permanentes auxquelles pourraient s'attacher des règles stables ?*⁷⁸⁵ » La situation décrite par Catala est loin d'être évitée puisque le juriste se retrouve aujourd'hui confronté à des problèmes de droit sans cesse renouvelés, et toujours plus imbriqués au progrès scientifique. Ainsi, la notion de donnée personnelle et sa protection paraissent être, aujourd'hui, de plus en plus insaisissable pour le juriste. Les différentes évolutions technologiques, l'élaboration de que certains auteurs décrivent comme un « *biopouvoir algorithmique*⁷⁸⁶ », ou encore la réduction de l'individu à une trace, ont tendance à brouiller le caractère éminemment personnel de la donnée. La surveillance diffuse, en

⁷⁸⁵ CATALA Pierre, *Le droit à l'épreuve du numérique - Jus ex Machina*, Presses Universitaires de France, Collection Droit, Ethique, Société, Première édition, mai 1998, p. 226. Voir spécialement Chapitre 13 pp. 224 - 244. Ce chapitre développe des réflexions que l'auteur a présenté oralement le 12 mai 1982 lors des Deuxièmes Entretiens du droit de l'informatique de Nanterre.

⁷⁸⁶ ROUVROY Antoinette, Berns Thomas, « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événements car constitué de corps « numériques »... », *Multitudes* 2010 / 1 (n° 40), p. 88 - 103, En ligne: <https://www.cairn.info/revue-multitudes-2010-1-page-88.htm> (dernière consultation: 5 mars 2018)

tant que principal moyen de ce « *nouveau pouvoir statistique*⁷⁸⁷ », engendre traitement d'informations non personnelles, qui par truchement technologique, ou interconnexion de bases de données, rendent leur caractère personnel à ces données. Le juriste doit-il alors se saisir de l'entier processus ? Ou, comme l'indique la loi, uniquement du traitement de données à caractère personnel ?

305. Le déficit de conscience des enjeux de la surveillance diffuse engendre un déficit d'effectivité global des premières législations informatiques et libertés. Si les notions de data, d'informations et de données personnelles soulèvent des interrogations, il semble en réalité que l'entièreté de l'opération de traitement des données qu'envisage la surveillance diffuse doit être questionnée (section 1). On constatera alors une impossibilité d'application des principes fondamentaux des premières législations informatiques et libertés (section 2).

Section 1. L'insaisissabilité de la protection des données personnelles au vu de la surveillance diffuse

306. La surveillance diffuse cherche à recueillir toujours plus d'informations sur les individus. Ces informations ne sont pas forcément des données strictement personnelles. Pourtant le traitement d'informations et de données personnelles (Paragraphe 2) est au coeur de la cible des recherches de la surveillance diffuse. En ce qu'elle souhaite établir des profils les plus individualisés possibles, et en ce qu'elle permet de réduire l'individu à une trace ce double effort de la surveillance doit être garder en tête. Qu'elle soit personnelle ou non, l'information que traite la surveillance porte sur l'individu, et c'est bien cette opération qui paraît dangereuse en termes de libertés individuelles et de vie privée. De plus, l'élargissement progressif de la notion de donnée personnelle, opéré par la jurisprudence ou la doctrine, a tendance à marquer d'incertitude et d'ineffectivité le champ d'application de la loi (Paragraphe 1). Que l'on pense à des données strictement techniques, tels que la métadonnée, le log mais également à l'adresse IP; ou que l'on songe à des numéros d'immatriculation de véhicules, de machines, l'incertitude saisit le juriste quant à l'applicabilité ou non de la définition même de la donnée à caractère personnelle.

⁷⁸⁷ Ibid.

Paragraphe1. L'élargissement progressif de la notion de données personnelles facteur de son ineffectivité

307. L'élargissement progressif de la notion de données personnelles s'est d'abord appliqué à des données d'identification techniques. Certaines de ces données, bien que non personnelles au sens de l'article 2 de la loi informatique et libertés, ont été reconnues par la pratique jurisprudentielle comme personnelle. Prenant appui sur le contentieux lié à l'adresse IP, il paraît intéressant de démontrer que l'opération de qualification juridique de la donnée en tant que personnelle ou non met à l'épreuve la « *sagacité des juristes*⁷⁸⁸ », pour reprendre les termes de Pierre Catala (A). L'élargissement du concept juridique de données personnelles s'est ensuite attaché à prendre en compte les évolutions techniques et les nouveaux usages. Issu des révélations de l'affaire Snowden, l'exemple récent de la notion de métadonnées, et plus globalement des données de connexion, devant recevoir le qualificatif de données personnelles du fait de la surveillance diffuse reflète parfaitement cette affirmation (B).

A. La délicate opération de qualification juridique de la donnée en tant que donnée personnelle: l'exemple des données d'identification techniques considérées comme des données personnelles

308. La loi de 1978 visait à l'origine les informations nominatives. Ce terme permettait d'identifier clairement pour le juriste ce qui devait entrer ou non dans le champ d'application de la loi. Avec sa modification en 2004 par la transposition de la directive, la loi informatique et libertés élargit son champ d'application par le recours à la notion de données à caractère personnel. De par sa définition même, la donnée à caractère personnel renvoie en effet à un vaste champ d'analyse, que les techniques et les usages informatiques n'ont de cesse de faire évoluer. Pour rappel, l'article 2 de la loi informatique et libertés dispose qu'est une donnée à caractère personnel « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont*

⁷⁸⁸ Ainsi que le rappelait Pierre Catala, « *l'informatique et la télématique demeurent tributaires d'une technologie en constant devenir. Aussi les problèmes de droit qu'elles proposent à la sagacité des juristes sont-ils sous la dépendance de données techniques mouvantes* ». in. CATALA Pierre, *Le droit à l'épreuve du numérique - Jus ex Machina*, Presses Universitaires de France, Collection Droit, Ethique, Société, Première édition, mai 1998, p. 225 - 226. Voir spécialement Chapitre 13 pp. 224 - 244. Ce chapitre développe des réflexions que l'auteur a présenté oralement le 12 mai 1982 lors des Deuxièmes Entretiens du droit de l'informatique de Nanterre.

propre ». Aussi et pour déterminer si une personne est identifiable, il faut, selon la loi, considérer « *l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ». L'opération de qualification juridique d'une information en tant que donnée à caractère personnel (1) présente un enjeu considérable puisque de cette opération découlera l'application du régime de protection envisagée par la loi. L'étude des jurisprudences françaises et européennes en la matière démontre que ces données reçoivent leur qualification de « donnée personnelle » au vu du traitement réalisé sur ce type de données techniques (2).

1. La qualification de l'adresse IP en tant que donnée à caractère personnel...

309. La donnée d'identification technique peut être envisagée comme toute information d'identification attribuée à un appareil connecté à internet, permettant la communication entre ces appareils. Tel est le cas par exemple de l'adresse IP. Cette dernière peut être statique - une machine reçoit la même adresse IP dans le temps - ou dynamique - l'adressage change à chaque nouvelle connexion. Ainsi, lorsqu'un internaute se connecte sur un site, l'adresse IP de l'ordinateur qu'il utilise sera collectée. Elle identifie alors une machine, et non l'individu qui utilise l'ordinateur. Dans ce cas précis, et étant donné qu'elle n'est pas couplée à une information identifiante⁷⁸⁹, on voit mal comment l'adresse IP pourrait recevoir le qualificatif de donnée personnelle. Pourtant, les juges européens et français en ont décidé autrement à plusieurs reprises. S'appuyant sur une jurisprudence constante qui adopte une vision élargie de la définition de la donnée personnelle⁷⁹⁰, le juge européen considère l'adresse IP comme une donnée à caractère personnel. Par deux arrêts opposant des

⁷⁸⁹ Un compte client par exemple

⁷⁹⁰ En ce sens: CJCE, Affaire C-101/01, Lindqvist, arrêt de la Cour du 6 novembre 2003, Recueil de la jurisprudence 2003 I-12971. Le point 24 de cet arrêt est particulièrement clair sur ce point: « *la notion de « données à caractère personnel » employée à l'article 3, paragraphe 1, de la directive 95/46 englobe, conformément à la définition figurant à l'article 2, sous a), de celle-ci, « toute information concernant une personne physique identifiée ou identifiable ». Cette notion comprend assurément le nom d'une personne joint à ses coordonnées téléphoniques ou à des informations relatives à ses conditions de travail ou à ses passe-temps* ». Dans le point suivant la Cour précise: « *quant à la notion de « traitement » de telles données employée à l'article 3, paragraphe 1, de la directive 95/46, elle comprend, conformément à la définition figurant à l'article 2, sous b), de celle-ci, « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel* ». Cette dernière disposition mentionne plusieurs exemples de telles opérations, parmi lesquels figurent la communication par transmission, la diffusion ou toute autre forme de mise à disposition de données. Il s'ensuit que l'opération consistant à faire figurer, sur une page Internet, des données à caractère personnel est à considérer comme un tel traitement ». En ligne: <http://curia.europa.eu/juris/showPdf.jsf?docid=48382&pageIndex=0&doclang=FR&dir=&occ=first&part=1&cid=1403476> (dernière consultation: 5 mars 2018).

fournisseurs d'accès à Internet et des titulaires de droits de propriété intellectuelle rendus en 2008⁷⁹¹ et 2012⁷⁹², la Cour de Justice déclare que la communication par des fournisseurs d'accès à internet des adresses IP de leurs clients constitue un traitement de données à caractère personnel, et reconnaît par là la qualification de donnée personnelle à l'adresse IP.

310. Ainsi, dans l'arrêt *Promusicae* rendue en 2008, la Cour estime: « *il n'est par ailleurs pas contesté que la communication, sollicitée par Promusicae, des noms et des adresses de certains utilisateurs de KaZaA implique la mise à disposition de données à caractère personnel, c'est-à-dire d'informations sur des personnes physiques identifiées ou identifiables, conformément à la définition figurant à l'article 2, sous a), de la directive 95/46 (voir, en ce sens, arrêt du 6 novembre 2003, Lindqvist, C-101/01, Rec. p. I-12971, point 24). Cette communication d'informations qui, selon Promusicae, sont stockées par Telefonica - ce que cette dernière ne conteste pas - , constitue un traitement de données à caractère personnel, au sens de l'article 2, premier alinéa, de la directive 2002/58, lu en combinaison avec l'article 2, sous b), de la directive 95/46. Il doit donc être admis que ladite communication relève du champ d'application de la directive 2002/58, étant observé que la conformité du stockage des données lui-même aux exigences de cette dernière directive n'est pas en cause dans le litige au principal*⁷⁹³ ».

311. En 2012, la Cour opérant par renvoi à l'arrêt de 2008, renouvelle sa décision et déclare: « *en vue de donner cette réponse utile, il convient, d'abord, de rappeler que, dans l'affaire au principal, Bonnier Audio e.a. souhaitent la communication, aux fins de son identification, du nom et de l'adresse d'un abonné à Internet ou d'un utilisateur d'Internet faisant usage de l'adresse IP à partir de laquelle il est présumé que des fichiers contenant des œuvres protégées ont été illicitement échangés. Il y a lieu de constater que la communication souhaitée par Bonnier Audio e.a. constitue un traitement de données à caractère personnel au sens de l'article 2, premier alinéa, de la directive 2002/58, lu en combinaison avec l'article 2, sous b), de la directive 95/46. Cette*

⁷⁹¹ CJCE, Affaire C-275/06, arrêt de la Cour (grande chambre) du 29 janvier 2008, *Promusicae* contre Telefonica de Espana SAU, Recueil de la jurisprudence 2008 I-00271, Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=70107&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=1413942> (dernière consultation: 5 mars 2018)

⁷⁹² CJUE, Affaire C-461/10, arrêt de la Cour (troisième chambre) du 19 avril 2012, publié au Recueil numérique (Recueil général), *Bonnier Audio AB*, contre *Perfact Communication Sweden AB*, Disponible en ligne: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=1421614> (dernière consultation: 5 mars 2018)

⁷⁹³ Op. Cit. point 45

communication relève donc du champ d'application de la directive 2002/58 (voir, en ce sens, arrêt Promusicae, précité, point 45)⁷⁹⁴ ».

312. Bien qu'il ne soit pas mentionné clairement qu'une adresse IP soit une donnée à caractère personnel, le juge européen rappelle qu'une communication d'adresse IP par un fournisseur d'accès à internet combinée avec le nom d'abonné, ou des informations clients permettent l'identification d'une personne, et donc par là constitue un traitement de données à caractère personnel. En 2000, le Groupe de l'article 29 déclare que *« pour obtenir une connexion, le particulier doit conclure un contrat (la connexion est gratuite) et donner ses nom, adresse et autres données à caractère personnel. En général l'utilisateur reçoit un nom d'identification utilisateur (UserID qui peut être un pseudonyme) et un mot de passe pour éviter qu'une autre personne ne puisse utiliser son inscription. Il semble que les fournisseurs d'accès à Internet, ne fût-ce que pour des raisons de sécurité, aient la coutume d'enregistrer systématiquement dans un fichier la date, l'heure, la durée et l'adresse IP dynamique donnée à l'utilisateur Internet. Aussi longtemps qu'il est possible de faire un lien entre le fichier-registre et l'adresse IP d'un utilisateur, cette adresse doit être considérée comme une information personnelle⁷⁹⁵ »*. Et d'affirmer plus loin que *« les fournisseurs d'accès Internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP donnée à l'utilisateur Internet. Il en va de même des fournisseurs de services Internet qui conservent un fichier-registre sur le serveur HTTP. Dans ces cas-ci, on peut parler, sans l'ombre d'un doute, de données à caractère personnel dans le sens de l'article 2 a) de la directive⁷⁹⁶ »*. En réalité, il faut retenir de ces positions du groupe de l'article 29, que l'adresse IP faisant partie des données de trafic, conservées pendant un an par les opérateurs de communications électroniques, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, doit être considérée comme une donnée personnelle puisqu'elle rend, au vu de ce traitement, une personne identifiable.

⁷⁹⁴ Op. Cit points 51 et 52.

⁷⁹⁵ Groupe sur la protection des personnes à l'égard du traitement des données à caractère personnel, *Document de travail: Le respect de la vie privée sur Internet - Une approche européenne intégrée sur la protection des données en ligne -*, Adopté le 21 novembre 2000, 5063/00/FR/Final, WP 37, p. 12

⁷⁹⁶ Ibid. p. 22. Le Groupe de l'article 29 réitérera sa position en 2007, et déclarera que *« les fournisseurs d'accès Internet (...) devront traiter toutes les informations IP (statiques et dynamiques) comme des données à caractère personnel »*. In. Groupe de travail « article 29 » sur la protection des données, *Avis 4/2007 sur le concept de données à caractère personnel*, 20 juin 2007, 01248/07/FR, WP 136, p. 18

2. ... Du fait de l'opération de traitement

313. A l'occasion d'une délibération portant dénonciation au parquet d'infractions à la loi du 6 janvier 1978 concernant des activités de spamming⁷⁹⁷, la CNIL française, quant à elle, rappelle que *« les personnes titulaires d'une adresse électronique bénéficient des dispositions protectrices de la loi du 6 janvier 1978. En effet, une adresse électronique est une information nominative au sens de l'article 4 de la loi du 6 janvier 1978 qui précise : « Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ».* Ainsi, une adresse électronique est directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse et, lorsque tel n'est pas le cas, indirectement nominative dans la mesure où toute adresse électronique peut être associée à un nom ».

314. Alors que cette délibération de la CNIL fait expressément mention de l'adresse mail, on comprend que la logique mise en place pour l'adresse mail pourrait trouver application à l'adresse IP. La CNIL clarifie d'ailleurs sa position en 2007. S'inquiétant de deux décisions de la Cour d'appel de Paris qui considéreraient alors que l'adresse IP n'est pas une donnée à caractère personnel, la CNIL rappelle en effet que *« l'article 2 de la loi du 6 janvier 1978 modifiée en 2004 qui la définit, vise toute information relative à une personne physique qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à des éléments qui lui sont propres. Ce qui est le cas d'un numéro de plaque d'immatriculation de véhicule, d'un numéro de téléphone ou d'une adresse IP. L'ensemble des autorités de protection des données des Etats membres de l'Union européenne a d'ailleurs récemment rappelé, dans un avis du 20 juin 2007 relatif au concept de données à caractère personnel, que l'adresse IP attribuée à un internaute lors des ses communications constituait une donnée à caractère personnel⁷⁹⁸ ».* A la lecture de ces lignes, on voit bien que la CNIL cherche à rapprocher toutes données d'identification technique, tels que

⁷⁹⁷ CNIL, Délibération n° 02-075 du 24 octobre 2002 portant dénonciation au Parquet d'infractions à la loi du 6 janvier 1978, En ligne: https://www.cnil.fr/sites/default/files/typo/document/delib_spam.pdf (dernière consultation: 5 mars 2018)

⁷⁹⁸ CNIL, *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes*, 2 août 2007, En ligne: <https://www.cnil.fr/fr/ladresse-ip-est-une-donnee-caractere-personnel-pour-lensemble-des-cnil-europeennes> (dernière consultation: 5 mars 2018)

l'adresse IP, le numéro de téléphone, la plaque d'immatriculation à des données personnelles⁷⁹⁹.

315. La jurisprudence française a longtemps fluctué de l'une à l'autre des positions, ne sachant affirmer avec clarté si l'adresse IP constituait ou non une donnée personnelle. Entre 2006 et 2016, le juge judiciaire et le juge administratif ont eu à se prononcer sur la nature juridique de l'adresse IP. Ainsi en 2006, le Tribunal de Grande Instance de Bobigny saisi d'une action en contrefaçon de droits d'auteur et s'appuyant sur l'article 2 de la loi Informatique et Libertés, déclare qu'au regard de la définition posée par la loi de 1978, « *l'adresse IP constitue une donnée à caractère personnel en ce qu'elle permet d'identifier une personne en indiquant sans doute possible un ordinateur précis. Le numéro IP établit la correspondance entre l'identifiant attribué lors de la connexion à l'internaute et l'identité de l'abonné*⁸⁰⁰ ». Quelques mois plus tard, le TGI de Saint Briec, s'appuyant sur la définition technique de l'adresse IP, déclare que cette dernière « *est, au sens strict, un identifiant d'une machine lorsque celle-ci se connecte sur l'internet et non d'une personne. Mais au même titre qu'un numéro de téléphone n'est, au sens strict, que celui d'une ligne déterminée mais pour laquelle un abonnement a été souscrit par une personne déterminée, un numéro IP associé à un fournisseur d'accès correspond nécessairement à la connexion d'un ordinateur pour lequel une personne déterminée a souscrit un abonnement auprès de ce fournisseur d'accès. L'adresse IP de la connexion associée au fournisseur d'accès constituent un ensemble de moyens permettant de connaître le nom de l'utilisateur*⁸⁰¹ ». Dans deux autres arrêts rendus par la Cour d'Appel de Paris en 2007, les juges refusent la qualification de l'adresse IP en tant que donnée personnelle⁸⁰². Après plusieurs revirements jurisprudentiels, il faut attendre l'année 2016 et deux arrêts rendus, l'un par la Cour de Cassation, l'autre par la Cour de justice de l'Union Européenne

⁷⁹⁹ N'ayant qu'un avis consultatif, la position de la CNIL ne lie pas le pouvoir judiciaire, d'autant plus que cette position a été exprimé à travers non pas un avis ou une délibération, mais bien à travers un communiqué de presse.

⁸⁰⁰ TGI de Bobigny, 14 décembre 2006, Laurent F. c/ SACEM et autres, En ligne: <https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-bobigny-15eme-chambre-jugement-du-14-decembre-2006/> (dernière consultation: 5 mars 2018)

⁸⁰¹ TGI de Saint Briec, 6 septembre 2007, Ministère public, SSCP, SACEM c/ J. P. , En ligne: <https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-saint-briec-jugement-du-06-septembre-2007/> (dernière consultation: 5 mars 2018)

⁸⁰² La Cour d'Appel de Paris a rendu un premier arrêt le 27 avril 2007 dans lequel elle déclare que « *chaque ordinateur connecté à internet est identifié par un numéro unique appelé « adresse internet » ou adresse IP (internet protocol) qui permet de le retrouver parmi les ordinateurs connectés ou de remonter à l'expéditeur d'un message. L'adresse IP ne permet pas d'identifier le ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur* ». in. Cour d'Appel de Paris, 13^{ème} chambre, section B, arrêt du 27 avril 2007, Anthony G. c/ SSCP, En ligne: <https://www.legalis.net/jurisprudences/cour-dappel-de-paris-13eme-chambre-section-b-arret-du-27-avril-2007/> (dernière consultation: 5 mars 2018). Puis le 15 mai 2007, la même Cour d'Appel déclare que l'adresse IP qui est une « *série de chiffre (...) 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 pour se livrer à la contrefaçon* ».

pour mettre fin à l'incertitude qui entoure le statut juridique de l'adresse IP.

316. En octobre 2016, la CJUE a à nouveau eu l'occasion de se prononcer en faveur de la reconnaissance du statut de donnée personnelle pour l'adresse IP. Saisie d'une question préjudicielle opposant un particulier qui se plaignait de l'enregistrement et de la conservation de son adresse IP par la République fédérale d'Allemagne, après avoir consulté plusieurs sites internet des services fédéraux allemands, la Cour déclare: « *eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la première question que l'article 2, sous a), de la directive 95/46 doit être interprété en ce sens qu'une adresse IP dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne*⁸⁰³ ». La Cour de Cassation rend quant à elle un arrêt le 3 novembre 2016 où elle déclare que « *la collecte pendant plusieurs années, d'adresses IP qui permettent l'identification des utilisateurs constitue un traitement automatisé de données à caractère personnel contenu dans un fichier lequel doit donner lieu à déclaration à la CNIL*⁸⁰⁴ ».

317. La problématique du statut juridique de l'adresse IP se résume en ces termes: si l'adresse IP est envisagée comme une donnée personnelle, cela implique que toute manipulation de ce type d'informations doit être envisagée comme un traitement de donnée personnelle régi par la loi du 6 janvier 1978. Et de ce fait, bénéficie de dispositions protectrices prévu pour protéger la personne physique d'une part, et risque de tomber sous le coup des sanctions prévues en cas de non respect des dispositions légales prévues à cet effet d'autre part⁸⁰⁵. Encore faut il que cela concerne une personne physique dans la mesure où la loi du 6 janvier 1978 ne protège que cette catégorie de personnes. Si le statut juridique de l'adresse IP semble être clairement défini aujourd'hui, il n'en

⁸⁰³ CJUE, Affaire C-582/14, arrêt de la Cour (deuxième chambre) du 19 octobre 2016, publié au Recueil numérique, (Recueil général), Patrick Breyer contre Bundesrepublik Deutschland, En ligne: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=755321> (dernière consultation: 5 mars 2018)

⁸⁰⁴ Cour de Cassation, 1ère Chambre Civile, Audience publique du jeudi 3 novembre 2016, n° de pourvoi: 15-22595, publié au bulletin, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000033346676&fastReqId=233794771&fastPos=1> (dernière consultation: 5 mars 2018)

⁸⁰⁵ Cela implique le recours à la CNIL en amont de tout traitement pour autorisation, et en cas de conflit, c'est le tribunal de grande instance qui sera matériellement compétent.

reste pas moins que l'ensemble du contentieux lié à cette donnée met en lumière la question que le juriste doit se poser lorsqu'il est en face d'informations techniques.

318. Si cette information peut être combinée avec des données détenues par un tiers permettant l'identification d'un individu, et que cette opération peut être raisonnablement mis en oeuvre par ce tiers, il se peut que l'opération soit requalifiée en traitement de donnée à caractère personnel. Cette requalification de l'information technique en tant que personnelle, du fait de son traitement, doit être pris en compte dans une dimension prospective par le juriste. Car, en effet, la même logique est à l'oeuvre en matière de reconnaissance de plaque d'immatriculation. Cette donnée technique n'engendre pas identification du conducteur du véhicule lorsqu'il commet une infraction au Code de la route, mais bien le propriétaire du véhicule. Pourtant, la plaque d'immatriculation est conçue aujourd'hui comme une donnée à caractère personnel par la loi et la CNIL. Bien que le caractère identifiable de la personne en cause, au coeur de la notion de donnée personnelle⁸⁰⁶, laisse clairement à désirer, l'adresse IP, plus globalement les données techniques d'identification reçoivent le qualificatif de donnée personnelle sous prétexte qu'elles permettent de rendre une personne indirectement identifiable, et identifiée par recoupement d'informations. Or, lorsque l'on sait qu'un fournisseur d'accès à Internet peut attribuer la même adresse IP à plusieurs abonnés, ce rapprochement à la donnée personnelle laisse encore planer beaucoup d'incertitudes⁸⁰⁷.

B. Les données de connexion: des données devenues personnelles au vu de la surveillance diffuse

⁸⁰⁶ Le règlement européen 2016/679 du 27 avril 2016 abrogeant la directive européenne de 1995 reprend quasiment la même définition de la donnée personnelle que dans le cadre de la directive. Il dispose en effet qu'une donnée personnelle s'entend de « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Le règlement ajoute ici la notion d'identifiant en ligne en tant qu'élément permettant l'identification d'une personne, ce qui fait penser que le législateur européen vise l'adresse IP.

⁸⁰⁷ Sophie Lalande écrivait en 2003 que: « l'adresse IP n'est pas l'adresse d'une personne physique mais l'adresse du réseau local de la machine d'un utilisateur connectée au réseau Internet. Ainsi, chaque machine connectée directement à Internet est identifiée par une adresse IP unique. Les réseaux connectés au réseau Internet public doivent obtenir un identificateur de réseau officiel auprès de l'ICANN (The Internet Corporation for Assigned Names and Numbers) garantissant l'unicité des identificateurs de réseau IP ». In. LALANDE Sophie, *L'adresse IP de votre ordinateur: une donnée personnelle relevant du régime de protection communautaire?*, Droit-NTIC, 2003, En ligne: http://www.droit-tic.com/pdf/adr_ip.pdf (dernière consultation: 5 mars 2018). La technique d'adressage IP, ainsi compris, et la migration d'adresses de type IPv4 aux adresses de type IPv6 envisagée depuis 2016 a permis à Free d'envisager d'attribuer la même adresse IP à plusieurs abonnés. Voir en ce sens: CHAMPEAU Guillaume, *Free peut attribuer la même adresse Ip à plusieurs abonnés*, 15 février 2016, En ligne: <http://www.numerama.com/tech/145703-free-peut-attribuer-la-meme-adresse-ip-a-plusieurs-abonnes.html> (dernière consultation: 5 mars 2018)

319. Se livrant à l'expression « *d'opinions et d'impressions personnelles*⁸⁰⁸ », Jean Frayssinet écrivait en 2008 que « *l'incertitude du champ d'application, le déficit d'application effective et de conscience des enjeux, la détermination des rôles et le renforcement de l'autorité de la Commission Nationale de l'informatique et des libertés*⁸⁰⁹ » de la « *version 2004 de loi « informatique, fichiers et libertés »*⁸¹⁰ ». Concernant le risque de rétrécissement du champ d'application de la loi informatique et libertés, il écrivait alors que « *de manière paradoxale, la « version 2004 » de la loi « Informatique, fichiers et libertés », apparaît comme déjà datée et mal adaptée aux réalités. Le présent et l'avenir paraissent considérés dans le rétroviseur: on cherche à faire entrer les réalités nouvelles dans le cadre d'une situation dépassée*⁸¹¹ ».

320. Plus que de simples réflexions personnelles, la critique de la loi informatique et libertés opérée par Frayssinet est empreinte de clairvoyance. Dans cet article, Frayssinet décrivait avec force et prophétisme l'ensemble des problèmes que pose la notion de donnée personnelle de nos jours. Il écrivait ainsi à propos de « *l'incertitude de la définition du concept de données personnelles au sens de l'article 2, alinéa 2 de la loi, appliquée notamment au numéro IP et à tous les identifiants de la même sorte*⁸¹² ». Poursuivant son analyse en s'appuyant sur le contentieux lié à l'adresse IP⁸¹³, l'auteur s'interrogeait alors: « *faut-il tenir le même raisonnement à propos de numéros de téléphone fixe ou mobile, du numéro d'immatriculation d'un véhicule, des données ou des messages indésirés (spam) ?; faut-il considérer qu'on s'adresse à une machine (avec quel intérêt ?) ou qu'on vise une personne qui par présomption est d'abord l'abonné ou l'utilisateur principal ? Où passe la ligne séparant données personnelles et non personnelles ? Faut-il introduire de nouveaux critères en dehors de ceux prévus par la loi comme la finalité d'usage, le niveau de risque pour les droits et libertés ? Va-t-on vers des données mixtes à statut juridique fluctuant qui seraient des données non personnelles lors de la collecte et pour certains usages et qui deviendraient personnelles lorsque, même indirectement, elles pourraient être appliquées à une personne identifiée ou identifiable ? Y-a -t-il des données personnelles latentes impliquant la distinction entre données personnelles et données personnalisées ? Quel est alors le statut juridique*

⁸⁰⁸ FRAYSSINET Jean, « Trente ans après la loi Informatique et libertés se cherche encore », *Lamy Droit de l'immatériel*, dossier spécial « les trente ans de la loi Informatique et libertés », n°34, janvier 2008, pp. 69-73, p. 69

⁸⁰⁹ Ibid.

⁸¹⁰ Ibid.

⁸¹¹ Ibid

⁸¹² Ibid.

⁸¹³ Spécialement les arrêts de la Cour d'Appel de Paris de 2007

des données de connexion, de traçabilité et autres « fichiers logs » ?⁸¹⁴ ». L'ensemble des questionnements posés par Frayssinet en 2008 prennent tout leur sens à la lumière des révélations issues de l'affaire Prism, et spécialement à la lumière du concept de métadonnées (1) mis au jour par Snowden. Cette dernière est aujourd'hui reconnue comme une donnée à caractère personnel (2).

1. La métadonnée: une donnée de connexion

321. A la suite des révélations de l'affaire Snowden, le monde découvre la notion de métadonnées. Les journalistes s'emparent du sujet, et vont même jusqu'à nous expliquer « *en patates comment les métadonnées permettent de vous (nous) surveiller*⁸¹⁵ ». En éclairage à ces explications, les journalistes déclarent « *qu'ils s'agissent de la surveillance massive orchestrée par la NSA, l'agence du renseignement américaine, ou des nouveaux outils dont entend se doter le gouvernement français avec le récent projet de loi sur le renseignement, un mot revient systématiquement dans les débats: « métadonnées ». En quoi consistent exactement ces métadonnées ? Que peuvent-elles dévoiler sur le quotidien de chacun ?⁸¹⁶ ». Le juriste n'est quant à lui pas vraiment surpris. Les métadonnées appartiennent en réalité au concept vague mais consacré par le législateur européen des données de connexion. Ce dernier est délicat à définir du fait d'une réalité technologique en constante évolution. Les termes employés pour désigner la donnée de connexion varient au gré des législations sécuritaires et des possibilités techniques. Ainsi, les traces, les logs, les données de journalisation, les métadonnées, les données de trafic ou encore les données techniques semblent être des synonymes au concept de données de connexion.*

322. A la lumière de la directive 2002/58/CE du Parlement européen et du conseil du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques⁸¹⁷, et de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans

⁸¹⁴ FRAYSSINET, Op. Cit. p. 70.

⁸¹⁵ VIDBERG Martin, CLAIROUIN Olivier, *Comment les métadonnées permettent de vous surveiller (expliqué en patates)*, Lemonde.fr, 15 juin 2015, En ligne: http://www.lemonde.fr/pixels/video/2015/06/15/comment-les-metadonnees-permettent-de-vous-surveiller-explique-en-patates_4654461_4408996.html (dernière consultation: 5 mars 2018)

⁸¹⁶ Ibid.

⁸¹⁷ Directive 2002/58/CE du Parlement européen et du conseil du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive vie privée et communications électroniques), JOCE L 201/37 du 31 juillet 2002, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0058&from=FR> (dernière consultation: 5 mars 2018)

le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication modifiant la directive 2002/58/CE⁸¹⁸, la donnée de connexion paraît en effet recouvrir l'ensemble des termes précédemment évoqués et spécialement les données relatives au trafic, les données de localisation, les métadonnées, les logs. Ainsi, la directive de 2002 décrit la donnée de localisation et la donnée relative au trafic comme suit: « (14) Par «données de localisation», on peut entendre la latitude, la longitude et l'altitude du lieu où se trouve l'équipement terminal de l'utilisateur, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée. (15) Une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau⁸¹⁹ ».

323. La directive de 2006 présente, quant à elle, la donnée de connexion comme suit: « la présente directive ne porte que sur les données générées ou traitées par suite d'une communication ou d'un service de communication et non sur le contenu proprement dit des informations communiquées. Les données devraient être conservées de manière à éviter qu'elles ne soient conservées plus d'une fois. Les données générées ou traitées, lors de la fourniture des services de communications concernés, concernent uniquement les données qui sont accessibles. En particulier, s'agissant de la conservation des données concernant le courrier électronique par l'internet et la téléphonie par l'internet, l'obligation de conserver les données peut ne s'appliquer qu'à l'égard des

⁸¹⁸ Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication modifiant la directive 2002/58/CE, JOUE L 105/54 du 13 avril 2006, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32006L0024&from=FR> (dernière consultation: 5 mars 2018)

⁸¹⁹ Directive de 2002 précitée point 14 et 15

*données émanant des propres services des opérateurs ou des fournisseurs de réseau*⁸²⁰ ».

2. La qualification de la métadonnée en tant que donnée à caractère personnel

324. Suite à l'ampleur des problématiques révélés par Snowden face aux potentialités de la surveillance de masse, le groupe de l'article 29 s'est prononcé sur « *la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale*⁸²¹ » et plus particulièrement sur le concept de métadonnées, ainsi que son statut juridique. Les premières lignes de l'avis du Groupe 29 sont alors particulièrement éclairantes. Concernant les métadonnées, le Groupe 29 écrit que « *pour évaluer l'ampleur d'éventuelles infractions aux règles de protection des données, il convient tout d'abord de préciser clairement ce dont il s'agit. Les représentants des gouvernements se réfèrent souvent à la collecte de métadonnées, en sous-entendant que ce processus a une portée moindre que la collecte de contenus. Or, ce n'est pas exact. Les métadonnées sont toutes les données relatives à une communication, à l'exception du contenu même de la conversation*⁸²² ». Et d'ajouter: « *Leur analyse peut révéler des données sensibles à propos des personnes concernées, par exemple parce que certains numéros d'information liés à des centres médicaux ou religieux sont composés. Comme la Cour européenne des droits de l'homme l'a déjà indiqué dans l'affaire Malone*⁸²³, le traitement des métadonnées, en l'occurrence le «comptage», comporte des informations qui «font partie intégrante des communications téléphoniques. [...] Les révéler à la police sans l'accord de l'abonné porte donc aussi atteinte à un droit consacré par l'article 8». La Cour a maintenu cette position au fil des ans⁸²⁴ ».

325. En réalité, les métadonnées révèlent bien plus d'informations sur les individus que le

⁸²⁰ Directive de 2006 précitée point 13

⁸²¹ Groupe de travail « article 29 » sur la protection des données, *Avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale*, adopté le 10 avril 2014, 819/14/FR, WP 215, En ligne: <http://www.dataprotection.ro/servlet/ViewDocument?id=1287>

⁸²² Ibid. p. 5.

⁸²³ CEDH, n° 8691/79, 2 août 1984, Malone contre Royaume-Uni

⁸²⁴ Op. Cit. p. 5

contenu même de leurs communications⁸²⁵. C'est d'ailleurs pour cette raison que le statut juridique des données de connexion est aussi important. Une localisation, un horaire d'appel, un log peuvent être beaucoup plus « parlant » qu'un message. Se limitant à citer la définition de la donnée personnelle au sens de la directive 95/46/CE, et 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, l'avis du Groupe 29 déclare timidement que contrairement à d'autres pays, en Europe, « *les métadonnées sont considérées comme des données à caractère personnel qu'il convient de protéger*⁸²⁶ ». Face à cet avis lacunaire, il faut alors nécessairement se tourner vers deux arrêts rendus par la Cour de Justice de l'Union Européenne, l'un en 2014, l'autre en 2016. Dans son arrêt rendu dans deux affaires jointes, la Cour de Justice de l'Union Européenne est venue invalider en 2014⁸²⁷ la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques. Cette décision envoie un signal fort de l'institution envers la protection du droit fondamental au respect de la vie privée. Cette invalidation vient frapper les dispositions qui concernaient l'obligation de conservation de certaines informations sur le trafic et la localisation des internautes dans le but de rechercher et de constater les infractions graves.

326. Pour cela, la Cour se fonde sur le fait que l'obligation de conservation s'applique de manière générale sans exiger de lien entre la personne et un risque d'infraction⁸²⁸ ; qu'elle ne fixe aucune limitation à l'utilisation de ces données⁸²⁹ ; qu'elle n'établit aucun lien entre la durée de la

⁸²⁵ S'appuyant sur une déclaration écrite du professeur Felten devant le tribunal de district des Etats-Unis pour le district sud de New-York, dans le cadre de l'affaire n°13-3994 opposant l'American Civil Liberties Union (Aclu) et le Directeur du Renseignement Américain James Clapper, le Groupe 29 déclare qu'il est « *particulièrement important de souligner que les métadonnées donnent fréquemment des informations plus facilement que ne le font les contenus réels de nos communications. Du fait de leur nature structurée, elles sont faciles à regrouper et à analyser. Des outils informatiques sophistiqués permettent d'analyser de grands ensembles de données en vue de déterminer des relations et des caractéristiques intégrées, y compris des informations personnelles, des habitudes et des comportements. Ce n'est pas le cas pour les conversations, qui peuvent avoir lieu sous n'importe quelle forme ou dans n'importe quelle langue* » (p. 5). Il est à préciser ici que la décision pour cette affaire fut rendu par la United States Court of Appeals for the Second Circuit, le 7 mai 2015, et statue en faveur de l'ACLU. In. United States Court of Appeals for the second circuit, ACLU v/ Clapper, 7 mai 2015, Case 14-42, Document 168-1, En ligne: <https://www.eff.org/document/aclu-v-clapper-second-circuit-opinion> (dernière consultation: 5 mars 2018)

⁸²⁶ Op. Cit. p. 5

⁸²⁷ CJUE, Affaires jointes C-293/12 et C-594/12, Arrêt de la Cour (grande chambre), du 8 Avril 2014, publié au Recueil numérique (Recueil général) Digital Rights Ireland Ltd Contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., Demandes de décision préjudicielle, introduites par la High Court (Irlande) et le Verfassungsrichtsof, En ligne: <http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-293/12> (dernière consultation: 5 mars 2018)

⁸²⁸ Ibid. point 57 et 58

⁸²⁹ Ibid. point 59.

conservation et la nature de l'infraction⁸³⁰ ; que la durée de conservation pouvant aller jusqu'à deux ans est disproportionnée⁸³¹ ; et enfin, qu'elle n'impose pas le stockage de ces données sur le sol Européen⁸³². Plus précisément, elle constate que « *la conservation des données aux fins de leur accès éventuel par les autorités nationales compétentes, telle que prévue par la directive 2006/24, concerne de manière directe et spécifique la vie privée et, ainsi, les droits garantis par l'article 7 de la Charte. En outre, une telle conservation des données relève également de l'article 8 de celle-ci en raison du fait qu'elle constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de cet article (arrêt Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 47)*⁸³³ ».

327. Par la reconnaissance du traitement opéré par les fournisseurs d'accès, les juges européens reconnaissent ici le caractère personnel des métadonnées et des données de connexion. Les juges ajoutent également que « *pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence (voir, en ce sens, arrêt Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 75). Il en résulte que l'obligation imposée par les articles 3 et 6 de la directive 2006/24 aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications, telles que celles visées à l'article 5 de cette directive, constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte. En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Leander c. Suède, 26 mars 1987, série A no 116, § 48; Rotaru c. Roumanie [GC], no 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), no 54934/00, § 79, CEDH 2006-XI). Ainsi, les articles 4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits*

⁸³⁰ Ibid.

⁸³¹ Ibid. point 63.

⁸³² Ibid. point 68

⁸³³ Ibid. point 29

garantis par l'article 7 de la Charte.⁸³⁴ ». L'invalidation de cette directive a alors enclenché en Europe la suspension de l'application et la censure des lois imposant aux opérateurs de télécommunications de conserver les métadonnées de toutes les communications et connexions de leurs abonnés. C'est le cas notamment pour l'Irlande, l'Autriche, la Roumanie, la Slovaquie, la Slovénie, les Pays-Bas et la Bulgarie⁸³⁵. En France, cette directive touche le dispositif de la loi du 9 juillet 2004 dont les mentions figurent aux articles L.34-1 et suivants et R.10-13 du code des postes et communications électroniques. Les distinctions sont principalement liées au fait que la conservation est limitée à la recherche, la constatation et la poursuite des infractions pénales ; que la durée de conservation est limitée à un an pour tous les cas ; et que son accès est réservé aux autorités identifiées. Plus généralement, l'invalidation de la directive et la reconnaissance par la CJUE des données de connexion en tant que données à caractère personnel touchent l'ensemble des dispositifs sécuritaires issus de la loi sur le Renseignement, mais également de la loi sur la surveillance internationale des communications électroniques. Alors que le juge européen envoie dans le cadre de l'arrêt de 2014 un signal fort contre la surveillance de masse, la France maintient en effet ses positions en faveur de ce type de surveillance⁸³⁶.

Paragraphe 2. La délicate détermination du champ d'application de la loi face à la notion de traitement de données personnelles dans le cadre de la surveillance diffuse

328. Si la notion de données à caractère personnel pose des problèmes quant à l'opération de qualification de ce type de données, le concept de traitement de données à caractère personnel n'est pas non plus sans poser des problèmes d'interprétation, de définition, et de détermination de son champ d'application. Pour rappel, la loi informatique et libertés s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données personnelles contenues ou appelées à figurer dans des fichiers. L'article 2 de cette dernière déclare que « *constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification,*

⁸³⁴ Ibid. Points 33, 34 et 35

⁸³⁵ Voir en ce sens: CHAMPEAU Guillaume, *Données de connexion: la France « ne pourra pas continuer à ignorer » la CJUE*, 12 mars 2015, En ligne: <http://www.numerama.com/magazine/32470-donnees-de-connexion-la-france-ne-pourra-pas-continuer-a-ignorer-la-cjue.html> (dernière consultation: 5 mars 2018)

⁸³⁶ Nous évoquerons plus en détail cet élément par la suite de notre analyse

*l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction*⁸³⁷ ».

329. Ainsi que l'écrivait Jean Frayssinet, « *la seconde notion essentielle pour la détermination du champ d'application de la loi de 1978, est celle de traitement, qu'il soit manuel ou automatisé. Elle pose aussi des problèmes de définition et de détermination de la portée des dispositions de la loi au regard des évolutions des techniques et des usages. (...). Comme pour la notion de donnée personnelle, la notion de traitement, pourtant largement définie par la directive de 1995 et la loi modifiée de 1978, donne encore lieu à des errements interprétatifs lourds de conséquence. On n'est plus à l'époque de l'existence des seuls fichiers segmentés à finalité déterminée. Les concepts de base de la loi doivent pouvoir s'appliquer aux activités de Google et autre MSN ou Gmail, aux moteurs de recherche de personnes comme Spock ou Facebook, aux nouvelles formes de profilage, de scoring et de traçabilité (RFID et autres, nanotechnologies...)*⁸³⁸ ». L'affirmation de Frayssinet selon laquelle nous ne sommes plus « *à l'époque des seuls fichiers segmentés à finalité déterminée* » reflète entièrement le problème de la surveillance diffuse (B). L'ensemble des décisions de la Cour de Justice de l'Union Européenne, que ce soit au regard des concepts liés aux traitements de données d'identification technique (adresse IP, données de trafic) ou à ceux liés aux données de connexion - spécialement aux métadonnées - (A), tendent d'ailleurs à confirmer ce propos.

A. Les traitements de métadonnées: analyse de l'arrêt Tele2 Sverige rendu par la CJUE en 2016

330. Le caractère technique des données de connexion, qu'elle soit de localisation, de date, qu'elles permettent de retrouver et d'identifier la source d'une communication, ou de comprendre

⁸³⁷ Article 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée. Le règlement européen 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 du 27 avril 2016 n'apporte que peu de nouveautés dans la définition du traitement puisque son article 4 le définit comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

⁸³⁸ Op. Cit. p. 70.

quel matériel est utilisé pour réaliser cette communication, reste assez problématique dans la caractérisation de ce type de données. La même logique se retrouve dans le cadre de la notion d'adresse IP⁸³⁹, ou plus globalement dans le cadre des données de trafic. Bien que contestables dans les faits puisqu'à nouveau une adresse IP, par exemple, identifie une machine, et non une personne, les décisions rendus par la Cour de justice de l'Union Européenne ont au moins le mérite d'illustrer le fait que la collecte et le traitement de données à certaines fins suscitent l'ambition de les utiliser à plus large échelle. Il semble utile de rappeler que la communication des données de trafic était, avant ces décisions, strictement encadrée et limitée aux poursuites judiciaires de droit pénal, à la protection de l'ordre public et à la défense nationale, et non aux actions de droit civil. Le même raisonnement s'applique dans le cadre de l'arrêt Digital Right Ireland de 2014, et Tele2 Sverige de 2016 rendus par la CJUE. Pour rappel, dans l'arrêt de 2014 les juges se fondent sur le fait que l'obligation de conservation s'applique de manière générale sans exiger de lien entre la personne et un risque d'infraction⁸⁴⁰ ; qu'elle ne fixe aucune limitation à l'utilisation de ces données⁸⁴¹ ; qu'elle n'établit aucun lien entre la durée de la conservation et la nature de l'infraction⁸⁴² ; que la durée de conservation pouvant aller jusqu'à deux ans est disproportionnée⁸⁴³ ; et enfin, qu'elle n'impose pas le stockage de ces données sur le sol Européen⁸⁴⁴.

331. En 2016, la CJUE renouvelle sa position dans deux affaires jointes portant à nouveau sur l'obligation générale imposée aux fournisseurs de services de télécommunications de conserver des données relatives aux communications électroniques⁸⁴⁵. Saisie par voie préjudicielle par des juridictions d'appel suédoise et britannique, la CJUE était invitée à répondre à la question de savoir si les régimes nationaux qui imposent aux fournisseurs une obligation générale de conservation des données sont compatibles avec le droit de l'Union. Elle a pu par la même préciser l'interprétation à apporter dans un contexte national à l'arrêt de 2004. Les juges européens déclarent ainsi que

⁸³⁹ Arrêts précités de la CJUE Promusicae de 2008, et Bonnier Audio AB de 2012.

⁸⁴⁰ Ibid. point 57 et 58

⁸⁴¹ Ibid. point 59.

⁸⁴² Ibid.

⁸⁴³ Ibid. point 63.

⁸⁴⁴ Ibid. point 68

⁸⁴⁵ CJUE, Affaires jointes C-203/15 et C-698/15, Arrêt de la Cour (grande chambre) du 21 décembre 2016, publié au Recueil numérique (Recueil général), Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a., Demandes de décision préjudicielle, introduite par le Kammarrätten i Stockholm et la Court of Appeal (England and Wales) (Civil Division), En ligne: <http://curia.europa.eu/juris/liste.jsf?num=C-203/15> (dernière consultation: 5 mars 2018)

« prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 27). En particulier, ces données fournissent les moyens d'établir, ainsi que l'a relevé M. l'avocat général aux points 253, 254 et 257 à 259 de ses conclusions, le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications⁸⁴⁶ ».

332. Et d'ajouter également que « l'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 37). Même si une telle réglementation n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel desdits droits (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 39), la conservation des données relatives au trafic et des données de localisation pourrait toutefois avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt *Digital Rights*, point 28)⁸⁴⁷ ». Enfin la Cour déclare que la conservation des données instituée par la directive de 2002 constitue, non pas la règle, mais bien une exception⁸⁴⁸. L'ensemble de cette jurisprudence tend donc à reconnaître dans l'activité de conservation des métadonnées, et plus globalement, des données de connexion, un traitement de données à caractère personnel qui 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

⁸⁴⁶ Ibid. point 99

⁸⁴⁷ Ibid. points 101 et 102.

⁸⁴⁸ Ibid. point 104

*communication électronique*⁸⁴⁹ ».

B. L'interconnexion et l'interopérabilité des données comme réel problème posé par la surveillance diffuse

333. Bien qu'il soit heureux d'avoir une vision élargie de la notion de donnée personnelle, les exemples liés à l'adresse IP et aux métadonnées montrent à quel point il est délicat pour le juriste de percevoir l'ensemble des possibilités qu'offrent les nouvelles technologies et que sous-tendent les traitements, les interconnexions, l'interopérabilité au coeur même de la surveillance diffuse (1). Ces éléments participent d'un déficit d'effectivité globale des premières législations informatiques et libertés (2)

1. L'interconnexion et l'interopérabilité des données personnelles et non personnelles au coeur de la surveillance diffuse

334. C'est bien la notion de traitement qui pose le plus de problème, et tend à conférer à des informations techniques le statut de données personnelles. Dans les faits, prises isolément, les données de connexion, qu'elles soient de localisation, de précision d'une date, du matériel utilisé pour réaliser la communication, et/ou les données de trafic restent des données techniques. Et c'est bien comme cela qu'il faut comprendre le point 99 précité de l'arrêt Tele2 Sverige rendu en 2016. Les juges précisent bien en effet que « *prises dans leur ensemble, ces données sont susceptibles de permettre des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées*⁸⁵⁰ ». Si l'on examine la décision du juge européen, et spécifiquement ce point a contrario, cela démontre bien que si ces données étaient compartimentées, isolées, fragmentées, sans possibilité d'interconnexion, elles constitueraient purement et simplement des données techniques. Dans l'ensemble des décisions de la CJUE précitées⁸⁵¹, le juge européen motive sa décision en se fondant sur la notion de traitement. Dans les arrêts Promusicae et Bonnier Audio, le juge déclare que la communication sollicitée par les ayants droits ou les titulaires de propriété

⁸⁴⁹ Ibid. Décision de la cour point 1.

⁸⁵⁰ Op. Cit.

⁸⁵¹ Promusicae, Bonnier Audio e.a., Digital Rights Ireland, Tele2 Sverige

intellectuelle des informations « *constitue un traitement de données à caractère personnel*⁸⁵² ». Dans les deux arrêts précités concernant les données de connexion, le juge ne vient pas apposer clairement le statut de données personnel aux métadonnées. Il vient, là aussi, au travers de la notion de traitement reconnaître le caractère personnel de ces données. En effet, dans l'arrêt Digital Rights Ireland de 2014 et Tele2 Sverige de 2016, le juge européen se positionne d'abord sur l'imposition de conservation des données imposées aux fournisseurs de services de communications électroniques. En 2014, il déclare ainsi que « *la conservation des données aux fins de leur accès éventuel par les autorités nationales compétente (...) constitue un traitement de données à caractère personnel au sens de cet article et doit nécessairement satisfaire aux exigences de protection des données découlant de cet article*⁸⁵³ ». Et d'ajouter de manière maladroite: « *pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence*⁸⁵⁴ ». Bien que l'on ne saisisse que peu la nature sensible de ces informations décrite par la CJUE, on sait par contre ici que c'est bien la conservation de ces données, et donc leur traitement qui pose problème, et qui confère leur caractère personnel à ces informations.

335. De la même manière, dans l'arrêt rendu en 2016, le juge européen déclare que « *relève, en particulier, de ce champ d'application une mesure législative, telle que celle en cause au principal, qui impose à ces fournisseurs de conserver les données relatives au trafic et les données de localisation, puisqu'une telle activité implique nécessairement un traitement, par ceux-ci, de données à caractère personnel*⁸⁵⁵ ». Et de compléter sa logique de manière très précise en déclarant que « *dans ces conditions, une mesure législative par laquelle un État membre impose, sur le fondement de l'article 15, paragraphe 1, de la directive 2002/58, aux fournisseurs de services de communications électroniques, aux fins mentionnées par cette disposition, d'accorder aux autorités nationales, dans les conditions prévues par une telle mesure, l'accès aux données conservées par lesdits fournisseurs porte sur des traitements de données à caractère personnel par ces derniers, traitements qui relèvent du champ d'application de cette directive*⁸⁵⁶ ». La conservation des

⁸⁵² Op. Cit. Et spécialement le point 45 de l'arrêt Promusicae, et les points 51 et 52 de l'arrêt Bonnier Audio e.a.

⁸⁵³ Op. Cit. point 29

⁸⁵⁴ Op. Cit. Point 33.

⁸⁵⁵ Arrêt de la CJUE Tele2 Sverige de 2016 précité, point 75

⁸⁵⁶ Ibid. Point 78.

données, étant par définition un traitement, il semble que dans la logique de l'analyse des juges européens cela suffit à conférer à ces données leur caractère personnel. D'autant plus lorsque ces données sont interconnectées avec des bases de données client⁸⁵⁷. Et d'autant plus dans le contexte de la découverte d'une surveillance généralisée.

336. L'ensemble des arrêts de la Cour de Justice de l'Union Européenne illustre parfaitement la problématique plus globale de la surveillance diffuse: le fait que la conservation de données à certaines fins suscite l'envie de les utiliser à d'autres fins, et à plus large échelle. C'est d'ailleurs ce que cherche à faire comprendre le juge européen dans l'arrêt de 2016 lorsqu'il déclare « *qu'il convient de relever, d'une part, qu'une telle réglementation a pour effet, eu égard à ses caractéristiques décrites au point 97 du présent arrêt, que la conservation des données relatives au trafic et des données de localisation est la règle, alors que le système mis en place par la directive 2002/58 exige que cette conservation des données soit l'exception*⁸⁵⁸ ».

2. Une volonté d'élargissement constante des premières législations informatiques et libertés comme facteur de leur manque d'effectivité

337. L'exemple de la métadonnée reflète parfaitement de l'incompréhension totale des possibilités offertes par les nouveaux usages technologiques, et par les discours de légitimation liés, par exemple, à la conservation des données dans un but sécuritaire ou de prévention. Ainsi que le démontrait Frayssinet avec raison « *si le risque de rétrécissement du champ d'application de la loi de 1978 soulève l'inquiétude, l'étendue de ce champ, paradoxalement, amène à s'interroger sur l'effectivité du respect des dispositions législatives. La connaissance du terrain, secteur public comme secteur privé, oblige de constater que les fichiers manuels et les traitements automatisés de données personnelles qui sont, à des degrés variables, dans l'illégalité sont, et de loin, beaucoup plus nombreux que ceux qui respectent les règles de la loi. L'extrême faiblesse des contentieux civils, administratifs et pénaux, la modération des sanctions intervenues, le niveau de méconnaissance dans tous les milieux juridiques des enjeux et des utilisations possibles d'une législation riche et pleines de ressources par rapport aux réalités affecte la crédibilité de la*

⁸⁵⁷ On pense notamment ici à l'adresse IP

⁸⁵⁸ Ibid. p. 104

législation « Informatique, fichiers et libertés ».⁸⁵⁹ ».

338. Ainsi, on pourrait, en plus des notions de données personnelles et de traitement, souligner d'autres incertitudes posées récemment par certaines dispositions de la loi Informatiques et Libertés et de la Directive de 95. Par exemple, l'article 8 de la loi Informatique et Libertés concernant les données sensibles⁸⁶⁰, face aux études statistiques sur la mesure de la diversité, de la discrimination et de l'intégration⁸⁶¹ jugées inconstitutionnelles en 2007⁸⁶². Le rôle de la CNIL doit également être soulevée comme participant d'une confusion des genres. Ainsi que le notait Frayssinet, *« la CNIL et ses représentants contribuent parfois à la confusion. Son président dans les médias et son site tendent à faire croire que l'institution et la loi de 1978 modifiée ont dans leur champ de compétence la vidéosurveillance. Or, celle-ci relève de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité modifiée par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers. Seuls les enregistrements visuels de vidéosurveillance utilisés dans des traitements automatisés en contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement des personnes physiques sont soumis à la loi de 1978 modifiée. Dans la pratique, le cas est très rare comme peuvent en témoigner les commissions départementales chargées de donner un avis aux Préfets qui autorisent l'installation d'un système de vidéosurveillance. C'est le ministre de l'Intérieur de l'époque, M. Charles Pasqua, qui s'était opposé fortement à l'acceptation d'une compétence large de la CNIL en la matière⁸⁶³ »*. L'évolution constante de la doctrine de la CNIL, bien qu'heureuse, participe à rendre délicate les opérations de qualification juridique des données et

⁸⁵⁹ Op. Cit. p. 70 - 71

⁸⁶⁰ La CNIL a dû repenser sa doctrine concernant les études sur la diversité. Voir en ce sens: CNIL, Statistiques ethniques, quel cadre légal, 7 mai 2015, En ligne: <https://www.cnil.fr/en/node/15780> (dernière consultation: 5 mars 2018)

⁸⁶¹ Ces études étaient envisagées (et soutenues par la CNIL) dans le cadre de l'article 63 de la loi n° 2007-1631 du 20 novembre 2007 relative à la maîtrise de l'immigration, à l'intégration et à l'asile, JORF n° 270 du 21 novembre 2007, page 18993, texte n°1

⁸⁶² Décision n°2007-557 DC du 15 novembre 2007, Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2007/2007-557-dc/decision-n-2007-557-dc-du-15-novembre-2007.1183.html> (dernière consultation: 5 mars 2018)

⁸⁶³ Op. Cit. p. 70

des traitements. La même logique a été à l'oeuvre dans le cadre de la biométrie par exemple⁸⁶⁴.

339. Enfin, (et) à l'image des déclarations des juges européens dans l'arrêt de 2016, on rappellera que c'est à l'Etat qu'il revient de garantir le contrôle effectif du niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel⁸⁶⁵. Or, comment faire en sorte d'obtenir un contrôle efficace quant aux droits fondamentaux et aux libertés des citoyens alors que l'Etat, dans le cadre de la surveillance diffuse, est aussi décisionnaire du niveau de sécurité approprié ? Dans une société où la gouvernance par la peur, le contrôle social attentionnel et la gouvernementalité algorithmique sont les nouvelles manières de gouverner les citoyens est-il encore clairement possible d'obtenir un niveau de protection élevé des données à caractère personnel et de la vie privée de ces derniers ? L'ensemble de ces interrogations est au coeur des enjeux de la surveillance diffuse comme en atteste les arrêts de la CJUE de 2014 et de 2016. Rendu dans le contexte des révélations de l'affaire Snowden, et donc des programmes de surveillance de masse, ces arrêts démontrent l'importance du rôle du juge dans la garantie des droits fondamentaux. La prohibition tacite de la surveillance de masse qu'engendre ces arrêts doit être soulignée. Il n'en reste pas moins que l'impact de ces décisions dans les droits nationaux, et spécialement en France, reste encore à démontrer.

340. Citons à nouveau Frayssinet en guise de conclusion qui s'étonnait et s'inquiétait que: *« trente ans après son vote, on s'interroge encore sur le champ d'application de la législation « Informatique, fichiers et libertés » alors que des données relatives à des personnes sous des formes de plus en plus variées font l'objet de traitements à finalités démultipliées dans une société caractérisée par le « tout numérique ». Cette insécurité juridique et pratique doit être rapidement*

⁸⁶⁴ Evolution de la doctrine de la CNIL par une modification de ses critères d'analyse. Avant 2004, la CNIL opérait une distinction en terme de criticité (d'intrusivité) de biométrie, selon si le dispositif se base sur une biométrie dite « à trace » ou « sans trace ». Les dispositifs biométriques « à traces » correspondent principalement aux les empreintes digitales et palmaires. Le risque de ces techniques réside dans le fait que ces traces peuvent éventuellement être capturées et reproduites à l'insu des personnes (fabrication d'un faux doigt...). A l'inverse, les dispositifs biométriques « sans traces » vont correspondre au contour de la main, au réseau veineux des doigts, au visage ou à l'iris. De par la difficulté supposée de les enregistrer sans le consentement de la personne, la CNIL les jugeait moins critiques en termes de risque pour la vie privée. A la suite des évolutions législatives et technologiques, une nouvelle doctrine s'est dessinée. La distinction s'appuie aujourd'hui sur trois catégories différentes : la biométrie de sécurité, la biométrie de service, les expérimentations.

⁸⁶⁵ Le point 123 de l'arrêt Tele2 Sverige déclare avec précision que: *« en tout état de cause, les États membres doivent garantir le contrôle, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel, un tel contrôle étant explicitement exigé à l'article 8, paragraphe 3, de la Charte et constituant, conformément à la jurisprudence constante de la Cour, un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel. S'il en était autrement, les personnes dont les données à caractère personnel ont été conservées seraient privées du droit, garanti à l'article 8, paragraphes 1 et 3, de la Charte, de saisir les autorités nationales de contrôle d'une demande aux fins de la protection de leurs données ».*

corrigée par le législateur et le juge suprême faute de quoi le cours de la loi risque de changer de lit, le juge venant détourner l'intention du législateur européen et français en amoindrissant le niveau de protection des droits et libertés individuels⁸⁶⁶ »

Section 2: Le constat nécessaire du déficit d'effectivité des premières législations informatiques et libertés tant au niveau du régime juridique de protection qu'au niveau international

341. La surveillance diffuse, et le tout numérique qu'elle implique, pour des objectifs de sécurité ou de bien-être, engendre un déficit de conscience de ses enjeux. Les discours en pagaille sur l'idéologie du « rien à cacher, rien à se reprocher » témoigne parfaitement de cette affirmation. Pourtant, que ce soit dans l'organisation de la traçabilité des individus, et dans la réduction de l'individu à une trace, la surveillance diffuse est dangereuse en terme de libertés et de droits fondamentaux. Ce déficit de conscience des enjeux de la surveillance favorise le déficit d'effectivité de la loi informatique et libertés, et par extension de la Directive de 95, et de la notion juridique de vie privée.

342. A l'appui de ce propos, il faut interroger les principes fondamentaux de la protection des données personnelles et les mettre en question face à la surveillance diffuse (paragraphe 1). Aussi, la conception du droit des données personnelles par référence au concept juridique de vie privée, bien qu'adaptée vis à vis de l'idéologie sécuritaire qu'emporte la surveillance, semble totalement inefficace face à l'ampleur des possibilités offertes par les nouveaux usages technologiques. Le principe de proportionnalité est ici pointé du doigt. Son application, permettant la balance des intérêts du traitement de données face aux droits fondamentaux, manque d'efficacité et de pertinence dans une société où l'idéologie sécuritaire gagne de plus en plus de terrain (paragraphe 2). Partant de l'ensemble de ces constats, il semble qu'il faille conclure au manque d'efficacité réelle des termes juridiques de vie privée, et de données personnelles.

⁸⁶⁶ Op. Cit. p. 70.

Paragraphe 1: Le respect des principes fondamentaux de la protection des données personnelles en question

343. En 2008, le Professeur Frayssinet décrivait le déficit d'effectivité de la loi informatique et libertés en ces termes: « *pourquoi appliquer un texte contraignant si le risque de se faire sanctionner par les juges, les médias, l'opinion publique reste très faible ? Le respect des principes d'une collecte et d'un traitement loyal et licite pour des finalités déterminées et une durée limitée, du consentement de l'information préalable de la personne concernée, du droit d'opposition, des règles applicables aux flux transfrontières de données, des formalités préalables à accomplir auprès de la CNIL est très relatif dans les administrations, comme dans les entreprises. Inquiétante aussi la faiblesse étonnante de l'exercice du droit d'accès aux données personnelles traitées, du droit de contestation, du droit d'opposition. Trente ans après son vote, on ne peut pas dire que les Français se sont accaparés la loi de 1978⁸⁶⁷ ».*

344. Les constats de Jean Frayssinet sont toujours autant d'actualité. Pour preuve, on s'attachera ici dans un premier temps à comprendre la délicate application des principes issus de la loi informatique et libertés décrits par l'auteur (A). Aussi, à l'international, la récente remise en question du Safe Harbor par la Cour de Justice de l'Union Européenne⁸⁶⁸, tend à démontrer l'inadéquation des règles applicables aux flux transfrontières de données (B), et donc plus globalement, à démontrer du déficit d'effectivité de la protection des données personnelles.

A. L'adéquation relative des principes fondamentaux de la protection des données personnelles à la surveillance diffuse

345. Au titre des principes fondamentaux de la protection des données personnelles, deux points semblent devoir être analysés. Ainsi le principe de finalité (1) et le recueil du consentement (2) semblent assez problématique au vu des objectifs poursuivis par la surveillance diffuse

⁸⁶⁷ FRAYSSINET Jean, Op. Cit., p. 71

⁸⁶⁸ CJUE, Affaire C-362/14, Arrêt de la Cour (grande chambre) du 6 octobre 2015, publié au Recueil numérique (Recueil général), Maximilian Schrems contre Data Protection Commissioner, Demande de décision préjudicielle, introduite par la High Court (Irlande), En ligne: <http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-362/14> (dernière consultation: 5 mars 2018)

1. La problématique de la finalité du traitement et la surveillance diffuse

346. Le Conseil Constitutionnel rappelle régulièrement que les exceptions au principe du respect de la vie privée doivent rester exceptionnelles. A travers sa décision du 19 janvier 2006 portant sur la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers⁸⁶⁹, le Conseil Constitutionnel a pu juger non conformes à la Constitution les exceptions mentionnées dans l'article L. 34-2 du Code des Postes et des Communications Electroniques destinées à prévenir les actes contre le terrorisme.

347. La loi du 23 janvier 2006⁸⁷⁰ permettaient un traitement automatisé de données personnelles relatives aux passagers enregistrés dans le système de contrôle de départ des compagnies aériennes. Dans sa décision, le Conseil rappelle « *qu'il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent le respect de la vie privée et la liberté d'entreprendre, respectivement protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789*⁸⁷¹ ». La doctrine s'est d'ailleurs prononcée à ce sujet, et déclare que « *sans critiquer, si peu que ce soit, la légitimité des politiques antiterroristes, les autorités de contrôle sont nécessairement amenées, devant un tel développement à s'interroger sur l'adéquation entre les objectifs poursuivis et les moyens mis en oeuvre, sur le respect rigoureux des seules finalités poursuivies*⁸⁷² ». Rappelons que la référence à la finalité servira jusqu'à la destruction des informations nominatives, puisque celles-ci ne pourront être « *traitée ultérieurement de manière incompatible avec les finalités*⁸⁷³ » initialement déterminées. A travers l'ensemble des exemples

⁸⁶⁹ Décision n°2005-532 DC du 19 janvier 2006 portant sur la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2006/2005-532-dc/decision-n-2005-532-dc-du-19-janvier-2006.979.html> (dernière consultation: 5 mars 2018)

⁸⁷⁰ 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, JORF n° 0020 du 24 janvier 2006, texte n°1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124&categorieLien=id> (dernière consultation: 5 mars 2018)

⁸⁷¹ Op. Cit. Considérant n° 9

⁸⁷² Voir en ce sens: LECLERCQ Pierre, « Un an d'application de la législation Informatique et Libertés », *Communication, Commerce électronique*, Octobre 2007, p. 29.

⁸⁷³ Article 6.2 de la loi du 6 janvier 1978

envisagés on voit bien à quel point il est délicat de concilier le respect de la vie privée d'une part, et la sécurité publique d'autre part. Sur des cas isolés, tels que par exemple le lieu de travail, la difficulté semble peu présente. Mais dans le cas de la surveillance diffuse, globale, utilisée dans sa fonction de sécurité, on voit bien que la conciliation entre le pouvoir souverain de l'Etat de garantir la sécurité par la lutte contre le terrorisme et la garantie des droits et libertés des citoyens reste délicate. Pour certains auteurs, elle relève d'un dilemme « cornélien⁸⁷⁴ ». Ainsi, Marie-Charlotte Roques-Bonnet écrit avec force: « *alors que la CNIL « ne dispose plus d'un pouvoir de contrôle sur ces fichiers dits de souveraineté », concilier deux droits inconciliables - respect de la vie privée et sécurité publique - s'avère cornélien. Il s'agit de garantir la souveraineté contre l'arbitraire. Souverainement les pouvoirs publics peuvent et doivent entreprendre de lutter contre le terrorisme. Ils ne sont néanmoins pas en droit de porter atteinte, de manière continue, aux libertés individuelles des citoyens⁸⁷⁵ ».*

348. La surveillance diffuse en ce qu'elle banalise son recours par les usages technologiques quotidiens réactive cette assertion de l'auteur de garantir la souveraineté contre l'arbitraire, et la dépasse. En 2015, Liesbet van Zoonen⁸⁷⁶ analyse les inquiétudes des citoyens liées à la vie privée. A travers des exemples tels que la gestion intelligente des déchets et la police prédictive, l'auteur démontre à quel point il est simple de passer d'une information à une donnée personnelle par truchement technologique. Ainsi concernant la gestion intelligente des déchets, l'auteur démontre que la puce placée sur la benne à déchets permet d'alerter le service de ramassage des ordures lorsque cette dernière est pleine. La puce permet de mesurer la charge de déchets et la localisation de la benne à ordures. Ces données impersonnelles sont collectées à des fins de service public. Par contre, si une carte magnétique permet à un individu, identifié par le badge, d'ouvrir la benne, on glisse progressivement vers une donnée personnelle. L'individu, étant rendu identifiable, on passe d'une donnée impersonnelle à une donnée personnelle tendant à faire fonctionner le service public. Au delà de l'usage purement étatique, la surveillance diffuse dans sa dimension marketing couple un ensemble de données qu'il n'est plus vraiment possible d'appréhender aux titres des finalités du traitement. La durée de conservation pose également problème. Dans le cadre des arrêts précités, concernant les données de connexion, métadonnées et adresse IP, montre bien que la condition de la

⁸⁷⁴ ROQUES-BONNET Marie-Charlotte, *Le droit peut-il ignorer la révolution numérique ?*, Préface de Lucien Rapp, Ouvrage publié avec le concours de la CNIL, Michalon Editions, 2010, p. 225.

⁸⁷⁵ Ibid.

⁸⁷⁶ VAN ZOONEN Liesbet, Privacy concerns in smart cities, *Government Information Quarterly*, 2016, En ligne: <http://www.sciencedirect.com/science/article/pii/S0740624X16300818> (dernière consultation: 5 mars 2018)

durée limitée est assez fluctuante, voire quasiment pas respectée. Dans l'ensemble de ces jurisprudences, c'est bien la conservation longue de ces informations qui étaient en cause.

349. Couplées aux analyses précédentes et aux mots de Jean Frayssinet, a-t-on vraiment conscience des possibilités nocives de la surveillance diffuse sur nos droits et libertés. A nouveau, la question de la garantie effective des droits et libertés dans une société de sécurité et de bien-être se limite-t-elle encore de nos jours à la seule balance entre sécurité et libertés ? La question n'est elle pas plutôt aujourd'hui dans l'équilibre entre le savoir et le pouvoir ?

2. La délicate opération de recueil du consentement

350. Les conditions de recueil du consentement préalable du sujet du traitement ont été précisées par la Commission Européenne en 2010. La Commission déclare ainsi que « *lorsqu'un consentement éclairé est exigé, les règles en vigueur prévoient que l'accord de l'intéressé sur le traitement de données à caractère personnel le concernant devrait consister dans toute manifestation de volonté, libre, spécifique et informée par laquelle il accepte ce traitement*⁸⁷⁷ ». Dans les faits, en 2010, la Commission s'inquiétait d'une garantie insuffisante quant au consentement libre et éclairé. La situation actuelle, sur ce point, ne semble guère avoir évolué. La Commission européenne poursuivait en effet son analyse en ces termes: « *Or actuellement, dans les États membres, ces conditions font l'objet d'interprétations diverses, allant de l'obligation générale d'obtenir un consentement écrit à l'acceptation d'un consentement implicite. En outre, dans un environnement en ligne – **vu l'opacité des politiques de protection de la vie privée** – les personnes ont souvent plus de difficulté à s'informer sur leurs droits et à donner un consentement éclairé. Cela est d'autant plus complexe que, dans certains cas, l'on ne voit pas clairement ce qui constituerait un consentement libre, spécifique et éclairé à un traitement de données, comme dans le domaine de la publicité comportementale en ligne où certains considèrent, mais pas d'autres, que les paramètres du navigateur de l'internaute expriment son consentement. Il conviendrait donc de clarifier les conditions du consentement de la personne concernée, afin de garantir qu'il est toujours accordé **en connaissance de cause, et de s'assurer que l'intéressé est pleinement conscient qu'il donne son autorisation et sait de quel traitement il s'agit**, conformément à l'article 8 de la Charte des droits*

⁸⁷⁷ Commission Européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Op. Cit., p. 9

*fondamentaux de l'Union européenne. La clarification des notions clés peut également favoriser les initiatives en matière d'autoréglementation visant à dégager des solutions pratiques conformes au droit de l'Union*⁸⁷⁸ ».

351. Les politiques de protection de la vie privée sont aujourd'hui toujours aussi opaques, et l'on peut douter que le citoyen, le consommateur donne toujours son autorisation en pleine conscience. Qu'il s'agisse des révélations de l'affaire Snowden, de l'absence de lecture des conditions générales d'utilisation de certains sites⁸⁷⁹, ou du pouvoir fort que les entreprises du secteur du numérique dispose à ce sujet⁸⁸⁰, l'individu est bien souvent dans l'obligation de donner son autorisation pour pouvoir utiliser pleinement des services et des applications. Ainsi, alors que de plus en plus de services et de produits technologiques fonctionnent sur la base de traitement d'informations, le client consommateur est sommé de payer le prix de l'appareil mais également de subir les modifications des conditions générales d'utilisation sous peine de ne pas pouvoir utiliser pleinement l'appareil, l'application... Lee Tien, avocat de la Fondation Electronic Frontier déclare à ce propos que: « *Les fabricants [de terminaux] peuvent évidemment faire beaucoup à ce sujet. Ils peuvent concevoir leurs systèmes en séparant plus la collecte de données de la partie fonctionnalités du produit. Il est évident que certaines fonctionnalités ne fonctionnent pas sans données, mais même alors, vous pouvez souvent choisir de stocker les données localement et de ne pas la transmettre à une quelconque société-mère. La société dans son ensemble s'oriente dans une direction où les appareils dans votre maison, traditionnellement notre espace le plus privé, sont largement contrôlés par d'autres personnes qui veulent savoir ce que vous faites*⁸⁸¹ ». Là encore, les principes issus de la loi informatique et libertés semblent être en déficit d'effectivité face à la surveillance diffuse.

352. Très globalement, ces droits et ces principes n'ont été que peu respectés, ainsi que le mentionnait Jean Frayssinet: « *trente ans après son vote, on ne peut pas dire que les Français se sont accaparés la loi de 1978*⁸⁸² ». Entre déficit de conscience des enjeux de la surveillance diffuse,

⁸⁷⁸ Ibid. p. 9-10.

⁸⁷⁹ Voir en ce sens: GAROSCIO Paolo, *Lisez les conditions d'utilisation ou vous finirez par laver des toilettes*, 22 juillet 2017, Clubic, <http://www.clubic.com/insolite/actualite-833734-lisez-conditions-utilisation-finirez-laver-toilettes.html> (dernière consultation: 5 mars 2018)

⁸⁸⁰ Voir en ce sens: AUFFRAY Christophe, *SONOS: les données ou la vie de vos (nos) appareils !*, 22 août 2017, ZDnet, En ligne: <http://www.zdnet.fr/actualites/sonos-les-donnees-ou-la-vie-de-vos-nos-appareils-39856314.htm> (dernière consultation: 5 mars 2018)

⁸⁸¹ Ibid.

⁸⁸² Op. Cit.

déficit d'effectivité de la loi, automacité du choix technique, complexité de mise en oeuvre des droits des citoyens et des principes issus de la loi Informatique et Libertés, bien-être promu par le tout numérique, sécurité promise par la surveillance, on a, ainsi que l'écrivait Frayssinet, véritablement « *l'impression que la loi de 1978 tourne à vide, manque d'adhérence sur les réalités et les comportements, ressemble à un village Potemkine dont l'existence suffit à rassurer et à légitimer le discours officiel sur l'existence d'un haut niveau de protection des droits et libertés des personnes dans une société démocratique*⁸⁸³ ».

B. L'inadéquation des flux transfrontières de données personnelles: la remise en cause du Safe Harbor par l'arrêt CJUE du 6 octobre 2015

353. Afin de donner son effectivité à la protection des données personnelles à l'international, l'Europe et les Etats-Unis ont au terme d'une collaboration longue et laborieuse élaboré un dispositif applicable aux flux transfrontières de données : le « Safe Harbor »⁸⁸⁴ (1). Sa récente remise en question (2) démontre de son inadéquation, ainsi que de son manque d'effectivité (2).

1. Le Safe Harbor: un instrument international sous influence européenne

354. Le Safe Harbor, également appelé sphère de sécurité est la résultante d'une longue négociation entre les États-Unis et l'Union européenne. En effet, l'Union européenne dans le cadre de la directive de 1995 a souhaité limiter le transfert des données à caractère personnel dans des pays ne disposant pas d'une protection adéquate⁸⁸⁵. Cette protection s'apprécie « *au regard de toutes*

⁸⁸³ Op. Cit. p.71.

⁸⁸⁴ On aurait pu citer d'autres exemples de traitement des flux transfrontières de données personnelles. On pense notamment à l'affaire dite « PNR » des données passagers des compagnies aériennes résultantes d'un penchant sécuritaire américain, Voir à ce propos: Groupe de travail « article 29 », Avis 2/2007 concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record - PNR) aux autorités américaines du 15 février 2007 et révisé et mis à jour le 24 juin 2008, 000345/07/FR, WP 132, 000345-01/07/FR, WP 151, Ou encore: Avis du Contrôleur européen de la protection des données *sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les Etats-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la Sécurité intérieure*, 2012/C 35/O3, JOUE du 9 février 2012, En ligne: [http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012XX0209\(03\)&from=FR](http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012XX0209(03)&from=FR) (dernière consultation: 5 mars 2018)

⁸⁸⁵ L'article 25 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 précise : « 1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat. (...) ».

les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées⁸⁸⁶ ». Afin de remédier à l'inquiétude européenne face aux flux transfrontaliers vers les États Unis et en vue de simplifier les actions, telles que la présence de clauses contractuelles effectuées par des autorités de contrôle européenne en cas de transfert de données, le Département du Commerce américain en particulier la National Information Agency a proposé des règles minimales pour assurer la protection des données personnelles par les entreprises américaines. La National Information Agency a tout d'abord proposé des *Elements of Effective selfregulation for privacy Protection*⁸⁸⁷ en 1998. Ce texte a donné lieu à de lourdes négociations entre la Commission européenne et les États Unis débouchant sur diverses modifications. Il a été en effet complexe de trouver un équilibre entre deux parties prônant deux modes de réglementations différents. A plusieurs reprises le Groupe de l'Article 29 s'est prononcé sur ces instruments, déplorant le manque de protection effective des données personnelles⁸⁸⁸.

355. Le Safe Harbor est conçu comme un dispositif non contraignant, dans le sens où il n'est pas imposé de fait aux entreprises américaines⁸⁸⁹, et qu'il est fondé sur la base du volontariat des entreprises du secteur à y adhérer. Les entreprises américaines désireuses d'obtenir des données européennes ont alors tout intérêt à souscrire aux principes du Safe Harbor. D'autant que, d'une part, la Commission européenne s'est prononcée en 2000⁸⁹⁰ en faveur du Safe Harbor, affirmant le

⁸⁸⁶ Article 25. 2 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. Journal officiel n° L 281 du 23/11/1995 p. 0031 - 0050

⁸⁸⁷ National Telecommunication and Information Administration, *Elements of Effective selfregulation for privacy Protection*, Janvier 1998, United States Department of Commerce, En ligne: <http://www.ntia.doc.gov/reports/privacydraft/198dftprin.htm> (dernière consultation: 5 mars 2018)

⁸⁸⁸ Voir en ce sens: Groupe de travail « Article 29 », Avis 1/99 du 26 janvier 1999 concernant le niveau de protection des données à caractère personnel aux États-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain, WP 15, 26 janvier 1999. Mais également: Avis 2/99 du 19 avril 1999 concernant la pertinence des « principes internationaux de la sphère de sécurité » publiés par le ministère du commerce des États-Unis le 19 avril 1999, 3 mai 1999, WP 19

⁸⁸⁹ Ces dernières fonctionnant sur le mode de l'autorégulation sur les problématiques de données personnelles et de vie privée.

⁸⁹⁰ Décision de la Commission n° 2000/520/CE du 26 Juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32000D0520&from=FR> (dernière consultation: 5 mars 2018)

niveau de protection adéquat offert par cet instrument aux entreprises y adhérant, ce qui ne limite plus les transferts transfrontaliers. D'autre part, il semble utile de rappeler que cet instrument ne concerne que les données de provenance européenne; un citoyen américain ne peut pas se prévaloir du Safe Harbor. On notera également que la Federal Trade Commission, un organisme américain spécialisé dans le domaine du droit de la concurrence et de la consommation⁸⁹¹, est compétente en cas de litige opposant un particulier et une entreprise ayant adhéré au Safe Harbor. Suite à leur adhésion, les entreprises doivent se conformer aux principes, et indiquer clairement dans leurs politiques de confidentialité, leur affiliation aux principes du Safe Harbor.

356. Dans sa dernière version, le Safe Harbor contenait sept principes essentiels. Le premier ressemble au principe d'information des consommateurs, utilisateurs, sur la finalité opérée par les entreprises dans le cadre de la collecte des données, précédemment décrit. Ce principe envisage également de permettre un droit d'accès sur leurs données aux individus en obligeant les entreprises à fournir une adresse de contact pour se faire. L'information doit comporter la mention d'une transmission des données ou non à des tiers. Le deuxième principe se pose sur un choix facultatif accordé par l'entreprise à l'utilisateur ou client de voir ses données transmises à des tiers ou utilisées à des fins autres que celles énoncées au préalable. Le troisième principe semble limiter cette transmission aux tiers, puisque celle-ci doit se matérialiser en une règle bien précise. La transmission ne peut s'effectuer, que si le tiers est également partie au Safe Harbor. En l'absence de cette condition préalable, un accord écrit entre l'entreprise et le tiers est exigé obligeant celui-ci à opter pour un niveau de protection équivalent au Safe Harbor. Le quatrième principe est consacré au droit d'accès effectif de toute personne sur ses propres données. On retrouve le droit d'accès, de suppression et de rectification sur les données, précédemment décrit dans le cadre de la législation française et européenne. Il existe une limite à ce droit : si les charges inhérentes au droit d'accès sont disproportionnées au risque de l'atteinte à la vie privée, le droit d'accès peut être refusé. On prend également en compte l'atteinte aux droits des tiers. Le cinquième principe repose sur la notion de sécurité des données. Les entreprises ayant adhéré au Safe Harbor ont l'obligation d'apporter une sécurisation aux données collectées, afin de les protéger contre les atteintes provenant des tiers, mais aussi contre les destructions ou le risque de détournement. Le sixième principe correspond à ce que l'on peut appeler l'intégrité des données. Celles-ci se doivent d'être exactes, à jour et pertinentes à la finalité donnée au préalable par les entreprises. Enfin, le dernier principe repose sur

⁸⁹¹ Tels que les manœuvres et les pratiques déloyales ou frauduleuses

des nécessaires procédures mises en place afin de mettre en pratique ces principes et d'édicter des sanctions telles que la suppression de l'entreprise de la liste du Safe Harbor.

357. On voit bien à la lecture de ces principes une influence de la vision européenne de la protection des données personnelles. La question se pose alors de connaître de l'effectivité réelle ou du déficit d'effectivité de ces principes appliqués aux flux transfrontières de données personnelles.

2. La remise en question des Safe Harbor

358. Le premier élément indiquant un déficit d'effectivité de ce dispositif réside dans la seule énonciation suivante: le Safe Harbor n'est pas un dispositif contraignant. Les politiques de confidentialité de certaines entreprises, spécialement les moteurs de recherche américain, n'ont alors dans les faits que peu d'effet contraignant, tant par le manque de contrôle d'organes ou de juridictions européennes sur des données personnelles européennes, que par le système d'adhésion à ces principes. Ensuite, et puisque que le Safe Harbor ne concerne que le transfert de données personnelles, ce dernier n'a en réalité que peu de force face à l'ampleur des possibilités offertes par les nouvelles technologies. En effet, par exemple, la simple consultation de données personnelles ne rentrent pas dans le cadre de ce dispositif. Rappelons ici que la CNIL considère que constitue un transfert de données vers un pays tiers « *toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire*⁸⁹² ». Rappelons également que selon l'arrêt Bodil Lindqvist rendu par la CJCE le 6 novembre 2003⁸⁹³, il « *n'existe pas de « transfert vers un pays tiers de données » au sens de l'article 25 de la directive 95/46 lorsqu'une personne qui se trouve dans un État membre inscrit sur une page Internet, stockée auprès d'une personne physique ou morale qui héberge le site Internet sur lequel la page peut être consultée et qui est établie dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à Internet, y compris des personnes se trouvant dans des pays tiers* ».

⁸⁹² CNIL, *Les transferts de données à caractère personnel hors Union européenne*, Novembre 2012, En ligne: <https://www.cnil.fr/sites/default/files/typo/document/GUIDE-transferts-integral.pdf> (dernière consultation: 5 mars 2018)

⁸⁹³ CJCE, Affaire C-101/01, Lindqvist, arrêt de la Cour du 6 novembre 2003, Recueil de la jurisprudence 2003 I-1297, Point n° 71.

359. Couplé à la question de la surveillance diffuse, l'ensemble de ces éléments tend à démontrer que les Safe Harbor auraient dû être applicables à ce phénomène tant pour de simples recherches sur Internet, que pour le stockage d'informations sur les serveurs d'entreprises américaines, que pour des activités de surveillance de masse. Pourtant, étant précisé que les Safe Harbor ne s'appliquent qu'au transfert de données, la simple consultation de données collectées ne rentre pas dans la grille d'analyse. La protection des données des citoyens européens ne semblent donc pas vraiment adéquate, et la notion même de transfert de données semblent alors avoir peu de sens au vu des potentialités de la surveillance diffuse. Cette affirmation prend d'ailleurs tout son sens avec l'arrêt rendu par la Cour de Justice de l'Union Européenne en date du 6 octobre 2015⁸⁹⁴. Dans le contexte des révélations faites par Snowden concernant les activités des services de renseignement des Etats-Unis, les juges européens ont, avec cette décision, suspendu l'application des Safe Harbor pour plusieurs raisons, et par là réaffirmé leur opposition à la surveillance.

360. S'appuyant sur l'arrêt Digital Rights Ireland, les juges déclarent 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*⁸⁹⁵ ». Et d'ajouter plus particulièrement à l'encontre des principes du Safe Harbor: « *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. En effet, l'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article. À cet égard, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit*⁸⁹⁶ ». Les juges européens concluent ensuite à l'inadéquation des Safe Harbor, en précisant

⁸⁹⁴ CJUE, Affaire C-362/14, Arrêt de la Cour (grande chambre) du 6 octobre 2015, publié au Recueil numérique (Recueil général), Maximilian Schrems contre Data Protection Commissioner, Demande de décision préjudicielle introduite par la High Court (Irlande), En ligne: <http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-362/14> (dernière consultation: 5 mars 2018)

⁸⁹⁵ Ibid. point 94

⁸⁹⁶ Ibid. point 95

que : « *il y a lieu de relever 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. Par suite, et sans qu'il soit besoin d'examiner les principes de la sphère de sécurité quant à leur contenu, il convient de conclure 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*⁸⁹⁷ ».

361. Au vu des conclusions de cet arrêt, les mots de Frayssinet selon lesquels la protection de la vie privée issue de la loi de 78, et par extension la directive de 95 « *ressemble à un village Potemkine dont l'existence suffit à rassurer et légitimer le discours officiel sur l'existence d'un haut niveau de protection des droits et libertés des personnes dans une société démocratique*⁸⁹⁸ » trouvent totalement application aux Safe Harbor. Jusqu'à cette décision, alors que pour le juriste la situation présentait quelques couacs, il suffisait pour les entreprises américaines et les politiques américains, de rassurer les européens par l'adhésion au Safe Harbor. Dans les faits, l'ensemble des traitements réalisés sous couvert de ces principes étaient dans l'illégalité. Le rôle des politiques européens est également au vu de cette décision à dénoncer. La Commission n'a pas, selon les juges européens, démontré, dans le cadre de sa décision 2000/520 précitée, que les Etats-Unis assuraient effectivement un niveau adéquat de protection. Plus que les simples accords et législations de protection des données personnelles, il semble bien qu'il faille conclure à un déficit d'effectivité de ces dispositions créant une instabilité, une insécurité juridique. Ce décalage des législations européennes et des dispositifs américains de protection des données à caractère personnel, s'explique en partie du fait « *d'un manque d'adhérence sur les réalités et les comportements*⁸⁹⁹ », pour reprendre à nouveau les mots de Jean Frayssinet. Ce manque d'adhérence sur les réalités se traduit également par une ambition toujours plus grande des Etats à rogner de plus en plus la vie privée des individus sous prétexte de sécurité, des entreprises à développer le marché du numérique, et des individus à s'inscrire dans une économie de la visibilité.

⁸⁹⁷ Ibid point 97 et 98.

⁸⁹⁸ Op. cit.

⁸⁹⁹ Op. Cit.

Paragraphe 2. La conception des données personnelles par référence à la vie privée: un choix heureux contre l'idéologie sécuritaire mais peu efficace dans son ensemble

362. Le droit des données personnelles s'est principalement organisé autour de la notion juridique de vie privée (A). Ce choix se retranscrit d'ailleurs dans la législation Informatique et Libertés au travers du principe de proportionnalité. Bien que ce choix soit heureux contre l'ingérence (numérique) des Etats dans la vie privée des citoyens, il semble là encore qu'un déficit d'effectivité soit à constater (B).

A. La conception des données personnelles par référence à la vie privée

363. Selon Benjamin Constant, « *dans une société fondée sur la souveraineté du peuple, il est certain qu'il n'appartient à aucun individu, à aucune classe, de soumettre le reste à sa volonté particulière; mais il est faux que la société toute entière possède sur ses membres une souveraineté sans bornes. L'universalité des citoyens est le souverain, dans ce sens, que nul individu, nulle fraction, nulle association partielle ne peut s'arroger la souveraineté, si elle ne lui a pas été déléguée. Mais il ne s'ensuit pas que l'universalité des citoyens, ou ceux qui par elles sont investis de la souveraineté, puissent disposer souverainement de l'existence des individus. Il y a au contraire une partie de l'existence humaine qui, de nécessité, reste individuelle et indépendante, et qui est de droit hors de toute compétence sociale. La souveraineté n'existe que d'une manière limitée et relative. Au point où commence l'indépendance et l'existence individuelle, s'arrête la juridiction de cette souveraineté*⁹⁰⁰ ». C'est de sa liberté, que l'individu puise les conditions nécessaires à sa vie en société, à sa citoyenneté. Le droit au respect de la vie privée est, pour reprendre les mots de Constant, cette « *partie de l'existence humaine qui (...) est de droit hors de toute compétence sociale* », c'est à dire hors de toute souveraineté. Et c'est bien dans ce souci de protéger la vie privée qu'un régime démocratique peut naître et prospérer. Le droit au respect de la vie privée est alors un principe essentiel d'une société libre et démocratique qui doit être interprété

⁹⁰⁰ CONSTANT Benjamin, *Principes de politique applicables à tous les gouvernements représentatifs et particulièrement à la constitution actuelle de la France*, Chez Alexis Eymery, Libraire, rue Mazarine, N° 30, Mai 1815, En ligne: http://davidmhart.com/liberty/FrenchClassicalLiberals/Constant/Books/Constant_1815Principes_de_Politique.pdf (dernière consultation: 5 mars 2018), p. 17-18

« à la lumière des conditions de vie actuelle⁹⁰¹ ». La référence à la vie privée sans cesse renouvelée par le juge dans le cadre de la protection des données personnelles est à saluer (1). Il aurait été néanmoins intéressant de reconnaître en cette protection un principe à valeur constitutionnel (2).

1. Le droit des données personnelles par référence à la vie privée

364. Le droit au respect de la vie privée est apparue de manière récente dans le droit interne. C'est la loi du 17 juillet 1970⁹⁰², à l'origine de l'article 9 du Code Civil, qui dispose en son article 22 que « *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*⁹⁰³ ». La surveillance diffuse, dans sa double nature, banale et imposée pour des raisons de sécurité, peut troubler le droit au respect de la vie privée. Pour rappel, l'article 34 de la Constitution laisse au législateur la responsabilité de fixer les garanties fondamentales devant s'appliquer aux citoyens pour l'exercice de leurs libertés fondamentales. L'une des prérogatives essentielles du législateur, pouvant entrer en conflit avec les droits et libertés fondamentales des citoyens, résident dans la sauvegarde de l'ordre public. Face à ce risque, le Conseil Constitutionnel, dans son rôle de garant des libertés publiques, doit assurer une analyse du respect de la proportionnalité entre les mesures entreprises et les possibles atteintes aux droits fondamentaux.

365. Par le rappel de l'article 2 de la Déclaration des Droits de l'Homme et du citoyen de 1789 qui dispose que : « *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* », le juge constitutionnel interprète le respect de la vie privée comme une des

⁹⁰¹ Voir par exemple l'arrêt de la Cour Européenne des droits de l'Homme n° 5856/72, 25 avril 1978, Tyrer contre Royaume-uni, par. 31, ou encore l'arrêt de la Cour Européenne des droits de l'Homme n° 15318/89, 23 mars 1995, Loizidou contre Turquie, par. 71. Si l'article 8 de la Convention Européenne de Sauvegarde des Droits de l'Homme énonce que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance », la Convention est considérée par la Cour Européenne des Droits de l'Homme « *comme un instrument vivant à interpréter à la lumière des conditions de vie actuelle* ». Cette interprétation dynamique et évolutive s'applique à l'article 8.

⁹⁰² Loi n° 70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens*, JORF du 16 juillet 1970, p. 06751 et s., En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT00000693897&pageCourante=06751 (dernière consultation: 5 mars 2018)

⁹⁰³ Ibid. Article 22, p. 06755

composantes de la liberté⁹⁰⁴. Les principes constitutionnels en matière de traitements de données à caractère personnel à destination pénale sont régulièrement rappelés par le Conseil qui a pu faire, progressivement, émerger une certaine doctrine en la matière. Ainsi qu'il s'agisse de fichiers d'analyse sérielle ou de fichiers d'antécédents judiciaires, les juges du Conseil Constitutionnel rappellent la préservation d'un équilibre entre la sauvegarde de l'ordre public et les libertés fondamentales par le respect de la proportionnalité. Garanti par le choix d'imposer un cloisonnement de chaque base de données et application permettant d'y accéder, le Conseil tend à préserver cet équilibre par le contrôle de l'étendue du champ de données personnelles accessible aux forces de l'ordre, mais également par l'imposition d'une limite temporelle de conservation des données produites en matière, par exemple, de rapprochement judiciaire, à une durée de trois ans afin de réduire le risque d'exploitation de ces données⁹⁰⁵. Sur le plan international, la Convention européenne des Droits de l'Homme dispose en son article 8 que « *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* ». Le non respect de cet article ouvre un recours auprès de la Cour européenne des droits de l'Homme.

366. Cette dernière a montré par sa jurisprudence en la matière qu'elle adopte une interprétation

⁹⁰⁴ Voir en ce sens: Décision n°94-352 DC du 18 janvier 1995 concernant la loi d'orientation et de programmation relative à la sécurité, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html> (dernière consultation: 5 mars 2018), et les décisions du Conseil Constitutionnel suivantes : Décision n° 99-416 DC du 12 juillet 1999 relative à la loi portant création d'une couverture maladie universelle, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-416-dc/decision-n-99-416-dc-du-23-juillet-1999.11847.html> (dernière consultation: 5 mars 2018), Décision n°99-419 DC du 19 novembre 1999 concernant la loi relative au pacte civil de solidarité, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-419-dc/decision-n-99-419-dc-du-9-novembre-1999.11849.html> (dernière consultation: 5 mars 2018)

⁹⁰⁵ Voir en ce sens les décisions du Conseil Constitutionnel suivantes : Décision n°2003-467 DC du 13 mars 2003 relative à la loi pour la sécurité intérieure, En ligne: <http://www.conseil-constitutionnel.fr/conseil-con..c/decision-n-2003-467-dc-du-13-mars-2003.855.html> (dernière consultation: 5 mars 2018), et Décision n°2011-625 DC du 11 mars 2011 relative à la loi d'orientation et de programmation pour la performance de la sécurité intérieure, En ligne: <http://www.conseil-constitutionnel.fr/decision/2011/2011-625-dc/decision-n-2011-625-dc-du-10-mars-2011.94924.html> (dernière consultation: 5 mars 2018)

large de la notion de violation de la vie privée⁹⁰⁶. La loi Informatique et Libertés s'inspire de cette vision protectrice de la vie privée de part le régime qu'elle met en place, mais aussi au regard de toute ingérence potentielle. Les principes posés par la loi Informatique et libertés tendent vers cette analyse.

2. Un principe essentiel d'une société libre et démocratique non reconnu par la Constitution

367. Il est admis de longue date par les jurisprudences nationales et européennes que l'encadrement de la protection des données personnelles doit se concevoir par référence à la vie privée. Ainsi, par exemple, l'arrêt rendu par la Cour Européenne des Droits de l'Homme le 4 décembre 2008 opposant M. S et M. Marper contre le Royaume-Uni⁹⁰⁷, déclare que « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (voir mutatis mutandis Z. c. Finlande, précité § 95). La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières*⁹⁰⁸ ».

368. Bien qu'il n'existe pas de consécration de la protection des données personnelles dans la Constitution de 1958 par référence à la notion de vie privée, cette assimilation aurait pu être opérée dans le cadre de différents projets de révision constitutionnelle⁹⁰⁹. Ainsi, le rapport du comité de réflexion sur le Préambule de la Constitution présidée par Simone Veil, et remis en 2008 au

⁹⁰⁶ Voir en ce sens: CEDH, Affaire Tyrer c. Royaume-Uni, Requête n°5856/72, Strasbourg, 25 avril 1978. La Cour rappelle dans cette affaire que « *la Convention est un instrument vivant à interpréter - la Commission l'a relevé à juste titre - à la lumière des conditions de vie actuelles* ». Il est intéressant d'ajouter ici que suivant cette interprétation de la Convention, le champ de protection de l'article 8 couvre aujourd'hui des domaines variés passant par le droit à l'intimité au droit des membres des minorités à un mode de vie traditionnel, et du droit à connaître ses origines au droit au changement d'identité sexuelle.

⁹⁰⁷ CEDH (Grande Chambre), Affaire S. et Marper contre Royaume-Uni, Requêtes n° 30562/04 et 30566/04, Strasbourg, 4 décembre 2008, En ligne: <https://rm.coe.int/16806ae19a> (dernière consultation: 5 mars 2018)

⁹⁰⁸ Ibid. Point 103

⁹⁰⁹ Pour une analyse enrichissante des évolutions et actes manqués de certains projets de révision constitutionnelle, Voir: VEIL Simone, *Redécouvrir le Préambule de la Constitution, Rapport du Comité de Réflexion sur le Préambule de la Constitution au Président de la République*, La Documentation française, Collection des rapports officiels, Décembre 2008, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000758.pdf> (dernière consultation: 5 mars 2018)

Président de la République, déclare en reprenant une intervention du président de la CNIL, Alex Türk, que « *le Conseil constitutionnel intègre, dans ses décisions, la loi « Informatique et Libertés » comme « protectrice des libertés individuelles ». Aussi cette loi se voit-elle conférer un statut particulier, celui des lois assurant la protection d'un principe de valeur constitutionnelle, à savoir la liberté individuelle, elle-même constitutive d'un principe fondamental garanti par les lois de la République. Dès lors, il serait temps, logique et pertinent de reconnaître de manière explicite dans notre Constitution ce principe devenu un principe de référence dans la jurisprudence du Conseil constitutionnel. De surcroît, bien que le droit à la protection des données personnelles soit une composante de celui assurant le respect de la vie privée, il demeure un droit autonome et spécifique qui mérite une reconnaissance particulière⁹¹⁰ ».* Et de conclure avec conviction que « *à l'heure où l'informatique est « partout », fait partie intégrante de notre vie quotidienne, où nos données sont l'essence même de notre identité et de notre personnalité, le droit à leur protection mérite d'être doté de la même valeur juridique que la liberté d'aller et venir, la liberté de culte, la liberté d'expression et tant d'autres libertés individuelles. Son importance est d'ailleurs d'ores et déjà consacrée par de nombreux textes et instruments internationaux⁹¹¹ ».*

369. Face à l'ampleur des possibilités techniques, il est clair que l'inscription des données personnelles dans le cadre de la Constitution, et des principes à valeur constitutionnelle permettrait de donner une force à ce droit, ou du moins, d'apporter une sécurité juridique, là où dans certains cas il manque d'effectivité et de pertinence par rapport aux réalités et aux comportements individuels. On notera en guise de référence que le rapport de 2008 mentionne une proposition de la loi constitutionnelle, qui en 1977, évoquait le respect de la vie privée et la protection des données personnelles au terme d'un article 23 ainsi rédigé: « *Tout homme a droit à la protection de sa vie privée. La loi assure notamment cette protection contre les dangers que peut comporter l'emploi de l'informatique ainsi que des techniques de collecte, conservation et utilisation d'informations⁹¹² ».* Cette évocation des actes manqués de la reconnaissance de la protection des données personnelles comme principe à valeur constitutionnelle doit nécessairement être mise en relation avec la Charte des droits fondamentaux de l'Union Européenne qui vient la reconnaître comme tel en son article

⁹¹⁰ Ibid. p. 185

⁹¹¹ Ibid. p. 186.

⁹¹² Ibid. p. 15.

8⁹¹³.

B. Le principe de proportionnalité des législations Informatiques et Libertés: un principe permettant la balance entre deux intérêts antagonistes

370. La protection de la vie privée s'organise autour d'une garantie de la liberté contre l'ingérence d'autorité publique ou privée autre que celle prévue par la loi. Ainsi qu'évoqué précédemment, la Convention européenne des Droits de l'Homme par exemple dispose en son article 8 que « *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* ». La loi Informatique et Libertés s'inspire de cette vision protectrice de la vie privée de part le régime qu'elle met en place, mais aussi au regard de toute ingérence potentielle. Les principes posés par la loi Informatique et libertés tendent vers cette analyse.

371. Le règlement européen tire d'ailleurs les enseignements des règles et jurisprudences précitées puisqu'il vient à nouveau préciser la « *fondamentalité* » de la protection des données personnelles en rappelant son origine : l'article 8 de la Charte des droits fondamentaux de l'Union européenne, et l'article 16 paragraphe 1 du Traité sur le fonctionnement de l'Union Européenne, disposant que toute personne a droit à la protection des données à caractère personnel la concernant. Le règlement tient donc à intégrer les enjeux actuels de la société numérique : sécurité, économie, justice et libertés, et vient préciser à nouveau l'un des piliers du droit à la protection des données à caractère personnel : le principe de proportionnalité. L'exposé des motifs du règlement européen est d'ailleurs riche en enseignements à ce sujet. Le point 4 déclare ainsi que « *le traitement des données*

⁹¹³ L'article 8 déclare: « *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* ». Pour rappel, la Charte des droits fondamentaux de l'Union européenne a été proclamée lors du Conseil européen de Nice le 7 décembre 2000. Le traité de Lisbonne, entré en vigueur le 1er décembre 2009, lui donne la même valeur juridique que celle des traités. Elle est donc contraignante pour l'ensemble des Etats membres et tout citoyen peut s'en prévaloir. Charte des Droits Fondamentaux de l'Union européenne, 2000/C 364/01, JOCE du 18 décembre 2000, En ligne: http://www.europarl.europa.eu/charter/pdf/text_fr.pdf (dernière consultation: 5 mars 2018)

à caractère personnel devrait être conçu pour servir l'humanité. Il n'est pas un droit absolu et doit être considéré par rapport à sa fonction dans la société, non sans avoir été mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique⁹¹⁴ ».

372. Le principe de proportionnalité des données collectées, ainsi que sa détermination, nécessitent une part d'appréciation et de maîtrise technologique qui n'est pas simple, ni pour le responsable de traitement, ni pour le juriste, ni pour la CNIL⁹¹⁵. Or, l'appréciation de la proportionnalité des données collectées est nécessaire pour déterminer la licéité du traitement. Il en résulte donc un contrôle du Conseil d'Etat de l'erreur manifeste. C'est d'ailleurs ce qui s'est produit en 2007 dans le cadre du contentieux entre les sociétés d'auteurs, titulaires de droits d'auteur, les fournisseurs de services électroniques, et la CNIL face à la reconnaissance du caractère personnel de l'adresse IP⁹¹⁶. Or, ainsi que le rappelle l'avocate générale dans le cadre de l'affaire *Promusicae* précitée, conformément à l'article 7 de la Charte des Droits fondamentaux, « *la communication de données à caractère personnel à un tiers porte atteinte au droit au respect de la vie privée des intéressés, quelle que soit l'utilisation ultérieure des informations ainsi communiquées, et présente ainsi le caractère d'une ingérence au sens de l'article 8 de la Convention Européenne des Droits de l'Homme. Une telle ingérence méconnaît l'article 8 de la Convention Européenne des Droits de l'Homme, sauf si elle est «prévues par la loi» (...). De surcroît, toute ingérence dans la vie privée - le traitement de données à caractère personnel - doit répondre à l'exigence de proportionnalité par rapport aux objectifs poursuivis. Il faut ainsi qu'un besoin social impérieux soit en cause et que la*

⁹¹⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE L 119 du 4 Mai 2016, p. 1 - 88, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR>, point 4 (dernière consultation: 5 mars 2018)

⁹¹⁵ Sur ce point, voir l'évolution de la doctrine de la CNIL en cinq ans à peine sur la biométrie.

⁹¹⁶ Conseil d'Etat, 23 mai 2007, n° 288149, Inédit au recueil Lebon, En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000018259508> (dernière consultation: 5 mars 2018)

*mesure prise soit proportionnée au but légitime recherché*⁹¹⁷ ». La conservation et la transmission des données de trafic, devenues données personnelles, n'étaient possibles, à l'époque de l'arrêt *Promusicae*, qu'aux autorités publiques compétentes, dans le cadre de procédures pénales. La législation européenne ne permettait pas de transmettre des données à caractère personnel directement aux titulaires de droits d'auteurs « *désireux de poursuivre civilement la violation de leurs droits*⁹¹⁸ ».

373. Dans la confrontation de deux droits fondamentaux, tels que le droit de propriété⁹¹⁹ des titulaires de droits d'auteur et le droit à la protection de la vie privée qu'offre le droit des données personnelles, il semble ici que l'on fasse fi du principe de proportionnalité permettant la balance entre la vie privée et les intérêts de la Nation, au bénéfice du droit de propriété. Ainsi que le rappelle l'avocate générale dans ses conclusions concernant cette affaire: « *c'est au législateur communautaire qu'il appartient en tout premier lieu d'établir un équilibre entre les positions concernées en matière de droits fondamentaux ainsi qu'à la Cour lorsqu'elle interprète le droit communautaire. Les États membres sont néanmoins, eux aussi, tenus d'en tenir compte lorsqu'ils épuisent leur compétence réglementaire résiduelle dans le cadre de la transposition de directives. De surcroît, les pouvoirs publics et les juridictions des États membres ne doivent pas seulement interpréter leur droit national d'une manière conforme aux directives sur la protection des données, mais également veiller à ne pas se fonder sur une interprétation de ces directives qui entre en conflit avec les droits fondamentaux protégés par l'ordre juridique communautaire ou avec les autres principes généraux du droit communautaire*⁹²⁰ ».

374. La même démonstration peut être effectuée pour le cas des métadonnées. Le principe de proportionnalité met en balance ici deux intérêts, la sécurité et l'ordre public d'une part, et la protection des données personnelles et de la vie privée d'autre part. Alors que le juge européen a rappelé que la conservation des données de connexion était une exception qui ne devait en aucun

⁹¹⁷ Conclusions de Mme Kokott - Affaire C-275/06, Conclusions de l'avocat général Mme Juliane Kokott, présentées le 18 juillet 2007, Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=62901&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=413083>, points 52, 53 et 54 (dernière consultation: 5 mars 2018)

⁹¹⁸ Ibid. point 3

⁹¹⁹ L'article 17 paragraphe 2 de la charte des droits fondamentaux démontre bien que la propriété intellectuelle relève du domaine de protection du droit fondamental à la propriété.

⁹²⁰ Ibid. point 56.

cas devenir la règle, garantissant ainsi le respect du droit fondamental à la vie privée, l'impact de ces arrêts⁹²¹ dans le droit interne est loin d'être clair. La France s'engage de plus en plus sur une stratégie juridique et législative prônant la sécurité au détriment de la vie privée. Les lois précédemment cités, qu'elles concernent le renseignement ou la surveillance internationale des communications électroniques tendent à démontrer que la France s'oppose à suivre l'opinion des juges européens sur la conservation généralisée des données de connexion. En effet, alors que fin 2014 un rapport du Conseil d'Etat concernant le numérique et les droits fondamentaux⁹²² déclarait, à propos de l'arrêt Digital Rights Ireland, que « *de manière schématique, deux lectures peuvent en être faites: celle d'une condamnation de l'insuffisance des garanties prévues par la directive; celle d'une condamnation de tout système de conservation générale des métadonnées, quel qu'il soit*⁹²³ ». Et d'alerter que « *depuis la loi du 10 juillet 1991, le législateur a procédé en la matière par extensions successives: création d'une procédure de réquisition administrative des métadonnées par la loi du 23 janvier 2006; pérennisation et extension des finalités de cette procédure, ainsi que des services habilités à la demander, par la loi du 18 décembre 2013. Il apparaît nécessaire aujourd'hui de procéder à un réexamen global du cadre juridique de la surveillance des communications, dans le but de préserver la capacité de notre pays à protéger sa sécurité nationale tout en apportant l'ensemble des garanties nécessaires à la protection des droits fondamentaux*⁹²⁴ ». A travers les lois précitées, la France envisage clairement la conservation généralisée de données de connexion. La Quadrature du Net, French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs ont d'ailleurs dénoncé auprès du Conseil d'État une incompatibilité manifeste de la législation française avec l'arrêt Digital Rights Ireland. Pourtant, le Conseil d'État a ignoré leurs demandes de questions préjudicielles à la Cour de justice de l'Union européenne. Plus étonnant, le Conseil d'État n'a pas entendu les critiques adressées à la législation française par la section des études du Conseil d'État dans le cadre du rapport de 2014. Par exemple, le système des « boîtes noires » de la loi sur le Renseignement qui collecte des données de connexion, soumise ensuite à un algorithme détecteur d'hypothétique terroriste, permet une conservation de cet ensemble de données pendant un an. Pour le Conseil constitutionnel, ce dispositif ne porte pas « *une atteinte*

⁹²¹ Spécialement: Digital Rights Ireland et Tele2 Sverige

⁹²² Conseil d'Etat, *Etude annuelle 2014 - Le numérique et les droits fondamentaux*, La Documentation française, Septembre 2014, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf> (dernière consultation: 5 mars 2018)

⁹²³ Ibid. p. 199

⁹²⁴ Ibid. p. 195.

*manifestement disproportionnée au droit au respect de la vie privée*⁹²⁵ ». Ce n'est pourtant pas l'avis de la Cour de Justice de l'Union Européenne rendu à travers les arrêts de 2014 et de 2016.

375. Bien qu'encadrée par la loi, limitant la durée de conservation de ces données, la conservation généralisée des données de connexion doit rester un exception selon la CJUE. Quid alors de la légalité de ces mesures ? Quid de la légalité de certaines législations, dont la loi britannique du 29 novembre 2016⁹²⁶ (Investigatory Powers Act) ? Mais plus important encore, quid de la réelle proportionnalité, et de l'effectivité de ce principe au regard des stratégies juridiques et légales nationales?

376. Les décisions de la CJUE sont extrêmement positives en ce sens qu'elles interdisent la collecte systématique de métadonnées. Il faut alors nécessairement déduire de la position des juges européen que la collecte de (méta)données est en soi une forme de surveillance en tant que telle, avant même toute exploitation. En tant qu'outil de surveillance, la collecte de données doit être très strictement encadrée et utilisée uniquement lors de cas précis, ciblés, graves et proportionnés. Toutefois, entre enjeu de sécurité, confrontation avec d'autres droits fondamentaux (droits de propriété intellectuelle et droit à la vie privée) et enjeu strictement économique, une question reste en suspens: où se situe la proportionnalité, c'est à dire la balance effective entre ces enjeux et la vie privée des individus ? A la lecture de cette brève énumération, on ne peut s'empêcher de constater que les barrières et limites posés par le législateur et le juge sont fragiles, puisqu'elles ne limitent que ceux qui acceptent de ne pas les franchir. D'où le constat clair d'un manque d'effectivité globale des législations informatiques et Libertés, du fait d'un manque de compréhension des comportements des individus et des Etats, des intérêts des Nations, mais également des possibilités technologiques servant la surveillance diffuse.

⁹²⁵ Décision n°2015-713 DC du 23 juillet 2015 concernant la loi relative au renseignement, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html> (dernière consultation: 5 mars 2018)

⁹²⁶ Investigatory Powers Act 2016 Chapter 25, 29 novembre 2016, En ligne: <https://www.legislation.gov.uk/ukpga/2016/25/contents> (dernière consultation 5 mars 2018). Cette loi a pour but de prévoir et d'encadrer l'interception des communications, le brouillage d'équipements, l'acquisition et la conservation de données de communication, de jeux de données et d'autres renseignements collectés en masse, mais également de prévoir davantage de pouvoirs en matière d'enquête et de sécurité nationale.

Conclusion de Titre

377. Malgré un champ d'application large et une avance réelle sur le temps technologique les premières législations informatiques et libertés ont, comme le rappelle Alex Türk « *révélé des faiblesses*⁹²⁷ ». D'une part, ainsi que le soulignait le rapport Braibant le système promu par la loi de 1978, souffre « *dans la pratique d'un déficit d'effectivité. Personne n'est en mesure d'évaluer aujourd'hui avec une certaine précision le nombre de traitements automatisés d'informations nominatives, qui constituent l'objet même de la loi. La CNIL en a enregistré 500000 environ. Encore ce chiffre doit-il être minoré d'environ 20%, pour tenir compte des traitements qui ont disparu sans que leur suppression ait été déclarée. De toute façon, le nombre actuel de traitements en fonctionnement est sans commune mesure avec celui des traitements déclarés ou autorisés. Trois millions d'entreprises sont dotés d'un ou plusieurs traitements, parfois plusieurs centaines. (...) Au total et même en tenant compte des traitements dispensés de déclaration, on peut avancer sans grand risque d'exagération que quelques millions de traitements ont échappé à son contrôle (la CNIL). Ces traitements ne sont sans doute pas « clandestins », mais ils sont en tout cas « irréguliers ». Le bilan de la répression administrative et pénale, est également faible - quelques dizaines de sanctions ou de poursuites*⁹²⁸ ». D'autre part, la multiplication de lois sectorielles applicables au casier judiciaire, aux permis de conduire, aux recherches en matière de santé, est venue brouiller le champ d'application de la loi. Ce brouillage se constate également du fait du déséquilibre qu'a instauré la loi de 1978 entre le secteur public et privé. Enfin, et comme le souligne Guy Braibant, l'existence de la CNIL, ainsi que des mesures de protection offertes par la loi de 1978 ont été « *trop largement ignorées*⁹²⁹ ».

378. Ce déficit d'effectivité des premières législations informatique et libertés est lié à l'absence de prise en compte réelle des enjeux même de la surveillance diffuse. La réduction de toutes activités humaines à un chiffre statistique pour reprendre les mots de Tarde, à une data produit en effet une confusion des genres. La surveillance diffuse cherche à collecter toutes données possibles, et spécialement des données non personnelles qui par truchement technologique ou interconnexion peuvent recevoir la qualification de données personnelles *a posteriori*. Le rôle du juge dans la

⁹²⁷ TURK Alex, *Rapport précité*, p. 20

⁹²⁸ BRAIBANT Guy, *Données personnelles et société de l'information - Rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46*, 3 mars 1998, La Documentation française, décembre 1998, section 6 du rapport.

⁹²⁹ Ibid.

qualification des données et des traitements de données est alors à souligner. En tant que garant des droits et libertés fondamentales, son travail de requalification est nécessaire pour appliquer à des traitements de données non personnelles, mais potentiellement intrusifs en terme de vie privée, le régime de protection des données personnelles et de la vie privée. Pour autant, l'élargissement toujours plus important de la notion de donnée personnelle du fait de la prise en compte des évolutions technologiques contribue à la confusion des genres.

379. Ainsi que le notait Pierre Catala, « *comment éviter, en effet, que la réponse de la loi au défi électronique ne s'élabore dans le désordre, sous forme de réglementations mal coordonnées, minutieuses à l'excès et cependant parcellaires, attelées au progrès scientifique et, comme lui, sans cesse remises en question, oubliées enfin de quelques vérités permanentes auxquelles pourraient s'attacher des règles stables ?*⁹³⁰ » La situation décrite par Pierre Catala est loin d'être évitée puisque le juriste se retrouve aujourd'hui confronté à des problèmes de droit sans cesse plus complexes, et toujours plus imbriqués au progrès scientifique.

⁹³⁰ CATALA Pierre, *Le droit à l'épreuve du numérique - Jus ex Machina*, Presses Universitaires de France, Collection Droit, Ethique, Société, Première édition, mai 1998, p. 226. Voir spécialement Chapitre 13 pp. 224 - 244. Ce chapitre développe des réflexions que l'auteur a présenté oralement le 12 mai 1982 lors des Deuxièmes Entretiens du droit de l'informatique de Nanterre.

Conclusion partielle

380. Dans la poursuite des questionnements de Pierre Catala, il faut garder en tête que la surveillance diffuse s'inscrit dans le prolongement du projet de société de l'information et de la communication, mais également du marché du numérique. Cet élément a permis de mettre en lumière le fonctionnement de ces projets de société fondés sur l'information et la transmission de l'information.

381. Tantôt enjeu économique, tantôt enjeu politique le concept d'information est la pierre angulaire de la surveillance diffuse. Cette dernière doit nécessairement être appréhendée comme un phénomène de société. L'analyse des discours technophobiques et technophiles permet de comprendre la surveillance comme un enjeu de société partagée entre des ambitions sécuritaires et marketing d'acteurs variés. Cet enjeu a été rendu possible grâce à la métamorphose de la société de l'information et de la communication en un véritable marché du numérique. Et c'est bien dans la volonté de création de ce marché du numérique que, d'une part, la surveillance a pu se diffuser, tant dans son idéologie de rationalisation des activités humaines, politiques et économiques, que dans son ambition à recueillir toujours plus d'informations. D'autre part, le marché du numérique a rendu acceptable le recours aux systèmes socio-techniques dans chacune des activités des individus. Favorisée par une gouvernementalité fondée sur la peur, cet usage des technologies a facilité la banalisation de la surveillance diffuse, ainsi qu'une véritable culture de la surveillance. Les individus, préparés à la normalisation des usages technologiques et aliénés par les peurs des sociétés de consommation et du divertissement, se sont alors pleinement insérés dans le jeu de la surveillance diffuse.

382. Ainsi dépouillés de toute rationalité, d'esprit critique, les individus se sont placés d'eux-mêmes dans le champs d'observation des caméras, des réseaux sociaux, des big data, et autres pratiques du numérique. La surveillance revêt alors une forme double: banale dans la collecte et le traitement d'informations concernant les activités quotidiennes des individus d'une part; et, d'autre part, imposée dans la poursuite des objectifs de sécurité. La surveillance a modifié l'exercice du pouvoir, le transformant en une sorte de « biopouvoir algorithmique » fondée sur la prédiction, la prévention, la promesse d'une absence de menaces et de risques, l'organisation et la prise en charge de la transparence des individus. Bien-être, liberté, consommation et sécurité sont ainsi les fers de lance de la surveillance diffuse, largement influencée par la promotion de la rationalisation permise

par les nouvelles technologies et l'incitation à l'auto-contrôle et à l'auto-contrainte.

383. Ainsi que Pierre Catala le poursuivait dans l'ouvrage précité « *en d'autres domaines, l'expérience montre que le droit s'est formé à partir d'une notion fondamentale et de quelques principes, autour desquels sont venues s'articuler des législations spécifiques. (...). Quand la complexité s'édifie ainsi par arborescence, le danger d'incohérence entre plusieurs des sous-ensembles n'est pas tout à fait écarté, mais il est certainement reporté à des distances plus rassurantes. Le moment paraît dès lors venu de formuler les définitions, les idées essentielles qui pourraient ordonner la lex ferenda d'une société informatisée, avant qu'une végétation spontanée de règles n'obscurcisse irrémédiablement le terrain. A cette fin, il faut que la pensée, fidèle au discours de la méthode, se tourne vers ce qu'il y a de plus général, voire de plus abstrait. Or, l'informatique ayant pour fonction de traiter l'information et la télématique de la déplacer, ces deux disciplines opèrent sur un dénominateur commun, l'information, qui devrait logiquement se retrouver au coeur de toutes les difficultés juridiques qu'elles suscitent⁹³¹ ».* Cette option n'a pas été privilégiée par les lois informatiques et libertés sur le continent européen, pour y préférer la notion de donnée personnelle, et la référence à la protection de la vie privée. Bien qu'heureux, dans le sens de la prise en compte de la vie privée, ces choix légaux ont rendu la protection des données personnelles et de la vie privée incohérente, mal coordonnée, obscure.

⁹³¹ Ibid.

Partie 2: L'intégration parfaite de la surveillance diffuse dans l'évolution des notions juridiques de vie privée et de données personnelles

384. Ainsi que le premier temps de l'analyse a permis de le démontrer, la surveillance diffuse s'est insidieusement et progressivement mise en place sous l'égide des premières législations informatiques et libertés. La référence contenue dans ces dernières à la protection d'une liberté fondamentale, la vie privée, permettait au juge un travail de requalification de la donnée, ou du traitement considéré, en donnée à caractère personnel, ou en traitement de données personnelles. La référence, dans l'esprit de ces lois, d'une balance permanente entre des intérêts concurrents, marché et liberté, sécurité et liberté permettait également d'offrir une forme de protection. Bien que l'analyse de ces législations a permis de démontrer un déficit d'effectivité globale de ces dernières du fait même de la surveillance diffuse, il n'en reste pas moins que le droit des données personnelles se concevait alors comme un frein à l'élaboration pleine et entière d'un marché économique. La prise en compte de la vie privée dans ces législations primait alors sur l'ambition du marché. Pour le dire autrement, la vie privée et les données personnelles constituaient une entrave à ce marché et permettaient ainsi un semblant de protection.

385. Avec l'arrivée de nouvelles législations concernant la protection de données personnelles et de la vie privée⁹³², ainsi que de réflexions nombreuses en terme d'économie de la donnée⁹³³ - libre circulation des données non personnelles, transfert hors Union européenne - la question de l'intégration de la surveillance diffuse dans l'évolution de ces notions juridiques doit être réactivée. Si les premières législations informatiques et libertés souffraient d'un déficit d'effectivité globale,

⁹³² Notamment: Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, JOUE L 119 du 4 Mai 2016, p. 1 - 88, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR> (dernière consultation: 5 mars 2018), et 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 de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision - cadre 2008/977/JAI du Conseil*, JOUE L 119 du 4 Mai 2016, p. 89 - 131, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0680&from=FR> (dernière consultation: 5 mars 2018)

⁹³³ Notamment: Proposition de Règlement du Parlement européen et du Conseil, COM (2017) 10 final, *concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive de 2002/58/CE (règlement « vie privée et communications électroniques »)*, Bruxelles, 10 janvier 2017, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017PC0010&from=EN> (dernière consultation: 5 mars 2018); et Proposition de Règlement du Parlement européen et du Conseil, COM (2017) 495 final, *concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne*, Bruxelles, 13 Septembre 2017, En ligne: <http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-495-F1-FR-MAIN-PART-1.PDF> (dernière consultation: 5 mars 2018)

du fait d'un déficit de conscience des enjeux de la surveillance diffuse, l'élaboration du règlement général sur la protection des données personnelles⁹³⁴ est intervenue alors que nous découvrons les potentialités néfastes de la surveillance de masse. Dès le premier considérant du règlement général sur la protection des données, le législateur européen rappelle la fundamentalité du droit à la protection à l'égard des traitements de données à caractère personnel des personnes physiques⁹³⁵. Passant de l'expression « *l'informatique doit être au service des citoyens*⁹³⁶ » au principe selon lequel « *le traitement des données à caractère personnel devrait être conçu pour servir l'humanité*⁹³⁷ », le règlement, et plus globalement les nouvelles législations européennes en matière de protection de la vie privée, semblent *a priori* prendre acte des erreurs des premières législations informatiques et libertés.

386. Au delà de ces rappels empreints de bonnes intentions, le règlement général sur la protection des données annonce clairement son ambition dès son deuxième considérant: « *le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et **d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques***⁹³⁸ ». Et d'ajouter comme un rappel en contre-champs des jurisprudences de la CEDH: « *le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, **la liberté d'entreprise**, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique*⁹³⁹ ».

⁹³⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, *Op. Cit.*

⁹³⁵ « *La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant* ». Ibid. p. 1

⁹³⁶ Article 1er de la loi Informatique et Liberté

⁹³⁷ Considérant n°4 du Règlement général sur la protection des données (RGPD), p. 2.

⁹³⁸ Considérant n°2 du RGPD p. 1

⁹³⁹ Considérant n°4 du RGPD, p. 2

387. Reconnaissant l'augmentation substantielle des flux transfrontaliers de données à caractère personnel, le règlement « *appelle les autorités nationales des Etats membres à coopérer et échanger des données à caractère personnel*⁹⁴⁰ ». Par cet encouragement lancé aux Etats et aux entreprises à traiter de la donnée, les institutions de l'Union européenne permettent la pleine intégration de la surveillance diffuse dans la société contemporaine. Plus que cet encouragement, l'Union européenne, à travers l'ensemble de ces législations et réflexions, reconnaît le puissant enjeu économique et politique que représente la data. Par là, l'Europe tente de favoriser l'élaboration d'un marché économique construit au détriment des libertés. L'organisation de la désinstitution du droit des données personnelles et de la vie privée (titre 1) se profile en effet sous l'ambition du règlement général de protection des données à créer une gouvernance des données. De fait, la désinstitution du droit des données personnelles et de la vie privée permet à la surveillance diffuse d'obtenir une assise juridique et de se déployer toujours plus dans nos sociétés. Rappelant que « *les gens ont pris l'habitude non seulement de partager plus d'informations de toutes sortes, mais ils le font de façon plus ouverte et avec plus de gens*⁹⁴¹ », Mark Zuckerberg se félicitait d'avoir contribué à établir un changement de vision des individus sur leur vie privée, concluant que cette dernière n'est plus « *une norme sociale*⁹⁴² ». Bien que ces propos s'assimilent à une auto-promotion, l'analyse reste vraie. La vie privée aujourd'hui n'est plus une norme sociale. Pire encore, on constate la désinstitution du Droit au profit de la nouvelle norme sociale admise qu'est devenue la surveillance diffuse (Titre 2). La surveillance diffuse permet le passage de la réglementation à la régulation, du gouvernement des hommes à la gouvernance par la donnée. Il faut ainsi comprendre et analyser le passage du gouvernement à la gouvernance (ou de la réglementation à la régulation) qui s'est institué progressivement dans le vocabulaire juridique. Ainsi que le rappelle Alain Supiot « *le propre de la gouvernante est en effet de reposer non pas sur la légitimité d'une loi qui doit être obéit, mais sur la capacité commune à tous les êtres humains d'adapter leur comportement aux modifications de leur environnement pour perdurer dans leur être*⁹⁴³ ».

⁹⁴⁰ Considérant n°5 du RGPD, p. 2

⁹⁴¹ JOHNSON Bobbie, *Privacy no longer a social norm, says Facebook founder*, The Guardian, 11 janvier 2010, En ligne: <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> (dernière consultation: 5 mars 2018)

⁹⁴² Ibid.

⁹⁴³ SUPIOT Alain, *La Gouvernance par les nombres - Cours au Collège de France (2012 - 2014)*, Editions Fayard, Collection Poids et Mesures du Monde, 2015, p. 57

Titre 1: La désinstitution du droit des données personnelles et de la vie privée sous l'empire des nouveaux instruments européens

388. Le milieu des années 2010 a été une période prolifique en termes de propositions de nouvelles réglementations, directives, et réflexions concernant les données personnelles, leur libre circulation, leur transfert et leur traitement, la vie privée, mais également les données non personnelles. Au regard du foisonnement de textes, il peut paraître paradoxal d'évoquer la désinstitution du droit des données personnelles et de la vie privée. Pourtant, à la lecture de ces différentes réglementations, il apparaît clairement que nous sommes passés de l'affirmation d'une liberté (vie privée) dans l'espace numérique (droit des données personnelles), à une gouvernance de ce droit en vue de faciliter l'élaboration du marché unique numérique, fondement même de la surveillance diffuse.

389. La gouvernance ne recouvre pas totalement le même champ que le droit, tout comme la régulation des données personnelles ne recouvre pas tout à fait le même champ que la réglementation des données personnelles. Ainsi que le démontre Alain Supiot, « *l'état de délabrement institutionnel où se trouve plongée l'Europe procède d'une certaine façon de penser le gouvernement des hommes, qui est apparue à l'aube des temps modernes et continue de dominer son imaginaire normatif. Cet imaginaire consiste à se représenter le gouvernement comme une technique de pouvoir, comme une machine dont le fonctionnement doit être indexé sur la connaissance scientifique de l'humain⁹⁴⁴* ». Et de préciser que « *d'une manière générale, la gouvernance occupe une position centrale dans un champ sémantique qui congédie le vocabulaire de la démocratie politique au profit de celui de la gestion⁹⁴⁵* ». Gérer l'être humain par ses données (personnelles ou non), voici en réalité l'ambition de la surveillance diffuse.

390. Afin de réaliser cette ambition, l'organisation de la gouvernance des données personnelles par le règlement général de protection des données doit être analysée (Chapitre 1), tout comme la proposition de règlement visant à organiser la libre circulation des données non personnelles (Chapitre 2).

⁹⁴⁴ SUPIOT Alain, Op. Cit., p. 36

⁹⁴⁵ SUPIOT Alain, Op. Cit., p. 63

Chapitre 1: L'organisation d'une gouvernance des données personnelles au titre du règlement général sur la protection des données personnelles

391. Après de longs débats entre les institutions européennes et les entreprises américaines du numérique - les GAFAM - le règlement général de protection des données personnelles a été adopté le 4 mai 2016 par la Commission européenne, le Parlement européen et le Conseil de l'Union. Il entrera en vigueur le 25 mai 2018 et poursuit un objectif d'uniformisation des législations européennes concernant la protection des données à caractère personnel, souhaitant garantir un niveau élevé de protection des citoyens tout en favorisant l'innovation et le progrès technique et scientifique dans l'Union européenne. Le règlement a très vite été présenté comme une révolution, un acte novateur qui permettrait de renforcer « *considérablement les droits des citoyens en leur donnant une plus grande visibilité sur leurs données et une meilleure maîtrise sur l'utilisation qui en est faite*⁹⁴⁶ ».

392. Le juriste reste sceptique face à la nouveauté de cette législation qui demande à être vérifiée. A la lecture du règlement, ce dernier semble plus relever d'une tentative de combinaison de l'ancienne réglementation et d'une ambition de régulation économique que d'une réelle révolution en la matière. Concernant son champ d'application, le règlement n'opère aucune novation. Il a vocation à s'appliquer à tous les traitements de données à caractère personnel, qu'ils soient automatisés ou non. Les définitions clés de la protection des données à caractère personnelle ne subissent aucune évolution réelle. Ni le concept de traitement, ni le concept de données ne sont en effet enrichis ou remis en question. Certains traitements sont exclus du champ d'application de ce règlement. Ainsi en est-il par exemple des traitements « *qui ne relèvent pas du champ d'application de l'Union, telles que les activités relatives à la sécurité nationale*⁹⁴⁷ », et des traitements mis en oeuvre « *par une personne physique au cours d'activités strictement personnelles ou domestique*⁹⁴⁸ », « *par les autorités compétentes à des fins de prévention et de détection des*

⁹⁴⁶ En ce sens, voir: NEUER Laurence, *Protection des données personnelles: ce règlement qui inquiète les entreprises - Le nouveau règlement européen expose les entreprises et acteurs du Net à de lourdes sanctions financières. Quels en sont les enjeux ? Comment s'y préparer ?*, *LePoint.fr*, 8 Février 2018, En ligne: http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/protection-des-donnees-personnelles-ce-reglement-qui-inquiete-les-entreprises-08-02-2018-2193245_56.php (dernière consultation: 5 mars 2018), et LAZARD Jean-Marc, *L'Europe réglemente l'utilisation des données: une révolution à venir*, *L'express*, 20 Mars 2017, En ligne: https://lexpansion.lexpress.fr/actualite/reglement-general-sur-la-protection-des-donnees-une-revolution-imminente-a-l-echelle-europeenne_1890897.html (dernière consultation: 5 mars 2018)

⁹⁴⁷ Considérant n° 16 du Règlement: « *le présent règlement ne s'applique pas au traitement des données à caractère personnel par les Etats membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union* ».

⁹⁴⁸ Considérant n° 18 du Règlement

*infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données*⁹⁴⁹ ». Le règlement s'applique au responsable de traitement, ainsi qu'aux établissements ou entités qui traiteront des données en qualité de sous-traitant ayant un lien géographique avec l'Union européenne⁹⁵⁰. Le considérant 23 du Règlement précise en effet qu'il trouvera application à partir du moment où l'entité qui traite les données pour son compte ou pour le compte d'un tiers est située sur le territoire de l'Union européenne, mais également et surtout en fonction du lieu où se trouvent les personnes concernées par le traitement⁹⁵¹.

393. De fait, le règlement général sur la protection des données semble réaffirmer un champ d'application bien établi, tout en l'élargissant par la prise en compte de certaines nouvelles pratiques permises par les nouvelles technologies. Ainsi, en est-il du suivi du comportement des individus, le profilage⁹⁵². Pour autant, en réduisant sa portée à la prise en compte de l'économie de la data, ainsi qu'à la responsabilisation des acteurs à travers l'application du principe

⁹⁴⁹ Considérant n° 19 du Règlement. Ces traitements font l'objet d'un acte juridique spécifique à savoir la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, Op. Cit.

⁹⁵⁰ Voir: Groupe de travail « Article 29 » sur la protection des données, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, Adopté le 16 février 2010, 00264/10/FR, WP 169, En ligne: https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp169_fr.pdf (dernière consultation: 5 mars 2018). Le règlement précise qu'il s'applique « *aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités* » (Considérant n° 18). Et de préciser que: « *Tout traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union devrait être effectué conformément au présent règlement, que le traitement lui-même ait lieu ou non dans l'Union. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard* » (Considérant n° 22).

⁹⁵¹ Le considérant 23 énonce: « *Afin de garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit en vertu du présent règlement, le traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait être soumis au présent règlement lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non. Afin de déterminer si un tel responsable du traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'Union, il y a lieu d'établir s'il est clair que le responsable du traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union. Alors que la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'Union* ».

⁹⁵² Le considérant 24 déclare : « *Le traitement de données à caractère personnel de personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait également être soumis au présent règlement lorsque ledit traitement est lié au suivi du comportement de ces personnes dans la mesure où il s'agit de leur comportement au sein de l'Union. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit* ».

d'accountability (section 1), le règlement organise une véritable gouvernance des données. Cet instrument, dont l'objectif principal est de renforcer la sécurité juridique et pratique pour les personnes physiques, les opérateurs économiques et les autorités publiques⁹⁵³, manque de pertinence. Il s'avère, à l'inverse de son objectif, potentiellement dangereux en terme de sécurité juridique et de liberté (section 2).

Section 1: L'organisation d'une protection fondée sur la responsabilisation des acteurs: l'accountability ou la gouvernance des données personnelles

394. Le règlement général de protection des données réitère les grands principes généraux de la protection des données personnelles, tant concernant les traitements que les données elles-mêmes: le principe de licéité du traitement, de loyauté et de transparence, de limitation des finalités, les principes de minimisation et d'exactitude des données, de limitation de la conservation des données, de sécurité, d'intégrité et de confidentialité des données. Il vient également affirmer un principe essentiel d'accountability, corollaire de l'organisation de la gouvernance des données. Défini comme une obligation de rendre compte⁹⁵⁴, le principe d'accountability est clairement affirmé par le règlement dans le cadre de ses considérants⁹⁵⁵ et de ses articles⁹⁵⁶. Le chapitre 4 du règlement énonce ainsi dès son premier article que « *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 oeuvre 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*

⁹⁵³ En ce sens voir considérant n° 7 du RGPD.

⁹⁵⁴ CHOFFEL Denis, ALDRIN Jérémy, « Réflexions autour de la notion « d'accountability » à travers l'application d'une grille d'analyse sur deux études de terrain en management public », *Gestion et management public*, 2015/3 (Volume 4/n°1), p. 45-58, : <https://www.cairn.info/revue-gestion-et-management-public-2015-3-page-45.htm> (dernière consultation: 5 mars 2018). L'accountability n'est pas une découverte dans la protection des données personnelles. Voir: Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel, 23 septembre 1980, Disponible en ligne à l'adresse suivante: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> (dernière consultation: 5 mars 2018), mise à jour en 2013, En ligne: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (dernière consultation: 5 mars 2018). Voir également, Groupe de travail « Article 29 », *Avis 3/2010 sur le principe d'accountability*, Adopté le 13 juillet 2010, 00062/10/EN, WP 173

⁹⁵⁵ Considérants 17 à 78, 82 à 84, 89 à 96, et 98 à 100

⁹⁵⁶ Par exemple l'article 5 qui rappelle les principes relatifs au traitement des données à caractère personnel déclare en son paragraphe 2 que « *le responsable du traitement est responsable du paragraphe 1 et est en mesure de démontrer que celui ci est respecté (responsabilité)* ».

*actualisées si nécessaire*⁹⁵⁷ ». Appliqué aux données personnelles, le principe d'accountability dans le cadre du règlement, vise à « *la mise en oeuvre de politiques appropriées en matière de protection des données par le responsable du traitement*⁹⁵⁸ », ou à la possibilité de faire application de codes de conduites et de mécanismes de certifications⁹⁵⁹.

395. Si ces éléments participent d'une responsabilisation de la personne ou de l'entité en charge du traitement au travers d'un ensemble de documents et d'une organisation d'une politique Informatique et libertés, c'est principalement parce que le règlement voit en la vie privée et la protection des données personnelles un risque que les responsables de traitements doivent gérer (paragraphe 1). L'étude d'impact sur la vie privée en représente la parfaite illustration. Le règlement transforme également la vision que les responsables de traitement doivent avoir concernant la vie privée. En transformant cette dernière en un véritable argument marketing, au travers de la privacy by design, le règlement va bien plus loin qu'une simple gouvernance des données. Il vise en quelque sorte une gouvernance de la vie privée (paragraphe 2).

Paragraphe 1: L'intégration d'une logique risque dans le cadre de la protection des données personnelles: les études d'impact sur la vie privée

396. Si l'analyse d'impact sur la vie privée s'avère intéressante en terme de protection des données personnelles c'est essentiellement du fait de la prise en compte du risque inhérent au traitement de données personnelles en terme de garantie des droits et libertés fondamentales (A). Dans cette vision de la gouvernance des données, un élément positif est à souligner. Ainsi que nous l'avons démontré à chaque risque identifié dans la société correspond aujourd'hui une mesure de sécurité. Cette logique est prise en compte dans le cadre du règlement puisque ce dernier renforce l'obligation de sécurisation des données (B).

A. La prise en compte du risque lié au traitement de données personnelles dans le cadre de l'analyse d'impact sur la vie privée

397. Au préalable à l'évocation de l'organisation de l'étude d'impact sur la vie privée (2), il est

⁹⁵⁷ Article 24 du règlement paragraphe 1, p. 47.

⁹⁵⁸ Ibid. Paragraphe 2.

⁹⁵⁹ Ibid. paragraphe 3.

nécessaire de comprendre la logique du règlement. En effet, si cette étude permet d'intégrer une logique risque/avantage, ou plutôt risque/sécurité, il faut nécessairement comprendre de quels risques et de quels traitements il s'agit (1).

1. Des traitements susceptibles de présenter des risques pour les droits et libertés des personnes physiques

398. Le règlement général de protection des données personnelles déclare dans ses considérants que: « *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 risque⁹⁶⁰* ». La question essentielle est donc celle de l'origine, de la nature, de la particularité et de la gravité du risque lié à l'opération de traitement. Quels sont alors les risques identifiés par le règlement en terme de protection des données personnelles et de la vie privée ? Quelles sont les opérations de traitement à risque ?

399. A la première question, le règlement est particulièrement clair et énonce que des traitements de données personnelles peuvent engendrer des dommages physiques, matériel ou un préjudice moral. Ainsi en est-il « *lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les*

⁹⁶⁰ Considérant n° 84 du RGPD, p. 16

préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées⁹⁶¹ ».

400. Les opérations de traitements pouvant représenter un risque élevé sont également évoquées par le règlement. Les traitements concernés peuvent être envisagés sous deux catégories distinctes. La première regroupe les traitements présentant des risques particuliers du fait de leur nature, de leur portée, de leur contexte ou de leurs finalités⁹⁶². Dans cette catégorie, le règlement envisage en particulier les opérations de traitement de données particulières ou relatives à des infractions ou condamnations pénales, les évaluations automatisées, systématiques et approfondies d'aspects personnelles en vue de prendre une décision produisant des effets juridiques, les opérations de surveillances systématiques à grande échelle d'une zone accessible au public⁹⁶³. La seconde catégorie représente « *l'opération ou l'ensemble d'opération de traitement spécifique⁹⁶⁴* » réglementé par le droit d'un Etat membre et présentant des risques spécifiques pour les droits et libertés des personnes concernées.

401. A travers cette liste de risques et de traitement représentant un risque, le règlement se veut particulièrement large dans l'application de la responsabilisation des personnes ou des entités en charge du traitement. La surveillance diffuse s'intègre pleinement dans la description de ces risques: volume important de données, nombre important de personnes concernées, profilage, algorithme prédictif, marketing et sécurité sont en effet clairement identifiés comme des risques engendrés pas la surveillance diffuse et encadrés par le règlement général. Le règlement paraît donc présenter certaines garanties dans la prise en compte de la dangerosité de la situation actuelle. D'autant qu'il précise qu'il « *convient de déterminer la probabilité et la gravité des risques pour les droits et libertés de la personne en fonction de la nature, de la portée, du contexte et des finalités du traitement⁹⁶⁵* ». Et d'ajouter que le risque doit faire « *l'objet d'une évaluation objective permettant*

⁹⁶¹ Considérant n° 75 du RGPD, p. 15

⁹⁶² Considérants n° 90 du RGPD, p. 17, et article 35 du RGPD, p. 53 - 54

⁹⁶³ Considérant n° 91 du RGPD, p. 17 - 18.

⁹⁶⁴ Considérant n° 93 du RGPD, p. 18.

⁹⁶⁵ Considérant n° 76 du RGPD, p. 15

de déterminer si les opérations de traitements des données comportent un risque ou un risque élevé⁹⁶⁶ ».

2. L'organisation de l'étude d'impact sur la vie privée

402. Aidé par le délégué à la protection des données personnelles, le responsable de traitement doit *« tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement. Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'autorité de contrôle soit consultée avant que le traitement n'ait lieu⁹⁶⁷ »*. Que contient alors cette analyse ? Que recouvre le concept de mesures appropriées que le responsable de traitement doit prendre ?

403. L'article 35 du règlement général prévoit que l'analyse d'impact doit contenir *a minima « une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime, poursuivi par le responsable du traitement; une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités; une évaluation des risques pour les droits et libertés des personnes concernées (...); et les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées⁹⁶⁸ »*. Alors que le Règlement général sur la protection des données entrera en vigueur très prochainement, la CNIL a pu développer sa doctrine concernant les études d'impact sur la vie privée et la protection des données. Ainsi, dès l'introduction de sa méthode pour mener à bien une étude d'impact sur la vie privée⁹⁶⁹, la CNIL rappelle les deux piliers essentiels sur lesquelles cette dernière repose : *« 1. les principes et droits fondamentaux, « non*

⁹⁶⁶ Ibid.

⁹⁶⁷ Considérant n° 84 du RGPD, p. 16

⁹⁶⁸ Article 35 du RGPD, paragraphe 7, p. 54

⁹⁶⁹ CNIL, *PIA, La méthode - Etude d'impact sur la vie privée (EIVP), Privacy Impact Assessment (PIA) - Comment mener une EIVP, un PIA - Contexte, mesures, risques décision*, Edition 2015, En ligne: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf> (dernière consultation: 5 mars 2018)

« négociables », qui sont fixés par la loi et doivent être respectés et ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ; 2. la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel⁹⁷⁰ ».

404. L'étude d'impact sur la vie privée doit s'inscrire dans une démarche globale permettant de délimiter et décrire le contexte du traitement envisagé, ainsi que ses enjeux ; d'identifier les mesures existantes ou prévues pour prendre en compte les exigences légales et de traiter les données liées à la vie privée de manière proportionnée; d'apprécier les risques sur la vie privée pour vérifier qu'ils sont convenablement traités; de prendre la décision de valider de la manière dont il est prévu de respecter les principes de protection de la vie privée et de traiter les risques, ou bien réviser les étapes précédentes⁹⁷¹. Aussi, cette démarche doit s'inscrire dès la conception d'un nouveau traitement de données à caractère personnel, voire dès la conception d'un outil technologique. Il semble nécessaire d'ajouter deux précisions à la démarche proposée par la CNIL. D'une part, et dès le début du projet, ou dès l'ambition de création d'un traitement, il est fondamental d'adopter une approche compréhensive du vocabulaire juridique et technique. Une donnée entendue dans son acception technique n'est pas toujours une donnée à caractère personnelle, mais elle peut le devenir. Ainsi, il est crucial de se mettre d'accord sur l'unité de mesure (donnée), et de développer un esprit curieux afin de donner tout son sens à l'analyse d'impact sur la vie privée: s'inscrire dans une démarche de sécurité du système d'information, et de respect de la protection des données à caractère personnel, tout cela dans un ensemble de données métiers. D'autre part, et concernant la phase décisionnelle que porte en son sein la démarche proposée par la CNIL, l'acceptabilité est une notion centrale en termes de protection de la vie privée et de droit des données à caractère personnel. Elle doit pourtant être bien conçue comme une acceptabilité juridique visant à recourir au consentement, plutôt qu'une acceptabilité sociale visant à légitimer le traitement, ou l'objet technologique. Enfin, et pour conclure sur la méthode proposée par la CNIL, le rapport de l'analyse d'impact doit être rendu accessible aux autorités de protection des données.

405. En réalité, sous la prétendue nouveauté de cette analyse d'impact, on voit bien ici que l'on reprend très clairement les obligations que la directive de 95 et de la loi Informatique et libertés

⁹⁷⁰ Ibid. p. 4

⁹⁷¹ Voir Annexe 2

envisageaient sous couvert de l'analyse du degré d'intrusivité. Proportionnalité et nécessité de la mesure envisagée, mise en balance de deux « intérêts légitimes », sont autant de notions déjà présentes sous l'égide de ces deux instruments. La démonstration précédente a montré les failles de ce système. Reste à savoir si la formalisation dans le cadre du règlement de cette démarche en tant qu'obligation pesant sur le responsable de traitement suffira à pallier les failles précédemment démontrées.

B. Le renforcement de l'obligation de sécurisation des données : un élément positif dans l'intérêt du responsable de traitement

406. L'analyse d'impact sur la vie privée, du moins la méthode proposée par la CNIL, est fortement influencée par les analyses d'impacts sur les systèmes d'informations, en matière d'opérateur d'importance vitale⁹⁷² et de cybersécurité (1). Cet élément mérite d'être souligné car il emporte une conséquence clairement inspirée de ce domaine: le renforcement de l'obligation de sécurisation des données et plus globalement du système d'information (2).

1. Une influence nette des politiques de cybersécurité

407. La sécurité fait l'objet d'une attention particulière dans le règlement. La section 2 du chapitre 4 de ce dernier est entièrement consacrée à la sécurité des données à caractère personnel, et cette notion apparaît en filigrane de l'ensemble des dispositions du règlement. Ainsi, il est prévu que « *compte tenu de l'état des connaissances, des coûts de mise en œuvre et 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 et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque*⁹⁷³ ». Le niveau de sécurité adapté prôné par le règlement semble être atteint par la mise en place d'une méthode d'évaluation des risques d'atteintes aux données envisagée sous couvert de l'étude d'impact sur la vie privée. Le considérant n° 85 précise que la violation de données à caractère personnel est caractérisée lorsqu'est constaté une perte de contrôle sur ces données, la limitation des droits des personnes concernées, une discrimination, un vol ou une usurpation d'identité, un renversement non autorisé de la procédure

⁹⁷² Voir en ce sens Annexe 2 et 3.

⁹⁷³ Article 32 du RGPD paragraphe 1, p. 51

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. Ces éléments rappellent les dispositions de la directive de 1995 et la loi de 78 concernant la destruction, l'altération, la divulgation et l'accès non autorisé à de telles données.

408. L'innovation du règlement se présente alors par une réelle politique de sécurité des données calquée sur la politique de cybersécurité⁹⁷⁴. C'est notamment le considérant 49 du règlement qui illustre cette inspiration. Il déclare: « *le traitement de données à caractère personnel dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations, c'est-à-dire la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux et de services de communications électroniques et des fournisseurs de technologies et services de sécurité, constitue un intérêt légitime du responsable du traitement concerné. Il pourrait s'agir, par exemple, d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par « déni de service » et des dommages touchant les systèmes de communications informatiques et électroniques*⁹⁷⁵ ». On notera qu'à l'initiative du Parlement européen et du Conseil, et dans un contexte de prise en compte de nouvelles menaces,

⁹⁷⁴ A ce titre on citera ici le rapport Lasbordes, publié le 13 janvier 2006 et intitulé la sécurité des systèmes d'information – un enjeu majeur pour la France, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000048.pdf> (dernière consultation: 5 mars 2018); le rapport Romani, du 8 juillet 2008, intitulé Cyberdéfense : un nouvel enjeu de sécurité nationale, En ligne: <https://www.senat.fr/rap/r07-449/r07-4491.pdf> (dernière consultation: 5 mars 2018), le rapport Bockel du 18 juillet 2012 intitulé La cyberdéfense : un enjeu mondial, une priorité nationale, En ligne: <https://www.senat.fr/rap/r11-681/r11-6811.pdf> (dernière consultation: 5 mars 2018), le livre blanc sur la défense et sécurité nationale de 2008, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf> (dernière consultation: 5 mars 2018), et de 2013 : <http://fr.calameo.com/read/000331627d6f04ea4fe0e> (dernière consultation: 5 mars 2018), Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. JORF n°0294. 19/12/2013. p. 20570. texte n° 1, En ligne: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id> (dernière consultation: 5 mars 2018), mais également: Commission des Communautés européennes, Com (2005), Livre vert sur un programme européen de protection des infrastructures critiques, présenté par la Commission, Bruxelles, le 17 novembre 2005, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52005DC0576&from=FR> (dernière consultation: 5 mars 2018)

⁹⁷⁵ Considérant n° 49 du RGPD, p. 9

une proposition de directive⁹⁷⁶ concernant des mesures a été imaginé pour tenter d'assurer un niveau élevé commun de sécurité des réseaux et de l'information de l'Union. L'objectif de ce texte est de sécuriser les systèmes d'information de certaines installations afin de prévenir tout risque d'intrusion malveillante et de piratage. Ce texte précise notamment les obligations à la charge des opérateurs d'infrastructures essentielles, similaires à celles imposées aux opérateurs d'importance vitale par la loi de Programmation Militaire de 2013. La directive entend s'appliquer aux opérateurs publics (mis à part les autorités judiciaires) et privés, aux opérateurs d'importance vitale (ou pour reprendre la dénomination européenne aux opérateurs d'infrastructure essentielle), aux fournisseurs de services numériques (sites de e-commerce, de cloud computing, moteurs de recherche). A travers cette directive, l'Europe entend poser un cadre global pour la protection des opérateurs essentiels, que chaque pays aura la responsabilité de transposer sur son territoire. Alors qu'elle n'était pas encore adoptée⁹⁷⁷ lors de l'adoption du règlement⁹⁷⁸, ce dernier a opéré une véritable anticipation de la directive NIS par application de l'existant, c'est-à-dire par application des éléments issus de la protection des infrastructures critiques et spécialement issue de la politique de sécurité des systèmes d'informations⁹⁷⁹.

409. De manière globale les Opérateurs d'Importance Vitale⁹⁸⁰ (OIV) doivent d'abord dresser la cartographie de leurs systèmes d'information d'importance vitale, la tenir à jour et la fournir à l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). Ils doivent définir et tenir à jour une politique de sécurité de leur système d'information (PSSI) approuvée par la direction de l'entreprise. Cette PSSI correspond en réalité à une véritable étude et analyse d'impact sur le système d'information. Cette dernière a pour objectif de formuler des orientations stratégiques en matière de sécurité des systèmes d'information (SSI) et de gestion de risques pour l'infrastructure concernée (secteur privé ou public). La PSSI doit alors décrire les éléments stratégiques, tels que les enjeux, les référentiels, les principaux besoins de sécurité, et les menaces, ainsi que les règles de

⁹⁷⁶ Directive NIS (Network and Information Security)

⁹⁷⁷ Une position de principe a été trouvée entre le Conseil et le Parlement européen en date du 17 mai 2016. En ligne: <http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf> (dernière consultation: 5 mars 2018).

⁹⁷⁸ La directive NIS sera adoptée le 6 juillet 2016: Directive (UE) 2016/1148 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, JOUE du 19 juillet 2016, L 194, p. 1 -30, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=FR> (dernière consultation: 5 mars 2018)

⁹⁷⁹ En ce sens voir annexe 2 et 3

⁹⁸⁰ Acteurs principalement touchés par la politique de sécurité des systèmes d'information avant le règlement et la directive NIS

sécurité applicables à la protection du système d'information de l'organisme.

410. Pour rappel, l'ambition de la LPM, ainsi que de ces arrêtés sectoriels est bien de faire de la sécurité des systèmes d'information un élément de la qualité de l'organisme. Cette dernière étant devenue un facteur indispensable au bon fonctionnement de l'entreprise ou de l'entité publique concernée. La PSSI fournit, dans ce cadre, un support au DSI, ou au responsable de la sécurité des systèmes d'information pour améliorer la sécurité de son système d'information. Les méthodes d'élaboration de la PSSI sont relativement claires depuis 2004⁹⁸¹. La mise en œuvre de cette PSSI doit faire l'objet d'un rapport annuel à la direction. L'Opérateur d'Importance Vitale doit procéder à « l'homologation » de son système d'information. Cette homologation correspond à une décision formelle prise par l'opérateur, à la suite d'un audit de sécurité, qui atteste que les risques pesant sur la sécurité de son système ont été identifiés et que les mesures nécessaires pour le protéger, sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'opérateur. Les arrêtés sectoriels pris en application de la loi de programmation militaire fixent également, et de manière non exhaustive des règles en matière d'authentification et de journalisation des accès au système d'information, d'analyse des logs, de système de détection d'intrusion, de traitement des incidents et alertes de sécurité, de comptes d'administration, de cloisonnement des applicatifs. Ces mêmes procédures sont mises en place par le règlement

2. Le renforcement de l'obligation de sécurisation

411. Globalement, le règlement prévoit que la politique de sécurité concernant les données personnelles doit porter notamment sur les méthodes d'identification et d'authentification des utilisateurs, la gestion des habilitations, la sensibilisation et la formation des utilisateurs à la culture informatique et libertés, la traçabilité et la journalisation des accès et de toutes actions sur les données, sécurisation des postes de travail et de l'informatique mobile et nomade, gestion des incidents, sécurisation des locaux, du réseau interne, des serveurs et des applications, sécurisation des échanges avec les tiers, chiffrement, anonymisation ou pseudonymisation des données le cas échéant, archivage et sauvegarde sécurisés, lutte contre la vulnérabilité des canaux informatiques (surveillance de l'activité du réseau, interdiction de toute communication directe entre des postes internes et l'extérieur, cloisonnement des réseaux en sous-réseaux, interdiction de raccordement

⁹⁸¹ Voir annexe 3

d'équipements informatiques non maîtrisés, etc.), mais également des canaux « papiers », mise à jour des logiciels et anti-virus. On le voit à travers cette liste tirée des considérants et des articles du règlement, la politique de sécurité visée par le règlement touche à la fois la sécurité physique et la sécurité logique du responsable de traitement. Tirant les enseignements de la PSSI, le règlement impose l'application d'un code de conduite ou d'un mécanisme de certification approuvé qui peut servir d'élément attestant du respect des exigences de sécurité⁹⁸². Un véritable audit de sécurité est mis en place, et doit être déployé par le responsable de traitement ou le sous-traitant, tout au long de la vie du traitement.

412. Le règlement envisage également plus particulièrement la gestion des failles de sécurité. Ainsi, dès lors qu'une violation de données à caractère personnel est constatée, le responsable de traitement devra notifier « *à l'autorité de contrôle dans les meilleurs délais et, lorsque c'est possible, 72 heures au plus tard après en avoir pris connaissance, à moins qu'il ne puisse démontrer, conformément au principe de responsabilité, qu'il est peu probable que la violation en question engendre un risque pour les droits et libertés des personnes physiques. Si une telle notification ne peut avoir lieu dans ce délai de 72 heures, la notification devrait être assortie des motifs du retard et des informations peuvent être fournies de manière échelonnée sans autre retard indu*⁹⁸³ ». Aussi, si la violation présente un risque élevé pour les droits des personnes concernés, cette faille devra être notifiée à cette dernière.

413. S'il est certain que le renforcement de l'obligation de sécurisation des données personnelles, et plus globalement du système d'information du responsable de traitement participe de l'objectif de renforcer la confiance dans les technologies de l'information et de la communication, on pourrait s'interroger sur les bénéfices réels pour le responsable de traitement. Ces mesures drastiques, calquées sur la politique de sécurité des système d'information d'importance vitale, ont certes un

⁹⁸² Article 40 du règlement

⁹⁸³ Article 33 du RGPD et spécialement ici considérant n° 85

coût technique⁹⁸⁴ et financier⁹⁸⁵, mais elles présenteront également un avantage certain pour le responsable de traitement. En effet, sous l'égide de la directive de 1995 et de la loi de 1978 le seul élément réellement craint par les entreprises et l'Etat, en charge de traitement, ne résidait pas dans l'application de ces textes. La politique du « pas vu-pas pris » régnait. Et lorsque les responsables de traitement ou l'entité en charge du traitement « se faisait prendre », c'est surtout la mauvaise publicité dans la presse, pouvant ternir son image de marque, ou une politique, qui était à craindre⁹⁸⁶. L'obligation renforcée de sécurisation des données permet ici un double avantage: la gouvernance des données en amont, le rétablissement de la (fausse) confiance des usagers, citoyens, utilisateurs et consommateurs. Aussi, cette obligation permet à l'entreprise, ou l'Etat, de sécuriser son patrimoine informationnel constitué entre autre par des données personnelles et non personnelles.

414. Bien que positive, cette obligation s'inscrit pleinement dans ce que la Privacy by design aura permis de peaufiner: la réduction de la vie privée à un argument marketing, et la future gouvernance de la vie privée, non plus par les individus, mais bien plutôt par les entreprises, les Etats, toutes entités en charge d'un traitement.

Paragraphe 2: La réduction de la vie privée à un argument marketing: la privacy by design

415. La privacy by design n'est pas une notion récente. Là encore sous la prétendue nouveauté du règlement, le juriste doit vérifier de quoi il s'agit vraiment. Ainsi, les origines de cette notion attestent d'un défaut de conception originelle La privacy by design, à son origine, était conçue comme un élément de remplacement au droit des données à caractère personnelles (A). Cet élément particulièrement éclairant quant à la potentialité néfaste que la privacy by design porte en son sein: la réduction de la vie privée à un argument marketing (B).

A. Les origines d'une notion potentiellement dangereuse en terme de droits et libertés des personnes concernées par des traitements de données à caractère personnel

⁹⁸⁴ On pense ici à l'anonymisation et à la pseudonymisation

⁹⁸⁵ Investissement dans la sécurité physique, coût supplémentaire liée au délégué à la protection des données personnelles...

⁹⁸⁶ On pense ici à l'exemple de la RATP et de son pass Navigo, de l'Etat français face au fichier EDVIGE ou TES.

416. Ainsi que le rappelait Jean Jacques Lavenue dans un article de 2012 s'interrogeant sur le choix à faire entre la privacy by design et la privacy by law: « *la « privacy-by-design » repose sur un concept fondamental aux contours incertains. La « Privacy » n'est pas la vie privée stricto sensu, et recouvre encore moins la notion de données personnelles telle que nous la connaissons en droit français, et plus largement, à l'échelle du droit applicable dans l'Union européenne. La notion de privacy pose un problème technique pour les juristes français. C'est un export linguistique d'un concept dont le développement est beaucoup plus étroit qu'un emprunt aux systèmes de Common Law. La privacy prise dans la logique industrielle trouve ses fondements dans un concept existant dans l'ordre juridique des Etats-Unis⁹⁸⁷ ».*

417. Alors que le début des années 2000 est profondément marqué par la recherche de solutions alternatives à la protection des données personnelles par le Droit, des notions telles que les privacy enhancing technologies (PET'S) et la privacy by design apparaissent. Alors que la première notion paraît séduisante, la seconde fait débat. Les PET's, encore appelée technologies renforçant la protection de la vie privée vise en réalité à promouvoir la conception de technologies de l'information et de la communication réduisant la collecte et l'utilisation de données à caractère personnel et à faciliter le respect des règles de protection des données. Elles correspondent à des procédés de cryptage, d'anonymisation et de pseudonymisation, ainsi que plus largement à des procédés anti-cookies pour la navigation sur Internet⁹⁸⁸. La seconde notion correspond au fait global de vouloir prendre en compte la vie privée dès la conception de l'outil technologique. S'il est vrai que cet objectif est séduisant pour assurer la protection des données personnelles, ce dernier n'est pas à l'origine sa vocation première. Ainsi que le rappelle le professeur Jean-Jacques Lavenue, pour Ann Cavoukian⁹⁸⁹ « *le droit y paraîtrait même, comme hypothèse de départ, disqualifié pour non-efficience. Ainsi qu'Ann Cavoukian le souligne sur son site : «La protection intégrée de la vie privée est fondée sur le principe selon lequel la protection de la vie privée ne pourra être assurée par le simple respect des lois et cadres réglementaires et doit, idéalement, être intégrée dans les*

⁹⁸⁷ LAVENUE Jean-Jacques, BAUDEN-HAMEREL Gaylord, DESRUMEAUX Nicolas, CODRON Clémence, « Privacy by design ou privacy by law? », *Revue Droit International, Commerce, Innovation et Développement (DICID)*, n° 2/2012, novembre 2012, Presses de l'Université de Bourgogne, pp. 77 - 104, p. 77, Disponible en ligne à l'adresse suivante <http://credimi.u-bourgogne.fr/images/stories/pdf/dicid%202-4.pdf> (dernière consultation: 5 mars 2018), Voir également: LAVENUE Jean-Jacques, « La privacy by design, panacée ou cheval de Troie ? », *Revue de la Recherche Juridique - Droit Prospectif*, 2013 - 1, pp. 59 - 73

⁹⁸⁸ Voir en ce sens: http://europa.eu/rapid/press-release_MEMO-07-159_fr.htm (dernière consultation: 5 mars 2018)

⁹⁸⁹ Docteur en psychologie et principale instigatrice du concept de privacy by design

activités de l'organisation ». ⁹⁹⁰ ».

418. En réalité, les technologies renforçant la protection des données personnelles et la *privacy by design* de Ann Cavoukian correspondent à ce que le règlement est parvenu à engendrer: une intégration de la vie privée dans une conception marketing. La prise en charge de la protection de la vie privée par l'industrie est exactement ce à quoi le règlement est parvenu, et qui était en germe dans la conceptualisation originelle de *privacy by design*. Un ensemble de lignes directrices, de guides de bonnes pratiques étaient même envisagée par Ann Cavoukian⁹⁹¹. Or, ces éléments ne sont pas du droit pur, ne permettent pas de vérifier l'efficacité d'une mesure, ni de contrôler véritablement le responsable de traitement. Cela explique certainement la diffusion de cette notion par, ce que Jean-Jacques Lavenue désignait comme des « *prosélytes agents de diffusion*⁹⁹² » principalement rattachés à des entreprises du numérique. Ces mêmes « *prosélytes agents de diffusion* » qui ont participé à l'élaboration du règlement général de protection des données.

419. Opérant une sorte de renversement de l'effectivité, garantie non plus par le droit mais par la confiance absolue en les responsables de traitements, la notion de Ann Cavoukian s'est pourtant diffusée largement, au point d'être contenue dans le règlement général de protection des données personnelles. S'il est vrai que d'autres mécanismes que le droit peuvent participer de la protection des données personnelles, il semble qu'il faille éclaircir leur place et leur rang. Si ces mécanismes remplacent l'effectivité du droit, c'est bien l'individu et la personne concernée par les traitements qui seront les principaux perdants.

B. La possibilité de réduire la vie privée à un argument marketing : la *privacy by design* dans le règlement général de protection des données personnelles

420. Le règlement général de protection des données personnelles affirme la *privacy by design* et la *privacy by default* comme des concepts opérants de la protection des données personnelles. Ces éléments sont des concepts clés du principe d'*accountability* que le règlement met en place. Le champ d'application de ces instruments doit être vérifié (1) afin de comprendre si la *privacy by law* est toujours d'actualité (2).

⁹⁹⁰ Op. Cit. p. 81

⁹⁹¹ Op. Cit. p. 83

⁹⁹² Op. Cit. P; 85

1. Champ d'application de la privacy by design sous l'égide du règlement

421. Si la privacy by design peut poser problème en terme d'utilisation du concept de privacy, le règlement vient en son article 25 affirmer la protection des données dès la conception et la protection des données par défaut. Plus précisément, cet article déclare que « *le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée*⁹⁹³ ». Son paragraphe 2 déclare que « *le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, 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*⁹⁹⁴ ».

422. Par la référence directe aux principes relatifs à la protection des données à caractère personnel, il semble *a priori* que le règlement prenne acte de l'importance et de l'effectivité du droit face aux simples mesures techniques. Au vu de ces articles, la protection des données personnelles devra être intégrée dès la conception des systèmes et des technologies mis en place. Le but principal est ici d'intégrer les possibles risques liés à l'application des principes fondamentaux de la protection des données personnelles, et de les anticiper tant en phase de détermination des moyens du traitement qu'au moment de sa mise en œuvre. Outre son lien avec le principe de minimisation des données personnelles⁹⁹⁵, la privacy by design telle qu'envisagée dans le règlement met en place un certain formalisme permettant de mettre en oeuvre cette démarche pas à pas. Ainsi est-il

⁹⁹³ Article 25 du RGPD, p. 48

⁹⁹⁴ Ibid.

⁹⁹⁵ Ce principe rappelé à l'article 5.1. c) du RGPD, et déjà présent dans le cadre des premières législations informatiques et libertés en vertu duquel les données personnelles doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* »

recommandé par exemple de mettre en place, au vu du principe d'accountability, un registre des activités de traitement. Plus en amont, la lecture des considérants du règlement semble imposer également un formalisme. En effet, le règlement précise que « *lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics*⁹⁹⁶ ».

423. Enfin, la protection des données par défaut semble dans les faits recouvrir les principes essentiels de la protection des données personnelles, déjà présents dans le cadre des premières législations informatiques et libertés: minimisation des données, proportionnalité entre les données collectées et le traitement envisagé, principe de pertinence, durée de conservation limitée, accessibilité.

2. Une tentative de réduction de la vie privée à un argument marketing ?

424. Si de prime abord la logique de privacy by design du règlement général de protection des données se réfère au droit, le paragraphe 2 de l'article 25 se réfère quant à lui à des mécanismes de certification de cette démarche pouvant « *servir d'élément pour démontrer le respect des exigences*⁹⁹⁷ » liées à la privacy by design et à la privacy by default.

425. Opérant par renvoi à l'article 42 du règlement, ce mécanisme de certification estampillé privacy by design et privacy by default laisse planer le doute du retour clair à un privacy by law. Dès le premier paragraphe, le juriste est assez surpris des mécanismes mis en place : « *les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des*

⁹⁹⁶ Considérants n° 78 du RGPD, p. 15

⁹⁹⁷ Article 25 du RGPD, Op. Cit.

données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération⁹⁹⁸ ». Le respect de la vie privée, ou plus précisément le respect de la protection des données personnelles deviendrait-il une marque, un label au même titre qu'un label bio est apposé sur des oeufs de poules élevées en plein air ? Cette incitation au respect de la protection des données personnelles, sous cette forme⁹⁹⁹, est-elle réellement faite dans l'intérêt de la protection des données personnelles, et, par voie de conséquences, des individus ?

426. Bien que la suite de cet article précise que l'obtention d'une certification « *ne diminue pas la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement et est sans préjudice des missions et des pouvoirs des autorités de contrôle¹⁰⁰⁰* », il n'en reste pas moins que les mécanismes de certification et de labellisation offrent aux responsables de traitements une véritable possibilité de réduire la protection des données personnelles à un argument marketing. Ainsi que le rappelait le professeur Jean-Jacques Lavenue, « *l'existence de standards ne correspond pas en soi à des normes techniques et industrielles telles qu'elles s'entendent à l'échelle économique. Hors du champ strict de la norme juridique, la normalisation constitue à la fois l'état de l'art, l'étalon ou la référence technique d'un secteur ou d'un type de produits ou de services, au profit de leur commercialisation. La dimension de la normalisation fait de plus en plus partie du lot commun lié à l'intelligence économique et à la compétitivité, lorsque la « normalisation informelle » rend l'Etat aveugle face à des organisations nord-américaines hors tutelle des Etats et des organisations de normalisations telles que l'ISO ou l'AFNOR. Elles permettent d'établir des standards de fait excluant la garantie de participation équilibrée telle que voulue dans les institutions recevant une participation des Etats¹⁰⁰¹ ».*

427. Fondés essentiellement sur des codes de bonnes conduites et des lignes directrices, tout se passe comme si ces mécanismes de certifications et de labellisation permettaient de réduire la vie privée à un argument marketing. Consensualisme des industriels, agrégation de leurs connaissances

⁹⁹⁸ Article 42 du RGPD, p. 58

⁹⁹⁹ Qui a prouvé en d'autres domaines être totalement inadéquate, voir par exemple: Extrait de « Razzia sur le bois » une enquête de Cash Investigation, diffusée le 24 janvier 2017 à 20h55 sur France 2, En ligne: https://www.francetvinfo.fr/france/video-cash-investigation-des-labels-en-bois_2012290.html (dernière consultation: 5 mars 2018)

¹⁰⁰⁰ Article 42 du RGPD; paragraphe 4, p. 59

¹⁰⁰¹ LAVENUE Jean-Jacques, *Op. Cit.*, p. 78

et de leurs pratiques concernant une technologie ou un traitement particulier, validation de ces éléments par des autorités de normalisation permettent en effet de définir *a minima* une méthodologie, ou pour reprendre les termes du Professeur Lavenue de « *définir le périmètre d'accès à une technologie*¹⁰⁰² » à l'instar, en France, des technologies biométriques. Avec le règlement général, il semble que, plus que le simple périmètre d'accès à la technologie, ces procédures de certification et de labellisation vise à définir le périmètre minimal du droit à la vie privée à respecter. Quand il est envisagé de se soumettre à ces codes de conduite et à ces certifications, non juridiques, il est recommandé de choisir ceux qui auront été agréés par l'autorité de contrôle compétente. Si rien n'est vraiment évoqué sur ces procédures d'agréments, on peut s'inquiéter de voir apparaître, à l'image des instituts de normalisation tels que l'ISO ou l'AFNOR, des « normes » relatives à la vie privée. Le groupe normalisation de l'AFNOR a, par exemple, envisagé en 2017 un guide dédié à l'apport des normes volontaires quant à la protection des données personnelles¹⁰⁰³. Les normes volontaires relatives à la protection de la vie privée sont, selon l'AFNOR, « *des outils de co-régulation complémentaires au cadre légal et réglementaire. (...) Lancée à l'initiative des acteurs du marché, la norme volontaire est un cadre de référence qui vise à fournir des lignes directrices, des prescriptions techniques ou qualitatives pour des produits, services ou pratiques au service de l'intérêt général*¹⁰⁰⁴ ». Plusieurs éléments doivent ici être relevés.

428. On peut, en effet, s'étonner que le chef du service de l'expertise technologique de la CNIL écrive dans ce guide que les normes volontaires prônées par l'AFNOR « *seront incontournables pour mettre en place un système de management en sécurité informatique, cadre de progrès qui devra notamment intégrer la protection des données personnelles*¹⁰⁰⁵ ». Qu'en est-il du droit ?

¹⁰⁰² Ibid. p. 79

¹⁰⁰³ Au titre de ce guide, les normes volontaires sont des outils « *insoupçonnés, inventées par les organisations elles-mêmes, par consensus après concertation. (...) Par ailleurs, le législateur européen et les autorités de contrôle considèrent désormais que la responsabilisation des organisations (notion d'« accountability » en anglais) doit devenir la pierre angulaire de la protection de la vie privée. L'approche préconisée consiste à mettre en œuvre des mesures pour satisfaire aux exigences légales ou réglementaires et à être en capacité d'en rendre compte. Dans ce contexte, l'organisation internationale de normalisation (ISO) et la commission électro-technique internationale (IEC) jouent un rôle déterminant. Et c'est grâce à l'engagement et aux compétences des professionnels qui apportent leurs connaissances au comité technique commun pour la sécurité des technologies de l'information dénommé (JTC 1/SC 27). Un groupe de travail est d'ailleurs dédié à la protection des données personnelles (WG 5 du SC 27). L'un des objectifs de ce groupe de professionnels est de faire en sorte que les normes volontaires puissent efficacement contribuer à la mise en œuvre de solutions pour protéger les données personnelles et la vie privée* ». AFNOR, *Guide protection des données personnelles - l'apport des normes volontaires*, Janvier 2017, p. 3, Disponible en ligne à l'adresse suivante : https://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf (dernière consultation: 5 mars 2018)

¹⁰⁰⁴ Ibid. p. 19

¹⁰⁰⁵ Ibid. p. 4

N'est-ce pas plutôt lui qui devrait être incontournable, plutôt que des normes envisagées par consensus et concertation d'entreprises et d'autorité de contrôle ? On peut également s'étonner que des normes telles que celles représentant le cadre de la vie privée¹⁰⁰⁶ soient jugées comme définissant les principes et la terminologie relatif à la protection de la vie privée, représentant une référence dans la gestion des mesures de protection des données personnelles d'une organisation, compatibles avec le cadre légal européen et, en tant que norme internationale, devant s'analyser comme d'application recommandée. Au vu de la conclusion du guide de l'AFNOR évoquant la priorité des autorités de contrôle européennes « *d'établir une norme d'exigences afin de réaliser des certifications de système de management intégrant la protection de la vie privée* », la logique du questionnement concernant la priorité à donner entre privacy by design ou la privacy by law doit être réactivée. On devrait même dire plus simplement que le futur réservé par ces modes d'actions a-juridique poseront bientôt la question du choix à faire entre la réglementation et la régulation, entre le Droit et la Norme ?

Section 2: Le règlement général de protection des données personnelles: un instrument dangereux en terme de sécurité juridique et de libertés

429. Le traitement de données personnelles a toujours été fondé sur le consentement préalable de la personne concernée. En ce que le règlement général de protection des données personnelles vient préciser les contours de la licéité des traitements de données personnelles, il apparaît que le consentement n'est plus une base légale au traitement de données personnelles (paragraphe 1). En cela, le règlement pose déjà un premier problème en terme de sécurité juridique, et de protection des libertés. Malgré la mise en place de gardes-fous (paragraphe 2), il faut, avant même son application réelle, prendre acte de la dangerosité du règlement général de protection des données personnelles.

Paragraphe 1: Licéité du traitement de données personnelles et consentement de la personne concernée

430. L'article 6 du Règlement général de protection des données personnelles opère une évolution radicale dans le cadre de la licéité du traitement de données. Jusqu'alors le consentement était le principe essentiel de tout traitement de données personnel, il devient aujourd'hui

¹⁰⁰⁶ Norme ISO/IEC 29100, Privacy Framework, voir le guide précité, p. 15

l'exception. L'article 6 déclare en effet que « 1. *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie: a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions*¹⁰⁰⁷ ».

431. L'instauration de ce double régime de traitement de données personnelles permet au responsable de traitement de choisir la base juridique de son traitement: traitement avec consentement (A) et traitement sans consentement (B). Ce double régime doit être analysé attentivement. Si ce double régime est en lui-même dangereux pour la sécurité juridique, la présentation de cette double hypothèse démontrera que l'une des bases légale du traitement de données (sans consentement) est essentiellement liée à l'intérêt légitime du responsable de traitement, si ce dernier est une entreprise, et, de l'intérêt général si ce dernier est un Etat¹⁰⁰⁸. En

¹⁰⁰⁷ Article 6, paragraphe 1 concernant la licéité du traitement, RGPD, p. 36

¹⁰⁰⁸ Voir en guise d'exemple: 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, Spécialement son considérant n°35 que nous reproduisons en partie ici: « *Pour être licite, le traitement des données à caractère personnel au titre de la présente directive devrait être nécessaire à l'exécution d'une mission d'intérêt général par une autorité compétente, fondée sur le droit de l'Union ou le droit d'un État membre, 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Ces activités devraient couvrir la protection des intérêts vitaux de la personne concernée. Dans le cadre de l'exécution des missions de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander ou ordonner aux personnes physiques de donner suite aux demandes qui leur sont adressées. Dans ce cas, le consentement de la personne concernée, au sens du règlement (UE) 2016/679, ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes. Lorsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix; sa réaction ne pourrait dès lors être considérée comme une manifestation libre de sa volonté* ».

cela, le règlement est également dangereux en terme de respect des droits et libertés fondamentales.

A. La fin progressive du principe des traitements avec consentement

432. Le règlement propose une nouvelle définition de ce que recouvre le consentement (2). Si la proposition d'une nouvelle définition est louable, encore faut-il vérifier si elle permet plus ou moins de sécurité juridique dans le domaine du traitement des données personnelles. Il faut également comprendre et analyser quels traitements sont concernés par le recueil du consentement préalable (1).

1. Les traitements concernés par le recueil du consentement préalable

436. Au delà de l'option laissée au responsable de traitement quant au choix de base juridique du traitement - sans consentement ou avec consentement, le règlement envisage certains cas où le consentement doit être recueilli préalablement. Avant de rentrer dans ces détails, il faut être assez clair sur le sujet. Sous l'empire de la loi de 1978 et de la directive de 95, le recueil du consentement préalable au traitement n'était que peu respecté. Avec le règlement, et cette possibilité de choix de base juridique au traitement, il y a fort à parier que bon nombre de responsable de traitement s'orienteront vers des traitements sans consentement.

437. Les cas de traitements avec recueil de consentement prévus par le règlement sont peu nombreux. Ils visent essentiellement des catégories de données dites « particulières ». Cette nouvelle catégorie de données recouvre en réalité les anciennes données sensibles. Pour rappel, le traitement de données sensibles était interdit sauf exceptions encadrées par la loi et ou la directive de 1995. Le paragraphe 1 de l'article 9 du règlement précise ainsi que : « *le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits*¹⁰⁰⁹ ». Si l'élargissement de la liste des données sensibles, devenues des données particulières, est intéressant; tout comme le rappel de

¹⁰⁰⁹ Article 9 du RGPD, p. 38

l'interdiction de principe de leur traitement, toute personne physique peut donner son consentement au traitement de ces données, et donc lever l'interdiction. Alors que les individus commencent seulement aujourd'hui à s'intéresser à la question de leurs données personnelles, vont-ils comprendre l'intérêt de la protection de ces données particulières ? En d'autres termes, lorsque la base juridique de ce type de données sera le consentement, seront-ils suffisamment informés du caractère éminemment sensible pour leur vie privée de ce type de traitement ? Il faut également préciser que dans le cas de traitement de données particulières, le consentement peut être remplacé par d'autres conditions, telles que la recherche scientifique, la médecine préventive ou la médecine du travail, l'intérêt public dans le domaine de la santé publique, des motifs « *d'intérêt public important*¹⁰¹⁰ », ou encore quand ces données ont été rendues publiques par la personne concernée, quand le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, à l'exécution des obligations et de l'exercice des droits propres au responsable de traitement en matière de droit du travail, de la sécurité sociale et de la protection sociale.

438. Les traitements qui auront pour base juridique le consentement préalable de la personne concernée devront en tout état de cause respecter les principes relatifs au traitement de données à caractère personnel; en ce compris: un traitement licite, loyal et transparent, une finalité déterminée explicite et légitime, une collecte de données adéquate, pertinente et limitée, de données exactes et, si nécessaire, tenues à jour, une durée de conservation limitée, et une garantie de sécurité des données. Le règlement précise également, que dans ce cadre, et que ce soit dans une situation de collecte directe auprès de la personne concernée, ou indirecte¹⁰¹¹, l'information de la personne concernée est obligatoire. La liste des informations à fournir est assez conséquente. Elle regroupe l'identité et les coordonnées du responsable de traitement, ou celles du délégué à la protection des données, les finalités du traitement et sa base juridique, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (lorsque le traitement n'est pas fondé sur le consentement), les destinataires des données, l'intention de transfert de données vers un pays tiers s'il y a lieu, ainsi

¹⁰¹⁰ Article 9 paragraphe 2, point g, p. 38.

¹⁰¹¹ Le règlement prévoit en effet des cas où les données à caractère personnel n'ont pas été collectées auprès de la personne concernée (Article 14). Le considérant 61 évoque la situation dans laquelle les données à caractère personnel sont obtenues d'une autre source que la personne concernée. Ce nouveau destinataire des données doit être mentionné dans le cadre de la première collecte de données et doit se plier aux mêmes obligations que le responsable de traitement s'il souhaite également traiter ces données. On précisera que le règlement donne la définition suivante du destinataire : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement* »

que la liste des droits de la personne concernée. Si la collecte de données est indirecte, le nouveau responsable de traitement doit en plus de ces informations, et dans le but de garantir un traitement équitable et transparent, respecter un délai raisonnable pour informer la personne concernée.

439. A la lecture du règlement et de la complexité de ces propositions, il semble paradoxal que le responsable de traitement s'oriente vers cette base juridique. D'autant que les traitement sans consentement paraissent pouvoir être essentiellement justifiés par un intérêt légitime ou un intérêt public important. Aussi, à la lecture de la nouvelle définition de la notion de consentement cette affirmation semble prendre tout son sens.

2. La nouvelle définition du consentement

440. L'article 4 du règlement définit le consentement des personnes concernées comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

441. Analysons ici les mots utilisés dans le cadre de cette définition du consentement, et plus particulièrement les mots « éclairé » et « libre ». Le consentement doit être éclairé. Cela suppose *a minima* de connaître l'identité du responsable de traitement et les finalités du traitement. Le règlement précise que si le traitement envisage plusieurs finalités, le consentement doit être recueilli pour chacune d'entre-elles. Le considérant 42 du règlement précise que « *des garanties devraient exister afin de garantir que la personne concernée est consciente du consentement donné et de sa portée* ». Et de poursuivre: « *le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* ». Le choix des termes de ce considérant n'est pas sans poser de problèmes. Comment définir la conscience du consentement donné et sa portée dans le cadre des traitements de données personnelles ? Doit-on s'attendre ici à un retour du concept de bon père de famille, abandonné par le droit civil français à la suite de la réforme de 2016 du droit des obligations ? Alors même que la surveillance diffuse infantilise l'individu faut-il croire qu'il est homme suffisamment raisonnable et doué de raison en matière de protection de ses données personnelles ? Qu'entend-on réellement par un consentement librement donné ? Peut-on réellement affirmer aujourd'hui que l'ensemble des technologies d'usage

quotidien, ou des technologies mises en place sur l'espace public, permettent à l'individu de donner librement son consentement ? Les applications mobiles représentent le parfait exemple du consentement librement donné. Certaines applications mobiles, spécialement des jeux, demandent à accéder à la fois au répertoire téléphonique, à l'appareil photo, aux coordonnées de localisation, aux données techniques (réseau de télécommunication et wifi), alors même que certaines de ces fonctionnalités n'ont clairement pas d'effet dans le cadre de cette application. Si l'utilisateur refuse l'accès à ces données, l'usage de ces applications est impossible. Le consentement librement donné réside-t-il alors dans le choix d'utiliser et/ou dans le choix de ne pas utiliser cette application ?

442. L'article 7 du règlement précise alors que « *au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat* ». De fait, le règlement reprend les mécanismes civilistes du droit des contrats. En effet, dans le cadre du droit des contrats, si le consentement est donné sous la menace d'une perte, il n'est pas valide. Appliquons ces éléments à la surveillance diffuse, et plus spécialement aux conditions générales d'utilisation d'un site internet, d'un réseau social. Pour accéder à ces sites, pouvoir les utiliser, l'utilisateur est obligé d'accepter les conditions générales d'utilisation prônant le traitement de données personnelles. Le consentement est bien obtenu sous la menace ici, puisque si l'utilisateur ne donne pas son consentement, il ne peut utiliser ce site. Le considérant 42 du règlement tend d'ailleurs vers cette analyse puisqu'il déclare clairement que « *le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* ». Basées sur le traitement de données personnelles et de nos habitudes d'achat et de consommation, permettant de profiler le consommateur et d'entrer au plus haut degré dans son intimité, les cartes de fidélité sont également un exemple très parlant concernant la liberté du consentement. Les cartes de fidélité des groupes de grande distribution, conférant une réduction sur le coût global des courses du quotidien, présentent un avantage pour les classes moyennes, et les plus démunis. Refuser le traitement de données personnelles, et partant de données impersonnelles (consommation), semblent délicat pour une bonne partie de ces personnes.

443. L'article 7 du règlement, ainsi que la lecture attentive des considérants de ce dernier laisse le juriste dans le doute le plus total. Le consentement ne devrait jamais représenté une contrepartie

d'un bien ou d'un service. Le règlement ne devrait pas organiser une protection de de la vie privée à double vitesse. A l'image du corps humain, placé hors commerce par le droit, la vie privée ne devrait pas avoir de valeur économique. A l'image de la liberté de disposer de son corps, l'individu devrait avoir la liberté de disposer de ses données personnelles. Ce rapprochement pour partie du droit des données personnelles au droit des contrats auraient pu être une véritable réussite si la logique avait été complète, logique et pertinente, quant à l'objet du contrat - la donnée personnelle ? La donnée impersonnelle ? Ou l'information?¹⁰¹², mais également pour chacune des parties concernées. Or, ici, la personne concernée qu'elle soit consommateur, client, ou simple citoyen ne semble pas être considérée comme une partie faible, ni même comme une partie à un quelconque contrat. Cette logique est également palpable dans le cadre des traitements de données à caractère personnel des mineurs de moins de 16 ans ou de 13 ans, en fonction de la législation nationale. Si le consentement des personnes dépositaires de l'autorité parentale doit être recueilli, c'est uniquement lorsque le traitement aura pour base légale le consentement.

B. L'apparition d'un nouveau principe: les traitements sans consentement pour « intérêt légitime »

444. Pour rappel, le responsable de traitement pourra avec le règlement fonder son traitement sur le consentement de la personne concernée, l'exécution d'un contrat, le respect d'une obligation légale, la sauvegarde des intérêts vitaux de la personne, l'exécution d'une mission d'intérêt public, la poursuite d'intérêts légitimes. Le responsable de traitement doit informer la personne concernée de la base légale choisie pour le traitement sous peine de sanctions équivalentes à quatre pour cent du chiffre d'affaire annuel mondial total de l'exercice précédent ou de vingt millions d'euros, le montant le plus élevé entre ces deux options étant retenu.

445. Si certaines de ces bases légales ne soulèvent que peu d'interrogations, la poursuite des intérêts légitimes et impérieux du responsable de traitement laisse le juriste dubitatif. A la lecture des considérants du règlement, une entreprise (ou un Etat pour motif d'intérêt public) peut avoir un intérêt légitime à traiter des données personnelles, à son profit, de ses clients, sans même recueillir le consentement de ces derniers. Pour rappel, le consentement n'étant plus une condition préalable

¹⁰¹² Voir en ce sens, le chapitre 2 de ce titre infra.

au traitement¹⁰¹³, il est donc possible de justifier ce dernier par l'intérêt légitime du responsable de traitement. Le considérant 47 du règlement apporte quelques précisions d'analyse concernant les intérêts légitimes. Ainsi, « *les intérêts légitimes (...) peuvent constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service* ». Les clients et les salariés d'une entreprise sont donc de potentielles personnes concernées par un traitement de données personnelles pour intérêt légitime. Et de poursuivre: « *l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut **raisonnablement s'attendre**, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée* ». On retrouve ici la même logique que dans le cadre des traitements avec consentement. Le choix des mots fait ici à nouveau penser au bon père de famille, et semble assez contradictoire avec la logique du règlement à renforcer l'obligation d'information. En réalité, si ces exemples constituent une grille d'analyse intéressante, il n'en reste pas moins de simples exemples.

446. Le responsable de traitement détermine et justifie lui-même l'existence de son intérêt légitime au traitement de données personnelles. Il doit, pour se faire, et au titre du considérant 47, s'assurer que « *les intérêts et droits fondamentaux de la personne concernée* » ne prévalent pas sur ses intérêts légitimes. La notion d'intérêt légitime était dans les faits déjà présente dans la directive de 1995. Elle ne présentait à cette époque que peu d'intérêt, puisque le consentement de la personne concernée était une condition préalable à ce dernier. Anticipant le futur règlement européen, le groupe de l'article 29 a jugé opportun d'émettre un avis sur la notion d'intérêt légitime poursuivi

¹⁰¹³ Le projet de loi français relatif à la protection des données personnelles ne semblent pas revenir sur cet élément: le consentement n'est plus une condition préalable au traitement. Voir en ce sens, Projet de loi n°490 *relatif à la protection des données personnelles*, (Procédure accélérée), Présenté au nom de M. Edouard Philippe, Premier Ministre, Par Mme Nicole Belloubet, garde des sceaux, ministre de la Justice, Enregistré à la Présidence de l'Assemblée nationale le 13 décembre 2017, Assemblée nationale, Quinzième législature, En ligne: <http://www.assemblee-nationale.fr/15/pdf/projets/pl0490.pdf> (dernière consultation: 5 mars 2018)

par le responsable de traitement au sens de l'article 7 de la directive de 1995¹⁰¹⁴. Cet avis précise que ce motif de traitement des données personnelles requiert « *une mise en balance qui compare l'intérêt légitime poursuivi par le responsable du traitement - ou par le ou les tiers auxquels les données sont communiquées - avec l'intérêt ou les droits fondamentaux des personnes concernées*¹⁰¹⁵ ». A la lecture de l'avis du groupe 29, il apparaît clair que le motif d'intérêt légitime doit être compris comme un critère de nécessité devant être « *formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée, (...) constituer un intérêt réel et présent*¹⁰¹⁶ ». Et d'ajouter que « *un intérêt légitime doit être acceptable au regard du droit, être licite, c'est dire conforme au droit en vigueur dans l'union et dans le pays concerné*¹⁰¹⁷ ».

447. En l'absence de précision réelle dans le règlement concernant cette notion, l'avis du Groupe 29 est salutaire. En effet, si l'interprétation des intérêts légitimes dans le cadre du règlement laisse place au doute, l'avis du groupe 29 par le rappel d'une condition de licéité de cette notion rassure. L'interprétation d'un traitement sans consentement préalable pour motif légitime, que laisse entendre le règlement, est contraire à la charte des droits fondamentaux (article 8) qui exige le consentement préalable au traitement de données personnelles. Dans l'attente de précisions supplémentaires quant à cette notion, il faut au travers des lignes qui précèdent prendre acte d'une insécurité juridique entourant ce texte. Cette insécurité sert parfaitement les intérêts de la surveillance diffuse. Entre la nouvelle définition du consentement, l'absence de référence claire au consentement préalable au traitement de données personnelles et les imperfections de rédaction de ce texte de consensus, la protection des données personnelles, organisée par le règlement, semble dangereuse en terme de protection des libertés et des droits fondamentaux, mais également en terme de sécurité juridique.

¹⁰¹⁴ Groupe de travail « article 29 » sur la protection des données, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable de traitement des données au sens de l'article 7 de la directive 95/46/CE, Adopté le 9 avril 2014, 844/14/FR, WP 217. On peut ainsi lire en page 5 de cet avis que « *Il est donc particulièrement opportun, alors que le travail d'élaboration d'un nouveau règlement général sur la protection des données se poursuit, de veiller à ce que le sixième motif justifiant le traitement (« l'intérêt légitime ») et sa relation avec les autres motifs soient mieux compris. En particulier, dès lors que les droits fondamentaux des personnes concernées sont en jeu, il convient de prendre dûment en considération le respect de ces droits lors de l'application de chacun des six motifs, sans discrimination. L'article 7, point f), ne doit pas devenir un moyen commode d'échapper à l'obligation de se conformer au droit applicable en matière de protection des données* ».

¹⁰¹⁵ Ibid. p. 4 - 5.

¹⁰¹⁶ Ibid. p. 26

¹⁰¹⁷ Ibid. p. 28

Paragraphe 2: Des gardes-fous existants mais inefficaces

448. Le règlement général de protection des données personnelles organise une nouvelle forme de responsabilisation des acteurs du traitement de données personnelles. L'entreprise, l'Etat et l'individu sont directement concernés par cet objectif. Si cet objectif paraît louable de prime abord, il faut en réalité se demander si cette responsabilisation est effective (A). Cet objectif de responsabilisation touche également les transferts de données hors Union européenne, revus et corrigés par le règlement général de protection des données personnelles. A travers l'exemple de la refonte des Safe Harbor, devenu Privacy Shield, il faudra conclure le propos sur le règlement général de protection des données personnelles par le constat d'un véritable acte manqué (B), opérant ainsi une véritable désinstitution du droit des données personnelles.

A. L'ineffectivité de la responsabilisation des acteurs opérant des traitements de données personnelles

449. En vue de responsabiliser les acteurs du numérique, le règlement passe d'une logique de contrôle *a posteriori* à un contrôle *a priori* directement intégré dans la culture de l'entreprise ou de l'Etat souhaitant opérer des traitements de données personnelles. Ainsi, l'un des acteurs majeurs de la responsabilisation, le délégué à la protection des données personnelles, est présenté à la fois comme le chef d'orchestre de la protection des données personnelles au sein de l'entité en charge d'un traitement, et comme une police interne (1). La responsabilisation des acteurs touche également l'individu qui se voit conférer de nouveaux droits (2). Pour certains auteurs tels que Antoinette Rouvroy et Thomas Berns, ces « *métadroits*¹⁰¹⁸ » se situent « *bien au-delà du seul droit au respect de la vie privée et à la protection des données à caractère personnelles brandis habituellement dans ce cadre*¹⁰¹⁹ ».

1. L'acteur majeur de la responsabilisation: le délégué à la protection des données personnelles

450. Le délégué à la protection des données personnelles n'est ni plus ni moins que l'extension au niveau européen d'une fonction déjà existante au niveau national: le correspondant informatique

¹⁰¹⁸ ROUVROY Antoinette, BERNS Thomas, *Le nouveau pouvoir statistique - Op. Cit.*, p. 100

¹⁰¹⁹ Ibid.

et libertés. Si la généralisation de cette fonction devenue obligatoire paraît intéressante pour la protection des données personnelles, elle correspond en réalité à l'ambition d'un renforcement de la gouvernance des données personnelles par l'affirmation d'une forme de contrôle *a priori*. Elle risque, également, au vu de l'échec des correspondants informatique et libertés¹⁰²⁰, de montrer rapidement des signes d'inefficacité.

451. La désignation d'un délégué à la protection des données personnelles est obligatoire tant pour les responsables de traitements que pour les sous-traitants, et ce, qu'ils appartiennent au secteur public ou privé, et spécialement si leur activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou si leur activité principale les amène à traiter des données « particulières » ou relatives à des condamnations pénales ou à des infractions¹⁰²¹. A nouveau, le règlement manque de précisions quant aux termes employés. Que signifie cette mention contenue dans le règlement de « suivi régulier et systématique » ? Comment évaluer un traitement « à grande échelle » ? Le groupe 29 s'est saisi de ces questions dès 2016 et apporte quelques éléments de réponse. Ainsi peut-on lire dans les lignes directrices dégagées par le groupe de l'article 29¹⁰²² que « *« les activités de base » ne doivent pas être interprétées comme excluant les activités pour lesquelles le traitement de données fait partie intégrante de l'activité du responsable de traitement ou du sous-traitant*¹⁰²³ ». Ainsi, il faut intégrer dans cette définition toute entité dont le modèle économique est fondé ou permis grâce à l'exploitation de données. Les hôpitaux ou les entreprises de sécurité privée sont alors deux exemples donnés par le groupe 29 pour illustrer ce concept d'activité de base. Concernant les traitements « à grande échelle », le groupe 29 admet qu'il est impossible de pouvoir quantifier le nombre de données ou d'individus à partir duquel on considérera que le traitement est à grande échelle. Pour déterminer la grandeur d'échelle du traitement, le groupe 29 recommande que des facteurs particuliers soient pris en compte: « *le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative, par*

¹⁰²⁰ En France, le Correspondant informatique et Libertés n'est chargé uniquement que des traitements relevant du régime de déclaration à la CNIL. Sa désignation était à l'origine facultative. Salarié de l'entreprise, il a été à de multiples occasions dépeint comme « *un mouton à cinq pattes* » de la protection des données personnelles. Voir en ce sens: RAY Jean-Emmanuel, *Le nouveau correspondant aux données personnelles*, Semaine sociale Lamy, 27 septembre 2004, n° 1183, p. 6.

¹⁰²¹ Article 37 du RGPD, p. 55

¹⁰²² Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices concernant les délégués à la protection des données*, Adoptées le 13 décembre 2016, Version révisée et adoptée le 5 avril 2017, 16/FR, WP 243 rev. 01, Disponible en ligne à l'adresse suivante: https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf (dernière consultation: 5 mars 2018)

¹⁰²³ Ibid. p. 8.

*rapport à la population concernée, le volume de données et/ou le spectre des données traitées; la durée, ou la permanence des activités de traitement des données; l'étendue géographique de l'activité de traitement*¹⁰²⁴ ». Ces facteurs laissent le juriste perplexe. Le groupe 29 relève d'ailleurs le manque de clarté du règlement quant à ces notions, évoquant l'existence « *d'une large zone grise*¹⁰²⁵ » permises par les orientations dégagées par le considérant 91 du règlement¹⁰²⁶.

452. Au-delà de sa désignation, le périmètre fonctionnel du délégué est assez large. Le règlement précise à plusieurs reprises que ce dernier doit être associé, par le responsable de traitement ou le sous-traitant, à toutes les questions relatives à la protection des données à caractère personnel de manière appropriée et en temps utile¹⁰²⁷. Afin de réaliser sa mission, le responsable de traitement ou le sous-traitant doivent fournir au délégué les ressources nécessaires pour exercer ses missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, tout en lui permettant d'entretenir ses connaissances spécialisées¹⁰²⁸. Chargé d'informer et de conseiller l'entité dans laquelle il exerce ses fonctions, de contrôler le respect du règlement et des dispositions européennes et nationales en matière de protection des données personnelles¹⁰²⁹, le délégué sert à la fois de police interne et d'auditeur en matière de données personnelles¹⁰³⁰. Il est également une sorte de lien-tampon entre l'entité et l'autorité de contrôle. Le règlement consacre une garantie d'indépendance du délégué, en ce qu'il met en place des obligations à la charge du responsable de traitement et du sous-traitant qui doivent veiller à ce que le délégué ne reçoive « *aucune instruction en ce qui*

¹⁰²⁴ Ibid. p. 9

¹⁰²⁵ Ibid.

¹⁰²⁶ Ce dernier déclare que les « *opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ainsi qu'à d'autres opérations de traitement qui engendrent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces personnes d'exercer leurs droits. (...) Le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire* ». Considérant 91 du RGPD, p. 17 -18

¹⁰²⁷ Article 38 du RGPD, P. 55 - 56

¹⁰²⁸ Ibid.

¹⁰²⁹ Article 39 du RGPD, p.56

¹⁰³⁰ Il peut également participer aux analyses d'impact en dispensant des conseils (sur demande).

*concerne l'exercice de ses missions*¹⁰³¹ ».

453. Enfin, il faut noter que l'indépendance du délégué à la protection des données personnelles est également garantie vis à vis de l'autorité de contrôle. Aucune obligation de délation n'est ici envisagée: le délégué à la protection des données personnelles n'est pas un contrôleur au service de la puissance publique. Cet acteur de la responsabilisation des données personnelles n'est pas sans poser de problèmes. Sa fonction et ses missions touchent directement la logique du droit de la responsabilité. A la lecture du règlement, le délégué à la protection des données personnelles n'est dans le cadre de ses prérogatives débiteur que d'une obligation de moyens, de prudence, de diligence, et de pédagogie. Tout se passe alors comme s'il était chargé de donner à l'entité dans laquelle il exerce sa mission une sorte de libre arbitre quant à la protection des données personnelles. A charge pour elle de respecter ces conseils. Sorte de docteur de la protection des données personnelles, il n'a pas l'obligation de soigner l'entité qui ne respecterait pas cette dernière. Cette approche de contrôle *a priori*, qui n'en est en réalité pas un, justifie à elle seule, le durcissement des sanctions envisagées par le règlement général¹⁰³².

2.Des « métadroits » pour assurer une meilleure protection des individus : l'exemple du droit à l'oubli

454. Si le contrôle *a priori* soulève des interrogations, l'exercice des droits des sujets du traitement, une fois ce dernier mis en oeuvre, s'avère également problématique. Du fait d'un déficit clair de conscience du lien que leurs données personnelles entretient avec leur vie privée, les individus n'ont, sous l'empire des premières législations informatique et libertés, que peu exercé leurs droits. Outre le droit à l'information des personnes concernées à l'égard des traitements de données personnelles, le responsable doit garantir un droit d'accès, de rectification, de suppression, d'effacement, un droit à la limitation, à la portabilité, à l'opposition, ainsi que le droit de ne pas faire l'objet d'une décision fondée essentiellement sur un traitement de données. Si le niveau de préoccupation des individus concernant la collecte et le traitement de données personnelles semble

¹⁰³¹ Article 38 du RGPD. Et de poursuivre: « *Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant* ».

¹⁰³² Pour rappel, ces dernière peuvent aller jusqu'à quatre pour cent du chiffre d'affaires annuel mondial total de l'exercice précédent ou 2à millions d'euros - le montant le plus élevé étant retenu.

augmenté¹⁰³³, ce n'est pas en reconnaissant des droits tels que la portabilité ou encore un droit à l'oubli que les comportements et habitudes des consommateurs de technologies changeront.

455. Antoinette Rouvroy et Thomas Berns évoquent des « métadroits » tels que la désobéissance, le droit de rendre compte¹⁰³⁴, et le droit à l'oubli. Pour ces auteurs, « *dans la mesure où il institue le corps statistique au départ de l'enregistrement, par défaut, de tous les événements, de tous les comportements, signifiants ou non pour ceux dont ils émanent, le gouvernement algorithmique constitue une sorte de mémoire digitale totale* » aux capacités de stockage virtuellement infinies, de nature à porter atteinte à la capacité d'oubli. Un droit à l'oubli se trouvait de fait garanti par l'obscurité pratique dans laquelle tombaient la plupart des faits et gestes posés, des phrases prononcées, une fois passé le temps nécessaire à l'oubli humain¹⁰³⁵ ». L'oubli informatique ne peut du fait des mémoires technologiques et des capacités de stockage recouvrir la même chose que l'oubli humain.

456. Le règlement général de protection des données personnelles prend d'ailleurs acte de cet élément puisqu'il consacre, en son article 17, un droit à l'effacement. Le législateur européen prend soin entre parenthèses et guillemets de préciser que ce droit à l'effacement s'assimile au droit à l'oubli. Suite à une demande d'effacement des données personnelles par la personne concernée, le responsable de traitement doit s'exécuter dans les meilleurs délais, et ce, lorsque « *les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière; la personne concernée retire le consentement sur lequel est fondé le traitement, (...) et il n'existe pas d'autre fondement juridique au traitement; la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2; les données à caractère personnel ont fait l'objet d'un traitement illicite;*

¹⁰³³ Voir en ce sens le sondage suivant: « vous souciez-vous des données collectées sur Internet vous concernant ? », 45 pour cent des français sondés se déclare tout à fait d'accord, En ligne :<https://fr.statista.com/statistiques/664257/francais-preoccupation-collecte-donnees-internet/> (dernière consultation: 5 mars 2018)

¹⁰³⁴ Pour Rouvroy et Berns, « *la possibilité de se rendre compte et de rendre compte de ce qui nous fait agir, par le langage notamment, et y compris en Justine, semble également compromise. Puisque le savoir sur lequel fonctionne la gouvernamentalité algorithmique émane spontanément d'une sorte de mémoire digitale totale, que le sens n'est plus construit, mais donné, immanent au « réel » et découvert dans les relations subtiles entre données, il n'est plus nécessaire de rien expliquer ni de rien interpréter. La connaissance purement prédictive n'équivaut en rien à ce que l'on considère spontanément comme un savoir des causes ou des justifications des comportements. Ceci signifie aussi que le gouvernement statistique du réel ne permet pas aux gouvernés de « rendre compte » par le langage, la plaidoirie, de leurs actions, attitudes, choix, etc.* ». ROUVROY Antoinette, BERNS Thomas, Op. Cit., p. 102

¹⁰³⁵ Ibid. p. 101

les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis; les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1¹⁰³⁶ ». Par cette liste détaillée, le règlement précise et renforce le droit à l'oubli. En cela, il élargit les conclusions de la décision du 13 mai 2014 de la Cour de Justice de l'Union Européenne qui avait condamné un moteur de recherche sur internet à déréférencer des liens vers des pages web contenant des informations sur un citoyen Espagnol¹⁰³⁷.

457. Pourtant, déréférencement, effacement et oubli ne sont pas synonymes. Le déréférencement est une modalité technique permettant une sorte de « suppression logique » des données. Ces dernières sont dans les faits toujours présentes dans la base de données, les logs et sauvegardes quotidiennes des serveurs de l'entité. Quant à l'effacement et l'oubli, ainsi que le rappelle Antoinette Rouvroy et Thomas Berns, « la très grande facilité de récupération et de recoupement des données enregistrées dans différents contextes, à différentes périodes, pour la construction et l'actualisation de profils utilisateurs, de consommateurs, de délinquants potentiels, de fraudeurs¹⁰³⁸ », en somme l'organisation de la surveillance diffuse, ne permet pas de garantir l'effectivité d'un vrai droit à l'oubli, essentiellement matérialisé par la possibilité de se créer un « dehors, un espace non identique au « réel » statistiquement enregistré¹⁰³⁹ ». La conclusion de ces auteurs concernant « les impossibilités de la désobéissance et de l'oubli, de même que l'érosion des possibilités de (se) rendre compte de ce qui nous fait agir » devrait pousser le juriste et le législateur à en appeler aux forces imaginantes du Droit pour paraphraser Mireille Delamas- Marty.

¹⁰³⁶ Article 17, paragraphe 1 du rGPD, p. 43 -44

¹⁰³⁷ CJUE, Affaire C-131/12, Arrêt de la Cour (grande chambre) du 13 mai 2014, Google Spain et Google Inc, Publié au Recueil numérique, Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30dd03f02947f35f4beeb42abca6d82bd0d4.e34KaxiLc3qMb40Rch0SaxyNaNz0?text=&docid=152065&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=1212706> (dernière consultation: 5 mars 2018). Le juge européen précise que: « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite ».

¹⁰³⁸ Op. Cit. p. 101.

¹⁰³⁹ Ibid. p. 102

B. Les transferts de données personnelles hors Union Européenne: l'exemple du Privacy Shield

458. Le chapitre 5 du règlement général de protection des données personnelles est entièrement dédié aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales. Le principe guidant ces transferts hors Union européenne est dégagé aux articles 44 et suivant, qui déclarent dans leur ensemble, que ces derniers ne peuvent avoir lieu que s'ils sont fondés sur une décision d'adéquation¹⁰⁴⁰, si le responsable de traitement a prévu des garanties appropriées et que les personnes concernées disposent de droits opposables et de voies de droit effectives¹⁰⁴¹, ou encore si l'autorité de contrôle compétente a approuvé des règles d'entreprises contraignantes soumises à des mécanismes de contrôle de cohérence¹⁰⁴². Les considérants du règlement précise à nouveau l'importance des flux de données à caractère personnel à destination ou en provenance de pays en dehors de l'Union pour le « *développement du commerce international et de la coopération internationale*¹⁰⁴³ ».

459. A la suite de la censure des Safe Harbor par la CJUE en 2015, le Privacy Shield a été jugé adéquat pour les transferts de données personnelles vers les Etats-Unis le 12 juillet 2016¹⁰⁴⁴ au vu de la directive de 1995. Son application n'a pas été remis en question par le règlement européen sur la protection des données personnelles. Le Privacy Shield repose, ainsi que le mentionne la décision d'exécution de la Commission, « *sur un système d'autocertification en vertu duquel les organisations américaines s'engagent à respecter une série de principes de protection de la vie privée, constitués de principes-cadres et de principes complémentaires (...), qui sont publiés par le ministère américain du commerce (...). Ce bouclier s'applique à la fois aux responsables du traitement et aux sous-traitants (mandataires), avec ceci de spécifique que les sous-traitants doivent être contractuellement tenus d'agir uniquement sur instruction du responsable européen du traitement et d'aider ce dernier à répondre aux demandes des personnes qui exercent leurs droits en*

¹⁰⁴⁰ Article 45 du RGPD, p. 61-62

¹⁰⁴¹ Article 46 du RGPD, p. 62

¹⁰⁴² Article 47 du RGPD, p. 63, et article 63 du RGPD, p. 73

¹⁰⁴³ En ce sens, voir le considérant n° 101 du RGPD, p. 19.

¹⁰⁴⁴ Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis, JOUE L207/1, du 1er août 2016, Disponible en ligne à l'adresse suivante: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016D1250&from=EN> (dernière consultation: 5 mars 2018)

*vertu des principes*¹⁰⁴⁵ ». Sans revenir sur les problématiques posés par les procédures de certification et de labellisation qui engendre un déplacement de focale - de la réglementation à la régulation - il semble important de clarifier les principes du Privacy Shield. Sauf exceptions¹⁰⁴⁶, les entités certifiées Privacy Shield s'engageront à respecter: le principe de notification qui recouvre le principe d'information¹⁰⁴⁷, le principe d'intégrité des données et de limitation des finalités¹⁰⁴⁸, le principe de choix¹⁰⁴⁹, le principe de sécurité¹⁰⁵⁰, le principe d'accès aux données qui ne peut être restreint que dans des cas exceptionnels.

460. Dès son adoption sous l'empire de la directive, cet accord avait suscité de vives réactions de la part du Groupe 29 reprochant le manque d'harmonie et de clarté général de cet instrument du fait de sa conclusion en urgence¹⁰⁵¹. Après une année d'application sous l'empire du règlement, la cohérence globale et la conformité de ce texte ont été à nouveau jugé par le Groupe 29¹⁰⁵² et la Commission européenne¹⁰⁵³. Cette dernière relève essentiellement des problématiques de fraudes aux systèmes de certification des entreprises, soit parce que ces dernières font référence à cette certification avant même de l'avoir obtenue, soit parce qu'elles usent de fausses certifications. Si ces éléments font essentiellement référence à un manque de contrôle de la part des autorités américaines¹⁰⁵⁴, l'enquête du Groupe 29 s'intéresse quant à elle à l'évaluation des aspects commerciaux de cet instrument et à l'accès permis au gouvernement des Etats-Unis sur les données personnelles transférées de l'Union Européenne. Le bilan dressé par le Groupe 29 est accablant: manque de clarté quant aux procédures même de certification à destination des entreprises, manque

¹⁰⁴⁵ Ibid, Point 14, p. 3

¹⁰⁴⁶ Constituées par la sécurité nationale, l'intérêt public ou l'application d'une loi.

¹⁰⁴⁷ Il consiste à informer les personnes sur les traitements de données les concernant, de la garantie d'un droit d'accès, à publier la politique de confidentialité et à la rendre accessible sur les sites de la Federal Trade Commission, dans la liste du Privacy Shield et sur le site de résolution des litiges

¹⁰⁴⁸ Les données doivent être fiables, à jour, exactes, complètes et la garantie qu'il ne peut y avoir d'utilisation ultérieure des données personnelles pour une finalité incompatible avec celle de la collecte.

¹⁰⁴⁹ Permettant à la personne en cas de nouvelle finalité de s'opposer au traitement

¹⁰⁵⁰ Qui impose aux adhérents au Privacy Shield et à leurs sous-traitants de prendre des mesures raisonnables et appropriées en tenant compte des risques.

¹⁰⁵¹ En sens: Groupe de travail « Article 29 » sur la protection des données, *Working document 01/2016 on the justification of interference with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data*, 13 avril 2016.

¹⁰⁵² Groupe de travail « Article 29 » sur la protection des données personnelles, EU - US Privacy Shield - First annual Joint Review, Adopté le 28 novembre 2017, 17/EN, WP 255

¹⁰⁵³ Commission, Européenne, Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield, Com (2017) 611 final, Bruxelles, 18 octobre 2017

¹⁰⁵⁴ Cet élément est aussi pointé du doigt par le groupe 29, Voir document précité, p. 12 et suivantes

d'informations claires à disposition des citoyens européens. Les potentielles voies de recours pour ces derniers sont, en pratique, trop complexes et peu accessibles¹⁰⁵⁵, spécialement dans des cas de surveillance organisée par les Etats-unis. Les réponses du gouvernement américain concernant le profilage des citoyens européens n'a également que peu convaincu le Groupe 29. Craignant que les données transférées servent au profilage des individus dans des décisions automatisées prises à leur rencontre, notamment par des organismes de crédit¹⁰⁵⁶, le Groupe 29 appelle la Commission européenne à réagir. Rappelons également que le Privacy Shield a été envisagé suite à l'invalidation des Safe Harbor au vu de la potentielle surveillance de masse opérée par le gouvernement des Etats-Unis. Le groupe 29 a axé la moitié de son enquête sur le traitement de données personnelles réalisé à des fins de sécurité nationale. Plus précisément, le groupe 29 s'inquiète de la réadaptation de la section 702 de la Foreign Intelligence Surveillance Act permettant aux renseignements américains de cibler les communications des individus (hors Etats-Unis). Sur la base des informations disponibles et fournies par le gouvernement américain lors de l'enquête du Groupe 29, ce dernier réclame des autorités américaines « *des preuves supplémentaires et des engagements juridiquement contraignants permettant d'étayer les affirmations des autorités américaines selon lesquelles la collecte de données en vertu de l'article 702 n'est pas aveugle et généralisé*¹⁰⁵⁷ » dans le cadre de nouveau programme de surveillance américain. En outre, il réclame également « *une évaluation indépendante de la nécessité et de la proportionnalité de la définition des « cibles » (...) en vue de clarifier l'accès massif et aveugle aux données de citoyens non américains*¹⁰⁵⁸ ».

461. L'ensemble des problèmes posés par le Privacy Shield, relevés dans le cadre de l'enquête du Groupe 29 n'est pas sans rappeler les problématiques posés par le Safe Harbor, problématiques qui

¹⁰⁵⁵ Sur ce point voir le rapport du Groupe 29 sur la première année d'application du Privacy Shield, p. 17 - 18

¹⁰⁵⁶ « *Les constatations recueillies au cours de l'examen conjoint semblent indiquer qu'aucune des données transférées dans le bouclier de confidentialité ne sont traitées par des systèmes automatisés de prise de décision (...). Cependant, les réactions des entreprises sont restées très générales, manquant de clarté (...). Le WP29 invite la Commission à envisager la possibilité de prévoir des règles spécifiques concernant la prise de décision automatisée afin de fournir des garanties suffisantes* ». Traduction libre de l'auteur des mots suivants: « *The findings gathered during the Joint Review seem to indicate that none of the data transferred under the Privacy Shield are processed through automated decision making systems, and the information provided on the Fair Credit Reported Act confirm that specific rules exist under US Law in certain fields. However the feedback from the companies remained very general, leaving unclear whether these assertions correspond to the reality of all companies adhering to the Privacy Shield, and these rules do not appear to cover all areas where automated decision making systems could be used given their very limited scope. The WP29 calls upon the Commission to contemplate the possibility to provide for specific rules concerning automated decision making to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, especially after having explored the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies if the analysis generates an actual need for additional safeguards* ». Rapport du Groupe 29 précité, p. 12.

¹⁰⁵⁷ Ibid, p. 16

¹⁰⁵⁸ Ibid.

ont d'ailleurs conduit à son invalidation. Ce sort risque également d'être réservé au Privacy Shield. Un recours a en effet été introduit par la quadrature du net, French data network, la fédération des fournisseurs d'accès à internet associatifs le 25 octobre 2016¹⁰⁵⁹, rejoints par l'union fédérale des consommateurs- que choisir le 26 octobre 2017¹⁰⁶⁰. Reprochant à la décision d'exécution de la Commission du 12 juillet 2016 relative à l'adéquation du privacy Shield d'être en violation avec le droit fondamental au respect de la vie privée, les requérants attaquent également le Privacy Shield qui, au vu de « *l'absence de limitation au strict nécessaire des exploitations autorisées par la réglementation des Etats-Unis*¹⁰⁶¹ » n'assure pas un niveau de protection des droits fondamentaux substantiellement équivalent. Entre l'absence de recours effectif garanti par ce dernier et l'absence de contrôle réellement indépendant concernant le respect de la vie privée par les Etats-Unis, le Privacy Shield est loin de garantir une protection équivalente à celle garantie dans l'Union européenne.

462. Les arguments des requérants reflètent parfaitement des problèmes posés par le passage d'une réglementation de la protection des données personnelles et du respect à la vie privée à une régulation, une gouvernance des données personnelles. De la garantie d'une liberté fondamentale, le droit des données personnelles est progressivement passé à la garantie d'un libre marché économique, et ce, malgré les différentes invectives du juge européen et des autorités européennes de contrôle tel que le groupe 29. Lorsque dès les premières lignes de l'ensemble des dispositions précitées, la mention de la libre circulation des données pour la réalisation d'un espace de liberté et d'une convergence des économies est quasiment préférée au rappel du droit fondamental au respect de la vie privée, la désinstitution du droit des données personnelles est admise. Lorsque l'ensemble des dispositions tendent vers un contrôle du marché par le marché économique, sa désinstitution est proclamée. La surveillance diffuse est alors en voie d'une parfaite intégration dans cette régulation.

¹⁰⁵⁹ Recours introduit le 25 octobre 2016 - La Quadrature du Net e.a./ Commission, Affaire T-738/16), Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=186645&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=177793> (dernière consultation: 5 mars 2018)

¹⁰⁶⁰ Ordonnance du tribunal (deuxième chambre), 26 octobre 2017, En ligne: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=197273&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1> (dernière consultation: 5 mars 2018)

¹⁰⁶¹ Op. Cit.

Chapitre 2: L'organisation de la marchandisation de la vie privée par les nouveaux instruments européens: vers une désinstitution du droit au respect de la vie privée et de la protection des données personnelles au profit de la surveillance diffuse

463. Au delà de la désinstitution du droit des données personnelles au travers du règlement général de protection des données personnelles, les instruments européens proposés depuis 2015 tendent de plus en plus à réduire le champ de la liberté fondamentale (la vie privée) à son versant économique - la libre circulation des données (personnelles ou non).

464. Si la préoccupation européenne de création d'un marché du numérique n'est pas nouvelle, sa volonté marquée de créer une économie fondée sur les données, « *devenues une ressource essentielle pour la croissance économique, la création d'emplois et la progrès sociétal*¹⁰⁶² », est quant à elle assez récente. Selon la Commission européenne, « *l' « économie fondée sur les données*¹⁰⁶³ » est caractérisée par un écosystème constitué de différents acteurs du marché (...) qui collaborent pour rendre les données accessibles et utilisables. Ces acteurs peuvent alors extraire de la valeur de ces données, en créant diverses applications susceptibles de faciliter grandement la vie au quotidien (gestion du trafic, optimisation des récoltes ou soins de santé à distance)¹⁰⁶⁴ ». Pour parvenir à la création de cette économie des données, la Commission reconnaît depuis 2012¹⁰⁶⁵, l'intérêt de la création de nouvelles règles « *modernes et cohérentes (...) pour que les données puissent circuler librement d'un Etat membre à l'autre*¹⁰⁶⁶ » et ce afin de rattraper le retard pris par

¹⁰⁶² Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions, Com (2017) 9 final, *Créer une économie européenne fondée sur les données*, Bruxelles, 10 janvier 2017, p. 2, En ligne: <http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-9-F1-FR-MAIN-PART-1.PDF> (dernière consultation: 5 mars 2018). Pour la Commission: « *l'analyse des données permet d'améliorer le processus décisionnel, l'innovation et la prévision des événements. Cette tendance mondiale représente un énorme potentiel dans divers domaines, allant de la santé, de l'environnement, de la sécurité alimentaire, du climat et de l'utilisation efficaces des ressources à l'énergie, aux systèmes de transport intelligents et aux villes intelligentes* »

¹⁰⁶³ La Commission définit ce concept comme suit : « *L'économie fondée sur les données mesure l'incidence globale du marché des données – c'est-à-dire le marché sur lequel les données numériques s'échangent sous forme de produits ou services dérivés de données brutes – sur l'économie dans son ensemble. Elle englobe la production, la collecte, le stockage, le traitement, la distribution, l'analyse, l'élaboration, la fourniture et l'exploitation des données grâce aux technologies numériques (European Data Market study, SMART 2013/0063, IDC, 2016)* ». Ibid.

¹⁰⁶⁴ Ibid. p. 2.

¹⁰⁶⁵ En ce sens, voir: Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions, COM (2012) 9 final, *Protection de la vie privée dans un monde en réseau - Un cadre européen relatif à la protection des données, adapté aux défis du 21^{ème} siècle*, Bruxelles, 25 janvier 2012, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012DC0009&from=EN> (dernière consultation: 5 mars 2018), Voir également: Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions, COM (2014) 442 final, *Vers une économie de la donnée prospère*, Bruxelles, 2 juillet 2014, En ligne: <http://ec.europa.eu/transparency/regdoc/rep/1/2014/FR/1-2014-442-FR-F1-1.Pdf> (dernière consultation: 5 mars 2018)

¹⁰⁶⁶ COM (2017) 9 final, Op. Cit., p.3

l'Europe dans la révolution des données par rapport aux Etats-Unis. Et de conclure que « *l'absence d'environnement juridique adapté aux échanges de données dans l'UE risquait de restreindre l'accès aux grands ensembles de données, de créer des barrières à l'entrée pour les nouveaux venus sur le marché et de freiner l'innovation. Des restrictions injustifiées à la libre circulation des données sont susceptibles d'entraver le développement de l'économie fondée sur les données* ». La consécration de la libre circulation des données par la Commission n'est pas à prendre à la légère. Elle concerne à la fois les données personnelles et les données non personnelles, les données générées par des machines ou par l'action humaine. La lutte contre les restrictions à la libre circulation des données se ressent dans le règlement général de protection des données personnelles, qui, au vu de ce qui précède, doit être analysé comme un instrument permettant de consacrer en partie de l'économie des données. Elle est également consacrée dans le cadre de la proposition de règlement du Parlement européen et du Conseil concernant un cadre applicable à la libre circulation des données à caractère personnel dans l'Union européenne¹⁰⁶⁷.

465. Il faut d'emblée conclure à la dangerosité de cet instrument qui méconnaît entièrement les enjeux de la surveillance diffuse précédemment évoqués, et plus particulièrement son ambition à la collecte de toujours plus d'informations afin de créer des profils les plus individualisés possibles. Dans la vision prônée par la proposition de règlement, la libre circulation des données (non) personnelles représente le facteur essentiel d'intégration complète de la surveillance diffuse, de désinstitution du droit des données personnelles et non personnelles, et, par voie de conséquence, de la vie privée (section 1). Cette proposition, ainsi que l'ensemble des travaux de la Commission visant à créer l'économie des données, marque un acte manqué. En effet, alors que ces éléments envisagent l'élaboration de la libre circulation des données, le statut juridique de ces dernières, qu'elles soient personnelles ou non, n'a jamais été questionné. De fait, seule la création de ce marché économique paraît important. Tout se passe alors comme si le droit des données, personnelles ou non, n'était plus réellement fondé à protéger la liberté fondamentale qu'est la vie privée. Le droit des données semble être aujourd'hui un droit économique visant à concurrencer le marché américain. La protection des individus est alors en souffrance, et il apparaît nécessaire d'appréhender le droit des données autrement. C'est au travers de la théorie juridique de l'information et de certains mécanismes civilistes que l'on trouvera des éléments de réponses visant

¹⁰⁶⁷ Proposition de Règlement du Parlement européen et du Conseil concernant un cadre applicable à la libre circulation des données à caractère personnel dans l'Union européenne, COM (2017) 495 final, 2017/0228 (COD), Bruxelles, 13 septembre 2017

une protection plus effective des individus (section 2).

Section 1: L'organisation de la libre circulation des données non personnelles comme facteur d'intégration complète de la surveillance diffuse et de désinstitution du droit au respect de la vie privée

466. La proposition de règlement concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne est dangereuse en ce qu'elle est un instrument au service de la marchandisation de la vie privée (paragraphe 1). Elle témoigne de l'absence de conscience des enjeux de la surveillance diffuse à construire, du fait des informations collectées, des profils les plus individualisés possibles. L'analyse de l'arrêt du Conseil d'Etat rendu le 8 février 2017¹⁰⁶⁸, évoquant l'individualisation d'une personne du fait de l'interconnexion de données entre elles permet d'ailleurs de prendre acte de la prégnance de cette analyse (paragraphe 2).

Paragraphe 1 La proposition de règlement sur la libre circulation des données non personnelles: un instrument au service de la marchandisation de la vie privée

467. La libre circulation des données est un enjeu majeur de l'élaboration de l'économie de la donnée. Permettant la réduction progressive du droit des données à un droit économique (A), la libre circulation des données prônée par ces nouveaux instruments européens interroge le juriste sur le statut juridique des données personnelles et non personnelles (B)

A. La réduction progressive du droit des données à un droit économique

468. La libre circulation des données est un enjeu majeur de l'élaboration de l'économie de la donnée. La réduction progressive du droit des données à un droit économique trouve sa consécration dans la proposition de règlement sur la libre circulation des données non personnelles (2). En ce que cette proposition vient se surajouter aux règles édictées par le règlement général sur la protection des données personnelles, il faut comprendre la consécration progressive de la libre

¹⁰⁶⁸ Conseil d'Etat, 8 février 2017, 10ème - 9ème Chambres réunies, n° 393714, JCDécaux, Mentionné dans les tables du recueil Lebon, En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?&idTexte=CETATEXT000034017907> (dernière consultation: 5 mars 2018)

circulation des données (1).

1.L'élaboration progressive de la libre circulation des données

469. Le principe de libre circulation des données à caractère personnel est prévue à l'article 16 du traité sur le fonctionnement de l'Union européenne. Ce principe est affirmé clairement par le règlement général sur la protection des données personnelles qui reprend, en son article premier, mot pour mot l'article 16 du traité précité. Ainsi est-il mentionné que « *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. (...). 3. 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*¹⁰⁶⁹ ».

470. La création de l'économie européenne fondée sur les données¹⁰⁷⁰ repose principalement sur la levée « *des restrictions injustifiées à la libre circulation des données*¹⁰⁷¹ ». Souhaitant protéger la sécurité et la fiabilité de la libre circulation des données, la Commission européenne va même plus loin. Les termes utilisés dans sa communication de 2017 sont particulièrement étonnants: « ***les préoccupations relatives au respect de la vie privée sont légitimes mais elles ne devraient pas être utilisées par les pouvoirs publics comme une raison suffisante pour restreindre la libre circulation des données de manière injustifiée*** ». Et de poursuivre en se félicitant de la protection que permettra le règlement général de protection des données personnelles. Ce dernier « *assurant un niveau élevé de protection des données à caractère personnel pour l'ensemble de l'UE. Il*

¹⁰⁶⁹ Article 1er du RGPD, p. 32

¹⁰⁷⁰ COM (2017) 9 final

¹⁰⁷¹ Ibid. p. 3. Et d'ajouter que « *ces restrictions résultent des exigences imposées par les autorités publiques quant à la localisation des données à des fins de stockage ou de traitement. (...) Dans sa stratégie relative au marché unique numérique, la Commission a annoncé qu'elle proposerait une initiative visant à lutter contre les restrictions à la libre circulation des données motivée par des raisons autres que la protection des données à caractère personnel au sein de l'UE et contre les restrictions injustifiées quant à la localisation des données à des fins de stockage ou de traitement. Au nombre de ces restrictions figurent des actes juridiques adoptés par les États membres ainsi que des règles et pratiques administratives d'effet équivalent. Leur nombre tend à augmenter avec la croissance de l'économie fondée sur les données, ce qui suscite des incertitudes quant aux possibilités de localisation du stockage ou du traitement des données. Tous les secteurs de l'économie et les organisations du secteur public comme celles du secteur privé risquent d'en pâtir, car cela pourrait rendre plus difficiles d'accès les services de données plus innovants et/ou moins onéreux. Les restrictions injustifiées quant à la localisation des données restreignent la liberté de prestation de services et la liberté d'établissement inscrites dans le traité et enfreignent également le droit dérivé applicable. Cela risque d'entraîner un morcellement du marché, de faire baisser la qualité du service pour les utilisateurs et de diminuer la compétitivité des prestataires de services de données, notamment les plus petits* » (p. 4).

renforce la confiance des consommateurs dans les services en ligne et garantit une application uniforme des règles dans tous les États membres en confortant les autorités nationales chargées de la protection des données. Le RGPD favorise la confiance nécessaire dans le traitement des données et constitue le socle de la libre circulation des données à caractère personnel dans l'UE ».

Précisons à nouveau ici qu'il n'est pas encore prouvé que le RGPD présente effectivement un niveau élevé de protection des données à caractère personnel, d'autant que ce dernier désinstitue le droit des données personnelles pour y préférer des contre-mesures proposées par les acteurs du marché.

471. La volonté d'élaborer l'économie des données est très surprenante. La lecture attentive de la communication de la Commission de 2017, spécialement les lignes qu'elles consacrent à son principe fondamental, laissent transparaître une idée générale: la protection des données n'est pas un objectif en soi, ni même un élément de sauvegarde des droits fondamentaux des personnes, mais bien avant tout un moyen et une fin destinée à construire le marché unique du numérique. Plus inspirée par l'efficacité économique que par les libertés fondamentales, la Commission déclare que *« le principe de libre circulation des données à caractère personnel, inscrit dans le droit primaire et le droit dérivé, devrait aussi s'appliquer dans les cas où le RGPD autorise les États membres à réglementer des questions spécifiques. Les États membres devraient être encouragés à ne pas utiliser les « clauses d'ouverture » prévues par le RGPD pour restreindre davantage la libre circulation des données. Dans ses conclusions du 15 décembre 2016, le Conseil européen a demandé la levée des obstacles qui subsistent au sein du marché unique, y compris ceux qui entravent la libre circulation des données¹⁰⁷² »*. Ces clauses d'ouvertures, mentionnées par la Commission, sont contenues dans le règlement général de protection des données personnelles. Elles permettent aux États membres d'adopter des règles et dispositions plus contraignantes en matière de protection des données personnelles. On pense notamment à l'âge des mineurs fixés dans le règlement à 16 ans, pouvant être ramené à 13 ans par la législation nationale. A lire la communication de la Commission, toute latitude exprimée dans le règlement est à prohiber. Quid ici de la loi pour une République numérique adoptée le 7 octobre 2016¹⁰⁷³ qui empiète à la fois sur le règlement général de protection des données, mais également sur la circulation des données et du savoir ? La Commission qu'il sera utile pour les *« États membres et d'autres parties prenantes (...)*

¹⁰⁷² Ibid. p. 9

¹⁰⁷³ Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016, En ligne: https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=40114AB2CC997861AA4011EAB0025ED6.tplgfr31s_3?cidTexte=JORFTEXT000033202746&categorieLien=id (dernière consultation: 5 mars 2018)

*d'examiner les justifications et la proportionnalité des restrictions*¹⁰⁷⁴ » en la matière.

472. Le droit des données (personnelles ou non) apparaît aux yeux de la Commission comme un instrument au service d'une gestion managériale, d'un nouveau management public visant moins la liberté qu'est la vie privée que la domination d'un marché économique fondé sur la donnée. On comprend dès lors mieux l'intérêt de la Commission de prôner la réassurance des citoyens européens vis à vis de la protection des données personnelles, de rétablir la confiance dans l'économie numérique et de renforcer la sécurité des données.

2. Une consécration dans la proposition de règlement de 2017

473. Le champ d'application du règlement général de protection des données personnelles exclut les données non personnelles. La proposition de règlement en la matière est envisagée de telle manière à ce qu'elle s'ajoute aux éléments du règlement général de protection des données personnelles. Dans sa proposition, la Commission énonce l'existence d'exigences en matière de localisation des données à caractère non personnel qui doivent être entendues comme de véritables entraves au marché du numérique et à l'économie de la donnée. Pour y remédier, tout en garantissant aux autorités compétentes des droits d'accès aux données à des fins de contrôle réglementaire, la proposition de règlement énonce le principe de libre circulation des données non personnelles¹⁰⁷⁵.

474. La proposition de règlement dispose d'un objet et d'un champ d'application très large. Elle vise en effet à « *assurer la libre circulation de données autres que les données à caractère personnel au sein de l'Union, en établissant des règles concernant les exigences de localisation des données, la disponibilité des données pour les autorités compétentes et le portage des données pour les utilisateurs professionnels*¹⁰⁷⁶ ». Elle s'applique « *au stockage ou tout autre traitement de données électroniques autres que les données à caractère personnel dans l'Union, qui est : (a) fourni en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'Union, par un fournisseur établi ou non dans l'Union, ou; (b) effectué par une personne physique ou*

¹⁰⁷⁴ COM (2017) 9, final, p. 9.

¹⁰⁷⁵ Article 4 de la proposition de règlement précité, p. 19.

¹⁰⁷⁶ Article 1er de la proposition de règlement, p. 18.

morale résidant ou disposant d'un établissement dans l'Union pour ses propres besoins¹⁰⁷⁷ ». Au titre de l'article 3, la catégorie des données non personnelles recouvre « les données autres que les données à caractère personnel¹⁰⁷⁸ ». Cette proposition concerne donc les prestations de service du numérique (hébergement, stockage), mais également tout traitement de données non personnelles.

475. Enoncé à l'article 4 de la proposition de règlement, la libre circulation des données au sein de l'Union vise à abolir toute entrave, nouvelle ou existante, en matière de localisation, de stockage et de traitement de ce type de données¹⁰⁷⁹. Selon la Commission, « *les nouvelles règles profiteront aux entreprises et organisations en renforçant la sécurité juridique et la confiance. De plus, elles ouvriront la voie à un véritable marché unique européen du stockage et du traitement des données et, partant, à un secteur européen des services en nuage compétitif, sûr et fiable ainsi qu'à une baisse des prix pour les utilisateurs de services de stockage et de traitement de données. Étant donné que les nouvelles règles ont pour finalité d'accroître la confiance, les entreprises devraient recourir davantage aux services en nuage et se lancer sereinement sur de nouveaux marchés. Elles pourront aussi transférer leurs ressources informatiques internes dans des endroits présentant le meilleur rapport coût-efficacité. Selon les estimations, le PIB de l'UE devrait en définitive enregistrer une croissance supplémentaire de 8 milliards d'euros par an¹⁰⁸⁰ ».*

¹⁰⁷⁷ Article 2, *ibid.*

¹⁰⁷⁸ Pour rappel, l'article 4 du RGPD définit les données à caractère personnel comme suit: « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».*

¹⁰⁷⁹ Nous reproduisons ici l'article 4 de la proposition de règlement concernant la libre circulation des données au sein de l'union: « *1. La localisation des données à des fins de stockage ou de traitement au sein de l'Union n'est pas limitée au territoire d'un État membre spécifique, et le stockage ou le traitement dans un autre État membre ne fait l'objet d'aucune interdiction ou restriction, sauf si elle est justifiée par des raisons de sécurité publique.; 2. Les États membres notifient à la Commission tout projet d'acte qui introduit une nouvelle exigence de localisation des données ou modifie une exigence de localisation des données existante conformément aux procédures définies dans la législation nationale mettant en œuvre la directive (UE) 2015/1535; 3. Dans un délai de 12 mois après le début de l'application du présent règlement, les États membres veillent à ce que toute exigence de localisation des données non conforme aux dispositions du paragraphe 1 soit abrogée. Si un État membre estime qu'une exigence de localisation des données est conforme aux dispositions du paragraphe 1 et peut donc rester en vigueur, il notifie cette mesure à la Commission, accompagnée d'une justification de son maintien en vigueur; 4. Les États membres publient en ligne les détails de toutes les exigences de localisation des données applicables sur leur territoire, par l'intermédiaire d'un point d'information unique qu'ils tiennent à jour; 5. Les États membres communiquent à la Commission l'adresse de leur point d'information unique visé au paragraphe 4. La Commission publie sur son site Web les liens vers ces points d'information unique ».*

¹⁰⁸⁰ En ce sens, voir: Commission européenne, Communiqué de presse - *Etat de l'Union 2017 : un cadre pour la libre circulation des données à caractère non personnel dans l'Union européenne*, Bruxelles, 19 septembre 2017, En ligne: http://europa.eu/rapid/press-release_IP-17-3190_fr.htm (dernière consultation: 5 mars 2018)

476. Cette proposition de règlement permettrait donc d'améliorer la cohérence entre les instruments juridiques européens et nationaux en terme de données non personnelles. L'objectif reste d'appliquer les principes de la libre de circulation dans l'Union Européenne au traitement et au stockage de données autres que les données à caractère personnel. Dans les faits, cette proposition ignore superbement les problématiques liées à l'opération de qualification des données en tant que personnelles. Quid des contentieux relatifs à l'adresse IP, aux métadonnées, et aujourd'hui à la mac adresse¹⁰⁸¹ ? Plus globalement, dans sa promotion de l'économie du marché économique et de la perception de la donnée comme une ressource devant être exploitée, la Commission joue le jeu de la surveillance diffuse. A moins de considérer le droit des données comme une technique de pouvoir visant plus à l'efficacité économique qu'à la protection de la vie privée des citoyens, l'ensemble des instruments proposés engendrent une insécurité juridique, et une totale incompréhension du fonctionnement des technologies de l'information et de la communication.

B. Une nouvelle vision européenne du statut juridique du marché des données ?

477. Le marché unique européen repose depuis sa création sur une logique d'efficacité économique matérialisée par le principe de libre circulation. Les quatre libertés fondamentales du marché unique de l'Union européenne sont la libre circulation des biens, des travailleurs, des services et des capitaux. Si dès l'origine la situation du droit des données personnelles dans ces quatre libertés fondamentales du marché unique était prétexte à interprétation, il semble plus que nécessaire de se demander où se situe le droit des données (personnelles et non personnelles) aujourd'hui.

478. Les premières législations informatiques et libertés nationales prônaient une réelle ambition de protection des libertés, en ce compris la vie privée. La directive de 1995 quant à elle souhaitait déjà trouver un point d'équilibre entre la libre circulation des données à caractère personnel et la protection de la vie privée. Soulignons ici que la directive dans ses considérants réaffirmait l'établissement et le fonctionnement du marché intérieur « *dans lequel conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, (et) nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes*

¹⁰⁸¹ Nous explorons ce contentieux spécifique en paragraphe 2 de cette section.

*soient sauvegardés*¹⁰⁸² ». Les instruments internationaux, tels que la Convention 108 du Conseil de l'Europe¹⁰⁸³ reconnaissent également « *la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples* ». Le règlement général de protection des données personnelles et la proposition de règlement concernant les données non personnelles réitèrent ces affirmations. Ils vont également un peu plus loin puisqu'ils font tous les deux mentions à répétition de la volonté de développer l'économie numérique, le marché unique du numérique et l'économie fondée sur les données.

479. Originellement conçue par référence à la liberté de circulation des services¹⁰⁸⁴, les nouveaux instruments européens entretiennent la confusion. La proposition de règlement envisage clairement la liberté de prestation de service puisqu'elle concerne la prestation des services d'hébergement (de stockage) ou de traitement des données. Toutefois, à la lecture de la communication de la Commission de 2017, fondement de l'élaboration de ce texte, ainsi que du règlement général de protection des données personnelles, cette affirmation ne semble plus vraie. L'insistance des institutions européennes sur les termes de données devant être exploitées comme des ressources, d'économie du numérique et d'économie fondée sur la donnée vont en effet beaucoup plus loin que la simple participation à la liberté d'établissement et de prestation de services. Tout se passe comme si ces instruments reconnaissaient tacitement une libre circulation d'un bien. La question envisagée par la Commission dans sa communication en 2017 quant à la possibilité d'appliquer un droit de propriété (intellectuelle) aux données non personnelles tend pleinement vers cette hypothèse. Or si tel est le cas, si nous passons progressivement à un droit des données devant être analysé comme une consécration de la libre circulation des biens, quel serait le régime de propriété applicable ? Le propriétaire des données (personnelles ou non) serait-il celui qui a élaboré le capteur ? Celui qui a enregistré l'information ? Ces questions paraissent aujourd'hui essentielles¹⁰⁸⁵, d'autant que la volonté de la surveillance diffuse de collecter toujours plus d'informations personnelles ou non brouille la frontière entre la donnée personnelle et la donnée non personnelle.

¹⁰⁸² Considérant n° 3 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*.

¹⁰⁸³ Convention STE - n°108 - pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 Janvier 1981, En ligne: <https://rm.coe.int/1680078b39> (dernière consultation: 5 mars 2018)

¹⁰⁸⁴ Voir en ce sens: OCHOA Nicolas, Op. Cit. p.149: « *le fondement essentiel de la libre circulation de l'information est à un double égard la liberté de prestation de service (...) parce que la communication transnationale d'informations constitue une prestation de service organisée de longue date par les personnes publiques dans le cadre d'un service public international* ».

¹⁰⁸⁵ Nous en donnerons des éléments de réponses dans la section 2 de ce chapitre.

Paragraphe 2: La volonté de la surveillance de construire des profils les plus individualisés possibles: analyse de l'arrêt JC Decaux du Conseil d'Etat du 8 février 2017

480. L'arrêt rendu par le Conseil d'Etat le 8 février 2017 s'inscrit exactement dans les problématiques posées par la surveillance diffuse et par la reconnaissance d'une libre circulation des données personnelles et non personnelles. Les juges administratifs ont été saisi d'un contentieux relatif à l'analyse du comportement des consommateurs permettant aux commerçants de mesurer l'audience de certains panneaux publicitaires (A). A cette occasion, ils ont pu affirmer que l'adresse mac des smartphones constituait une donnée personnelle. A ce titre, des mesures techniques telles que l'anonymisation devait être effective (B).

A. L'analyse des comportements des individus par la mesure de fréquentation et d'audience : un dispositif en développement fondé principalement sur l'analyse de données non personnelles

481. La décision des juges administratifs de reconnaître la mac adresse des smartphones comme étant des données personnelles s'inscrit dans la poursuite des contentieux précédemment cités, et plus spécialement celui lié à l'adresse IP (2). Au préalable à l'analyse de cet élément, il faut avant tout comprendre le dispositif mis en place par la société Decaux (1).

1.Le dispositif d'analyse de comportement des individus par la mesure de l'audience de panneaux publicitaires

482. Dans un monde d'hyperconnectivité lancé dans un processus de smartification (des villes, des maisons, des commerces), l'arrêt du Conseil d'Etat permet d'appréhender un dispositif qui risque de connaître un développement sans précédent. La mesure de l'audience des panneaux publicitaires et la mesure de fréquentation d'un commerce repose toutes deux sur le même principe: l'analyse du comportement des individus face à des sollicitations extérieures et la compréhension, la comptabilisation de l'impact de ces sollicitations. Ce dispositif fonctionne sur le traitement de données principalement non personnelles, qui si elles sont connectées à une donnée personnelle peuvent s'avérer dangereuse. Pour la bonne compréhension de l'analyse, rappelons qu'un rapport

du Parlement européen sur les incidences des mégadonnées de 2016¹⁰⁸⁶ s'inquiétait déjà des potentialités des technologies à déduire négativement ou positivement à partir d'une caractéristique humaine un ensemble de comportement¹⁰⁸⁷. Ainsi, le rapport du Parlement énonce que « *considérant que l'évolution des technologies de communication et l'omniprésence des appareils électroniques, des gadgets de surveillance, des médias sociaux, des interactions web et des réseaux, y compris des équipements qui communiquent des informations sans intervention humaine, ont conduit au développement d'ensembles de données massifs et de plus en plus volumineux qui, grâce aux techniques de traitement avancées et à l'analyse, fournissent des renseignements sans précédent sur le comportement humain, la vie privée et nos sociétés*¹⁰⁸⁸ ». Et de souligner que : « *le respect de la législation en vigueur sur la protection des données, combiné à des normes scientifiques et éthiques rigoureuses, est essentiel pour établir la confiance dans les solutions en matière de mégadonnées ainsi que leur fiabilité; souligne que les informations révélées par l'analyse des mégadonnées n'offrent une vue d'ensemble impartiale sur aucun sujet et ne sont fiables que dans la mesure permise par les données sous-jacentes; souligne que l'analyse prédictive fondée sur les mégadonnées ne peut offrir qu'une probabilité statistique et ne peut dès lors pas toujours prévoir avec exactitude les comportements individuels; souligne dès lors que des normes scientifiques et éthiques rigoureuses sont essentielles pour encadrer la collecte de données et évaluer les résultats de leur analyse*¹⁰⁸⁹ »

483. En l'espèce, la société Decaux a effectué une demande d'autorisation auprès de la CNIL afin de mettre en oeuvre un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de la Défense. Plus

¹⁰⁸⁶ GOMES Ana - Commission des libertés civiles, de la justice et des affaires intérieures, Rapport du Parlement européen (2016/2225 (INI)) *sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi*, 20 février 2017, En ligne: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0044+0+DOC+PDF+V0//FR> (dernière consultation: 5 mars 2018). Le Parlement précise ce qu'il entend par le concept de mégadonnées; « *A. on entend par mégadonnées la collecte, l'analyse et l'accumulation récurrente de gros volumes de données, notamment à caractère personnel, en provenance de diverses sources, qui font l'objet d'un traitement automatique par des algorithmes informatiques et des techniques de traitement de données avancées, en utilisant tant les données stockées que les flux de données, en vue de générer certains modèles, corrélations et tendances (analyse des mégadonnées)* » (p. 4). Cette définition de la mégadonnées et de ce qu'elle permet s'applique totalement à l'analyse du comportement des individus.

¹⁰⁸⁷ L'effet de halo mis en évidence par Thorndike et développé par Asch prend tout son sens ici. Voir en ce sens: TARDIEU Claire, « Corriger ou évaluer ? », *Cahiers de l'APLIUT*, Vol. XXVIII N° 3 | 2009, En ligne: <http://journals.openedition.org/apliut/65> (dernière consultation: 5 mars 2018)

¹⁰⁸⁸ Op. Cit. p. 4

¹⁰⁸⁹ Ibid. p. 8

particulièrement, à la lecture de la délibération de la CNIL¹⁰⁹⁰, la société JC Decaux souhaitait analyser la volumétrie et les axes de déplacements des individus sur ce périmètre. Ce type de dispositif et de traitement n'est pas nouveau. Il est encadré par la loi du 12 juillet 2010 portant engagement national pour l'environnement¹⁰⁹¹ qui instaure un article L. 581-9 dans le code de l'environnement sur ce point. Cet article consacré à la publicité à l'intérieur des agglomérations déclare en son alinéa 4: « *Tout système de mesure automatique de l'audience d'un dispositif publicitaire ou d'analyse de la typologie ou du comportement des personnes passant à proximité d'un dispositif publicitaire est soumis à autorisation de la Commission nationale de l'informatique et des libertés* ». La doctrine de la CNIL sur ce point est alors assez large. Selon cette autorité administrative, les dispositifs installés sur une voie publique ou privée ouverte à la circulation publique (mobilier urbain), ou non installés mais visibles d'une voie publique ou d'une voie privée ouverte à la circulation publique, ou installés dans des locaux principalement utilisés comme support de publicité (vitrine d'un espace de vente) doivent être soumis à autorisation préalable.

484. L'expérimentation de la société JC Decaux s'inscrit pleinement dans ce cadre puisque les outils de mesures d'audience qu'elle avait envisagés aurait dû être installés sur des dispositifs publicitaires. Six boîtiers de comptage WI-Fi devait en effet être installés sur le mobilier urbain pendant quatre semaines afin à la fois de dresser une volumétrie de fréquentation de la Dalle de La Défense, les taux de répétitions et les schémas de mobilité. La délibération précise quelque peu le procédé technique au vu des éléments fournis par le responsable de traitement. « *Six mobiliers publicitaires seraient équipés de boîtiers (...). Chaque boîtier comporterait une carte Wi-Fi permettant de détecter, sur une portée maximale de 25 mètres de rayon, l'adresse MAC de tout appareil mobile équipé d'une connectivité Wi-Fi activée. Chaque boîtier transmettrait, via une connexion sécurisée HTTPS, les données collectées à un serveur exploité par la société Fidzup, hébergé à Francfort¹⁰⁹²* ». Et de préciser que: « *Toutes les deux minutes, le boîtier transmettrait les données collectées au cours des deux minutes écoulées. Ces données seraient: l'adresse émise par la carte WI-FI des appareils situés à moins de 25 mètres du dispositif, l'heure exact de détection*

¹⁰⁹⁰ CNIL, Délibération n°2015-255 du 16 juillet 2015 refusant la mise en oeuvre par la société JC Decaux d'un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense (demande d'autorisation n° 1833589), En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000031159401> (dernière consultation: 5 mars 2018)

¹⁰⁹¹ Loi n° 2010-788 du 12 juillet 2010 portant engagement national pour l'environnement, JORF n°0160 du 13 juillet 2010 p. 12905, texte n° 1, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022470434&categorieLien=id> (dernière consultation: 5 mars 2018)

¹⁰⁹² CNIL, Délibération n) 2015-255 du 16 juillet 2015, Op. Cit.

des cette adresse, la puissance d'émission du signal WI-FI¹⁰⁹³ ». Au vu de ces éléments, la CNIL a été saisi d'une demande d'autorisation de données personnelles pour l'expérimentation de la société Decaux.

2.La qualification de l'adresse mac des smartphones en tant que personnelle: un contentieux pouvant être soumis à la même interprétation que le contentieux lié à l'adresse IP

485. La première étape de l'analyse de cet arrêt du Conseil d'Etat consiste à admettre que les jurisprudences de la Cour de Justice de l'Union européenne ont eu un impact positif dans la culture Informatique et libertés. De fait, la société JC Decaux a qualifié la mac adresse des smartphones en tant que données personnelles dans le cadre de sa demande d'autorisation. Si les arrêts de la CJUE ont eu impact positif, c'est aussi et surtout parce que la CNIL française ne cesse de développer sa doctrine en ce domaine. Sa position concernant la collecte massive d'identifiants Internet présente un intérêt non négligeable dans l'incompréhension générale qui règne autour des concepts de données personnelles et de données non personnelles.

486. L'adresse mac des smartphone est à rapprocher de l'adresse IP des ordinateurs. A moins qu'elle n'ait été modifiée par son propriétaire cette adresse permet d'identifier physiquement, par la carte réseau ou l'interface réseau, de manière unique, un appareil connecté au réseau (allant de la console de jeux, à la tablette et l'ordinateur, en passant par le smartphone). A l'instar de l'adresse IP, l'adresse mac permet donc d'identifier une machine sur le réseau Internet. Elle est donc à l'origine une donnée technique, une donnée non personnelle. Sans revenir sur les développements précédents concernant le contentieux de l'adresse IP, la logique de la société JC Decaux de procéder à la qualification par défaut de l'adresse Mac en tant que donnée personnelle doit être rapproché d'un autre contentieux tout aussi intéressant. Dans sa délibération du 17 mars 2011 concernant Google Street View, la CNIL a en effet sanctionner la société Google d'une amende de 100 000 euros assortie de la publication sur internet de cette décision¹⁰⁹⁴ concernant (entre autres) les données

¹⁰⁹³ Ibid.

¹⁰⁹⁴ CNIL, Délibération n°2011-035 du 17 mars 2011 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société X, En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023733987&fastReqId=1901417590&fastPos=1> (dernière consultation: 5 mars 2018). Il est intéressant de souligner ici la demande d'anonymisation effectuée par Google quant à la mention de son nom dans cette délibération.

SSID¹⁰⁹⁵ et Mac collectées par ce service. Pour le moteur de recherche, ces adresses ne constituent pas au vu de la législation européenne et française en la matière des données personnelles. Cette assertion est techniquement vraie. Le rapport d'expertise de la CNIL, cité par Google dans le cadre de la délibération de 2011 tend d'ailleurs vers cette assertion¹⁰⁹⁶. La CNIL conteste cette position soutenant que les données SSID et Mac, combinées aux données de localisation collectées sont des données à caractère personnel. Dans sa délibération de 2011, la CNIL constate que « *les identifiants SSID permettent d'identifier les réseaux Wi-Fi se trouvant à portée et de s'y connecter et que ces identifiants comportent fréquemment le nom et/ou le prénom des titulaires du réseau ; de tels éléments permettent alors manifestement d'identifier une personne physique. Ces données doivent alors être considérées comme constituant des données à caractère personnel*¹⁰⁹⁷ ». Et d'ajouter concernant l'adresse mac que « *une adresse MAC, qui n'identifie que le routeur Wi-Fi qui permet aux utilisateurs d'accéder à internet, ne peut être qualifiée, à elle seule, de donnée à caractère personnel. En revanche, une adresse MAC peut être captée par des sites Internet lors de la navigation de l'Internaute, après que ce dernier se soit identifié. Une fois reliée à ces éléments d'identification, elle constitue nécessairement une donnée personnelle. C'est en fonction de tels éléments de contexte qu'il convient de décider si une adresse MAC peut être considérée, ou non, comme une donnée à caractère personnel*¹⁰⁹⁸ ». Et de conclure en notant que « *la collecte conjointe d'identifiants SSID et d'adresses MAC, en association avec des données de géolocalisation, est de nature à qualifier l'opération de collecte initiée par la société dans cette affaire de traitement de données à caractère personnel*¹⁰⁹⁹ ».

487. La définition de la notion de données à caractère personnel doit être interprétée de manière extensive; c'est à la fois son principal point fort mais également sa principale faiblesse. Ainsi que le rappelle l'arrêt du Conseil d'Etat du 8 février 2017 dès son second considérant en citant la définition d'une donnée à caractère personnel donnée par le second alinéa de l'article 2 de la loi

¹⁰⁹⁵ Une donnée SSID est une clé alphanumérique de 32 caractères identifiant de manière unique un réseau sans fil. L'objectif de cette donnée est d'empêcher que d'autres équipements sans fil n'accède au réseau local de manière accidentelle ou intentionnelle, puisque pour que des appareils sans fil puissent communiquer, ils devront être configurés avec le même SSID.

¹⁰⁹⁶ On peut ainsi dans la délibération que le « rapport d'expertise de la CNIL lui-même n'identifierait aucune personne physique à partir de la combinaison des données SSID, MAC et des données de localisation - l'emplacement précis d'un routeur Wi-Fi ne pouvant en outre être déterminé avec certitude que dans des zones très peu peuplées

¹⁰⁹⁷ CNIL, Délibération n°2011-035 du 17 mars 2011

¹⁰⁹⁸ Ibid

¹⁰⁹⁹ Ibid.

Informatique et libertés. Cette approche est à nouveau consacrée dans le règlement général de protection des données personnelles. Son considérant 26 rappelle que : « *il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable(...). Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage* ».

B. L'anonymisation des données personnelles: des mesures techniques inopérantes pour garantir la protection de la vie privée ?

488. La question de la qualification des données d'identifications techniques en tant que données à caractère personnel étant réglée, il faut alors porter son attention sur les mesures que le responsable de traitement doit mettre en oeuvre pour garantir la vie privée des personnes dont les données sont collectées et traitées. Ainsi que ce soit dans la délibération de 2011 concernant Google, ou dans l'arrêt du Conseil d'Etat de 2017, une information claire doit être mise à la disposition des personnes¹¹⁰⁰. Il est aussi et surtout question d'anonymisation des données (1) permettant de faire en sorte que les principes de protection des données personnelles ne s'appliquent plus, et de faire émerger le concept de vie privée différentielle (2).

1. La question de l'anonymisation des données comme mesure technique de protection de la vie privée

489. Au titre des mesures techniques permettant de protéger la vie privée, l'anonymisation et la pseudonymisation ont depuis la directive de 95 jusqu'au règlement général de protection des

¹¹⁰⁰ Concernant la délibération de 2011, la CNIL reprochait un défaut d'information de la part de la société quant à la collecte des adresses MAC et des identifiants SSID. Google soutient que cette obligation lui aurait coûté « *un effort disproportionné pour fournir les informations requises par la loi à chacune des personnes concernées (à supposer que celles-ci soient connues), ce qui l'exonérerait de ses obligations en application de l'article 32-III de la loi informatique et libertés* ». Prenant en compte cet élément, la CNIL a admis que « *l'information individuelle des titulaires des adresses MAC et des identifiants Wi-Fi est effectivement impossible à mettre en oeuvre dans de telles circonstances, dès lors qu'aucun lien direct n'existe entre la société et ces personnes, y compris au moment où la société collecte leurs données via les terminaux des utilisateurs de ses services de géolocalisation* ». Et d'estimer que Google devait satisfaire à une obligation générale d'information. Cette obligation générale d'information semble peu adéquate, spécialement au regard de l'acteur de la collecte et du traitement de données concerné. Quant aux dispositifs de mesure de fréquentation et d'audience permettant l'analyse du comportement des consommateurs, la CNIL recommande une information claire devant être affichée dans les lieux où ils sont mis en place. Cette information doit préciser la finalité du dispositif et l'identité du responsable de traitement. En ce sens voir: <https://www.cnil.fr/fr/mesure-de-frequentation-et-analyse-du-comportement-des-consommateurs-dans-les-magasins> (dernière consultation: 5 mars 2018)

données personnelles toujours été entendues comme des mesures techniques permettant de garantir la vie privée des personnes. Selon le groupe de l'article 29, « *la pseudonymisation n'est pas une méthode d'anonymisation . Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile*¹¹⁰¹ ». Cette procédure d'anonymisation considérée comme réversible est alors à distinguer de l'anonymisation irréversible. La directive de 1995, spécialement son considérant 26, permet d'analyser l'anonymisation comme une technique permettant de supprimer assez d'éléments d'une donnée personnelle pour que la personne concernée ne puisse plus être identifiée. Le groupe 29 précise dans son avis de 2014 que « *les données doivent être traitées de façon à ne plus pouvoir être utilisées pour identifier une personne physique en recourant à « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre», soit par le responsable du traitement, soit par un tiers. Un facteur important est que le traitement doit être irréversible*¹¹⁰² ». Et de conclure que, eu égard aux connaissances techniques de 2014, « *aucune des techniques décrites dans le présent document ne satisfait de façon certaine aux critères d'une anonymisation efficace (à savoir, empêcher l'individualisation d'une personne concernée, la corrélation entre les enregistrements se rapportant à un individu et l'obtention par inférence de données concernant un individu). Cependant, dès lors que certains de ces risques peuvent être évités complètement ou partiellement au moyen d'une technique donnée, il est nécessaire de concevoir avec soin l'application d'une technique individuelle à la situation concernée et d'opter pour une combinaison de ces techniques en vue de renforcer la fiabilité du résultat*¹¹⁰³ ».

490. L'arrêt du Conseil d'Etat du 8 février 2017 se situe dans la droite ligne de la conclusion du Groupe 29. La méthode d'anonymisation employée par la société JC Decaux consistait dans le fait de retrancher le dernier octet de l'adresse Mac, « *avant de les compléter par une suite de caractères en application de la technique dite de « salage » et de mettre en oeuvre une méthode dite de « hachage à clé » , en transformant une donnée*¹¹⁰⁴ ». En réalité, la technique proposée par la société Decaux s'assimile à une technique de pseudonymisation qui selon la délibération de la CNIL ne

¹¹⁰¹ Groupe de travail « Article 29 » sur la protection des données, Avis 05/2014 sur les techniques d'anonymisation, Adopté le 10 avril 2014, 0829/14/FR, WP 216, p.3.

¹¹⁰² Ibid. p. 6.

¹¹⁰³ Ibid. p. 26. Précisons également que la norme ISO 29100 définit l'anonymisation comme le « *processus par lequel des informations personnellement identifiables (IPI) sont irréversiblement altérées de telle façon que le sujet des IPI ne puisse plus être identifié directement ou indirectement, que ce soit par le responsable du traitement des IPI seul ou en collaboration avec une quelconque autre partie* » (ISO 29100 : 2011).

¹¹⁰⁴ Conseil d'Etat 8 février 2017, Op. Cit.

peut pas être « *qualifié de technique d'anonymisation, notamment du fait que la société JCDecaux est en mesure de rejouer le procédé de chiffrement, cette société utilisant un sel qui lui est propre et connu, et en raison du faible taux de collision proposé*¹¹⁰⁵ ». A la lecture de l'arrêt du Conseil d'Etat, cette distinction entre pseudonymisation et anonymisation est contestée par le requérant. Tout en niant la valeur normative des avis du Groupe 29, le Conseil d'Etat rejoint la position de la CNIL et déclare que « *il résulte de la définition de la donnée personnelle donnée par les dispositions, citées au point 2 ci-dessus, de l'article 2 de la loi du 6 janvier 1978, qu'une telle donnée ne peut être regardée comme rendue anonyme que lorsque l'identification de la personne concernée, directement ou indirectement, devient impossible que ce soit par le responsable du traitement ou par un tiers. Tel n'est pas le cas lorsqu'il demeure possible d'individualiser une personne ou de relier entre elles des données résultant de deux enregistrements qui la concernent*¹¹⁰⁶ ». La pseudonymisation semble donc être reléguée à ce que le Groupe 29 entendait par mesure de sécurité. Au vu de la décision du juge administratif, il semble que cette technique d'anonymisation réversible doivent être aujourd'hui abandonnée au profit de l'anonymisation irréversible. Dans le premier cas, l'identification de la personne est encore possible par son individualisation qui correspond « *à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données*¹¹⁰⁷ ». Dans le second, tout caractère identifiant d'une donnée ou d'un ensemble de données est supprimé.

491. Citons en guise d'exemple la biométrie à lien faible reconnue comme une technique d'anonymisation relative à la biométrie. L'objectif de la biométrie à lien faible est d'éviter un lien direct entre l'identité d'un individu et ses données biométriques. Pour ce faire, le système étudié propose, pour une donnée biométrique plusieurs identités associées au lieu d'une seule. Ainsi, la vie privée des individus est préservée. Toutefois, certains problèmes techniques peuvent en découler. En effet, un des problèmes que pose cette pratique concerne la révocation à distance. La CNIL indique qu'il est important que l'individu puisse faire supprimer ses données biométriques, même lorsqu'il ne se trouve plus physiquement sur le site de l'entité qui les conserve. Or, comme l'association directe entre l'identité de l'individu et ses données n'existe plus, il n'est plus possible, à partir d'un nom, de supprimer ses données biométriques. Par conséquent, la révocation (ou même le changement de droits d'accès) ne peut se faire que si la personne est présente sur le site. Ainsi, ses

¹¹⁰⁵ Délibération 2015- 255 Op. Cit.

¹¹⁰⁶ Conseil d'Etat, 8 février 2017, Op. cit.

¹¹⁰⁷ Groupe de l'Article 29 sur la protection des données, Avis 05/2014 (Op. Cit). p. 13

données biométriques seront acquises en vue d'être comparées aux autres données, et les droits d'accès ainsi que (potentiellement) le groupe d'identité associé pourront être modifiés. Une alternative à ce problème serait de fournir à chaque utilisateur un numéro « identifiant » jetable ou aléatoire. Celui-ci n'aurait aucun lien avec l'identité des individus mais resterait lié à leur biométrie. Ils pourraient alors utiliser cet identifiant afin de faire supprimer leurs données personnelles à distance. Un deuxième problème technique concerne la taille de la base. En effet, pour que le système de biométrie à lien faible soit efficace (c'est-à-dire pour que l'on ne puisse pas retrouver l'identité d'une personne à partir de sa biométrie et inversement), un nombre important d'identités et de données biométriques doivent être associées.

492. A la lecture de ces éléments concernant les risques que comportent la biométrie à lien faible, il paraît surprenant que la CNIL comme le Conseil d'Etat rendent légitimes les techniques d'anonymisation irréversible et qu'ils relèguent à la position de simples mesures de sécurité, voire à l'abandon, des techniques d'anonymisation réversibles. Cette position semble également dangereuse en terme de protection de la vie privée. Mise en relation avec les propos de la Présidente de la CNIL et les objectifs du règlement général de protection des données, cette technique semble plus servir l'auto-contrôle des entreprises que la maîtrise par les individus de leurs données¹¹⁰⁸.

2.L'émergence du concept de vie privée différentielle ou la consécration de la perte de maîtrise des individus sur leurs données au profit du marché

493. Avant d'évoquer le concept de vie privée différentielle, il faut comprendre quelques éléments. Ainsi que le rappelle Isabelle Falque-Pierrotin, « *le droit des données personnelles relève à l'origine du droit fondamental et incessible à la vie privée*¹¹⁰⁹ ». Dans sa volonté d'élaboration du marché unique du numérique et de l'économie de la donnée, la Commission européenne envisage le droit des données, spécialement non personnelles, comme devant relever de la libre circulation des biens. La problématique de la donnée personnelle réside dans l'identification de la personne concernée. L'enjeu de l'anonymisation présente alors un double intérêt. Le premier est que depuis la directive de 1995, et sous l'empire du règlement général de protection des données personnelles, la

¹¹⁰⁸ En ce sens, voir: AUFFRAY Christophe, *CNIL : « pas d'innovation sans protection des données personnelles »*, 28 mars 2017, Disponible en ligne à l'adresse suivante: <http://www.zdnet.fr/actualites/cnil-pas-d-innovation-sans-protection-des-donnees-personnelles-39850464.htm> (dernière consultation: 5 mars 2018)

¹¹⁰⁹ LesEchos, *Isabelle Falque-Pierrotin: « ceux qui pensent être propriétaires de nos données se trompent »*, 25 novembre 2014, En ligne: https://www.lesechos.fr/25/11/2014/lesechos.fr/0203937716964_isabelle-falque-pierrotin----ceux-qui-pensent-etre-proprietaires-de-nos-donnees-se-trompent--.htm (dernière consultation: 5 mars 2018)

qualification des données en tant qu'anonymisées permet de faire sortir ces données de la catégorie des données personnelles. Ainsi que le rappelle le règlement général de protection des données personnelles, en son considérant 26, « *il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche*¹¹¹⁰ ». On comprend la logique qui se dessine en filigrane de l'arrêt du Conseil d'Etat de 2017. Car, en second lieu, l'anonymisation des données, devenues non personnelles, permet de considérer ces dernières comme devant entrer dans la logique de libre circulation des biens prônées par la Commission. D'une donnée personnelle protégée par le droit au respect de la vie privée, l'anonymisation transforme la donnée en une information non personnelle pour qu'elle entre ainsi dans le champ du marché économique - constituant ainsi une possibilité de cession de la vie privée à rebours. Les dispositifs de mesures d'audience et de fréquentation ne sont pas les seuls à tenter de comprendre le comportement humain. Dans une société où les logiques de performance, de rentabilisation, d'efficacité, de prévision ont pris place, l'étude et l'analyse du comportement humain est aujourd'hui essentiel. Ainsi que le démontre le Parlement européen dans le cadre de son rapport sur les mégadonnées, « *l'évolution des technologies de communication et l'omniprésence des appareils électroniques, des gadgets de surveillance, des médias sociaux, des interactions web et des réseaux, (...) fournissent des renseignements sans précédent sur le comportement humain, la vie privée et nos sociétés*¹¹¹¹ ».

494. Le concept de vie privée différentielle s'est popularisée depuis la keynote de 2016 de la société Apple. Lors de cette conférence, Craig Federighi¹¹¹² déclare: « *la vie privée différentielle est un sujet de recherche dans le domaine des statistiques et d'analyse des données qui utilise le hachage, le sous-échantillonnage et injonction de bruit permettant un apprentissage participatif tout en gardant les données des utilisateurs complètement privées. Apple a accompli un travail « super important » dans ce domaine pour permettre le déploiement de la vie privée différentielle à grande*

¹¹¹⁰ Considérant 26 du RGPD, p. 5

¹¹¹¹ Op. Cit.

¹¹¹² Vice - Président senior de l'ingénierie logicielle chez Apple

*échelle¹¹¹³ ». A la lecture de ces mots on peut se demander si la vie privée différentielle proposée par Apple consiste en une simple influence de la pseudonymisation et de l'anonymisation du droit européen des données personnelles, ou si elle opère une innovation réelle ? Le concept de vie privée différentielle, ou encore de confidentialité différentielle est apparu dans le début des années 2000 aux Etats-Unis. Les tenants de ce concept¹¹¹⁴ propose en réalité « une définition mathématique rigoureuse de la vie privée¹¹¹⁵ ». Et d'ajouter: « *Dans le cas le plus simple, considérons un algorithme qui analyse un ensemble de données et en retire des statistiques .Un tel algorithme est dit « différentiellement privé » si en regardant à la sortie du traitement, on ne peut pas dire si les données d'un individu ont été incluses dans l'ensemble de données original ou non. En d'autres termes, la garantie d'un algorithme différentiellement privé est que son comportement ne change guère lorsqu'un individu entre ou sort de l'ensemble de données - tout ce que l'algorithme peut produire sur une base de données contenant des informations individuelles est presque aussi probable qu'une base de données sans les informations de cet individu. Plus particulièrement, cette garantie est valable pour tout individu et tout ensemble de données. Par conséquent, indépendamment de l'excentricité des détails d'un individu, et indépendamment des détails de quiconque dans la base de données, la garantie de confidentialité différentielle est toujours valable. Cela donne une garantie formelle que les informations individuelles sur les participants à la base de données ne sont pas divulguées¹¹¹⁶ ».* Tout comme les techniques d'anonymisation irréversible européennes, la vie privée différentielle est une science mathématique qui tente d'apprendre le plus*

¹¹¹³ GREENBERG Andy, *Apple's « differential privacy » is about collecting your data - but not your data*, Wired, n 13 juin 2016, En ligne: <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/> (dernière consultation: 5 mars 2018). Traduction libre de l'auteur de: « *Differential privacy is a research topic in the areas of statistics and data analytics that uses hashing, subsampling and noise injection to enable...crowdsourced learning while keeping the data of individual users completely private. Apple has been doing some super-important work in this area to enable differential privacy to be deployed at scale* ».

¹¹¹⁴ DINUR Irit, NISSIM Koby, *Revealing Information while preserving Privacy*, 21 Décembre 2004, Université de Harvard, En ligne: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.1298&rep=rep1&type=pdf> (dernière consultation: 5 mars 2018), Mais aussi: DWORK Cynthia, ROTH Aaron, « *The Algorithmic Foundations of Differential Privacy* ». Foundations and Trends, *Theoretical Computer Science*, Vol. 9; N° 3-4, pp. 211 -407, 2014, En ligne: <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf> (dernière consultation: 5 mars 2018)

¹¹¹⁵ En ce sens, voir : Harvard University Privacy Tools Project, *Differential Privacy, What is differential privacy ?*, En ligne : <https://privacytools.seas.harvard.edu/differential-privacy>

¹¹¹⁶ Ibid. Traduction libre de l'auteur de: « *Differential privacy is a rigorous mathematical definition of privacy. In the simplest setting, consider an algorithm that analyzes a dataset and computes statistics about it (such as the data's mean, variance, median, mode, etc.). Such an algorithm is said to be differentially private if by looking at the output, one cannot tell whether any individual's data was included in the original dataset or not. In other words, the guarantee of a differentially private algorithm is that its behavior hardly changes when a single individual joins or leaves the dataset -- anything the algorithm might output on a database containing some individual's information is almost as likely to have come from a database without that individual's information. Most notably, this guarantee holds for any individual and any dataset. Therefore, regardless of how eccentric any single individual's details are, and regardless of the details of anyone else in the database, the guarantee of differential privacy still holds. This gives a formal guarantee that individual-level information about participants in the database is not leaked* ».

possible d'informations sur un groupe d'individus tout en apprenant le moins possible sur un individu isolé dans le groupe, tout cela, en anonymisant pleinement les données personnelles (individuelles). A l'image de la biométrie à lien faible, on ne peut ici extraire d'information sur une personne spécifique, puisque perdu dans le flot d'un groupe, on ne peut plus identifier ou individualiser une personne en particulier.

495. Sans revenir sur les problématiques dégagées précédemment quant à ce type d'anonymisation, il faut noter ici qu'on retrouve la même logique que celle qui a permise l'apparition de la *privacy by design*. Les promoteurs de la vie privée différentielle ne sont pas de simples universitaires, ils ont étroitement collaboré avec les GAFAM¹¹¹⁷. Cette position reste, sans paranoïa, assez ambiguë car le but de cette technique est de transformer la vie privée en une mesure quantifiable. Ces mesures d'anonymisation désinstituent le droit à la vie privée au profit, là encore, d'une logique marchande. Ainsi perçue, la vie privée n'est plus cette capacité de l'homme à s'isoler, à être laissé seul, afin de pouvoir s'individualiser, se former, s'exprimer. Pire encore, ce concept transforme l'individu en une statistique de groupe. Ainsi défini, la notion de *dividu*, chère à Deleuze et Guattari¹¹¹⁸, apparaît. Reprise plus récemment par Alexander Bard et Jan Söderqvist, le *dividu* est cet « *être humain perçu non pas comme indivisible (individu), mais comme divisible. Le dividu nourrit en son sein de multiples identités, dont aucune n'est perçue comme plus réelle ou plus originale que les autres, et permet à chaque facette de prévaloir sur les autres en fonction des nécessités de l'adaptation au contexte, alors que l'individu s'efforce de n'être qu'une même personnalité intégrée*¹¹¹⁹ ».

Section 2: Pour une appréhension de la surveillance diffuse au travers de la théorie juridique de l'information

496. Puisque aujourd'hui tout chez l'individu est source d'informations, et que la surveillance diffuse, basée sur l'information et la communication, cherche à en recueillir toujours plus, il semble qu'il faille rejoindre les propos de Pierre Catala lorsqu'il évoquait l'idée d'une *lex ferenda* d'une société informatisée fondée sur cette notion. La complexité des problèmes de Droit actuels soulevée

¹¹¹⁷ Cynthia Dwork travaillait chez Microsoft alors qu'elle envisage cette notion

¹¹¹⁸ DELEUZE Gilles, GUATTARI Félix, *Mille plateaux, Capitalisme et schizophrénie II*, Paris, Minuit; 1980.

¹¹¹⁹ BARD Alexander, SODERQVIST Jan, *Les Netocrates 2, The Body machine*, traduit de l'anglais par Abeline Majorel, Editions Léo Scheer, 2011, p. 521.

par la surveillance diffuse, l'incohérence de certaines dispositions légales face à ce phénomène, leur manque d'effectivité, pousse la pensée du juriste « *fidèle au discours de la méthode*¹¹²⁰ », à se tourner « *vers ce qu'il y a de plus général*¹¹²¹ ». L'appréhension de la surveillance diffuse par le recours à la notion d'information a en effet le mérite de traduire et de comprendre l'ensemble des problèmes posés par la surveillance diffuse. Le problème posé par la surveillance diffuse réside principalement dans la question de l'appropriation de ces données, de ces informations (paragraphe 2). La question de l'appropriation des données suppose de les comprendre comme des biens, puisqu'en droit seul un bien est susceptible d'appropriation (paragraphe 1).

Paragraphe 1: La catégorie juridique des biens comme possible réponse du droit aux problématiques posées par la surveillance diffuse sur le droit des données

497. En 2010, Thomas Berns et Antoinette Rouvroy soulignent que la gouvernementalité algorithmique que suppose la surveillance diffuse trouble le juriste. Ce dernier se trouve face « *au paradoxe suivant: quand bien même le caractère objectivement personnel des données en jeu est difficilement attestable, leur inscription dans le cadre général d'une gouvernementalité statistique (...) induit la possibilité d'une action sur les environnements qui les dépasse nettement*¹¹²² ». A la lecture de ces lignes, il faut nécessairement conclure au manque d'effectivité de la notion de donnée personnelle, ainsi qu'à son impossibilité à retranscrire de l'ambition de la surveillance diffuse. En effet, si une conception étriquée de cette notion soulève des inquiétudes en termes de droits fondamentaux des citoyens, son élargissement croissant semble tout autant dangereux pour permettre la garantie efficace d'une protection. La surveillance diffuse transforme l'enjeu de la protection des données personnelles et de la vie privée, et cela, que l'on évoque le fait qu'une information technique puisse être envisagée par truchement technologique, ou par opération de requalification par le juge, de donnée à caractère personnel; ou encore que la protection des données telle qu'envisagée actuellement puisse tendre de plus en plus vers la perte de sens du droit à la vie privée. Plus que l'enjeu de la protection, la surveillance diffuse brouille les notions juridiques au coeur même de cette protection. Le recours à la notion d'information (A) ainsi qu'à la théorie juridique de l'information présentée par Catala (B) semble apporter quelques réponses efficaces à la

¹¹²⁰ CATALA Pierre, Op. Cit.

¹¹²¹ Ibid.

¹¹²² ROUVROY Antoinette, BERNs Thomas, Op.Cit., p. 100.

surveillance diffuse, ou du moins tente d'apporter un peu de clarté à un droit qui en manque cruellement.

A. De l'utilité du recours à la notion d'information pour appréhender autrement le droit des données

498. La surveillance diffuse brouille la frontière entre les notions de données personnelles et de données non personnelles (1). Le recours à la notion d'information, saisie par le droit permet alors d'apporter quelques éléments d'éclaircissements (2)

1. Le brouillage de la frontière entre données personnelles et non personnelles par la surveillance diffuse

499. Le développement de l'informatique, l'avènement de la société fondée sur l'information et la communication ont fait de l'information même une réalité de plus en plus indépendante, constitutive d'une matière première, au même titre que l'énergie. Rappelons ici les mots de Wiener précédemment cités selon lesquels l'information « est le nom pour désigner le contenu de ce qui est échangé avec le monde extérieur à mesure que nous nous y adaptons et que nous lui appliquons les résultats de notre adaptation. Le processus consistant à recevoir et à utiliser l'information est les processus que nous suivons pour nous adapter aux contingences du milieu ambiant et vivre dans ce milieu. (...). Vivre, c'est vivre avec une information adéquate. Ainsi, la communication et la régulation concernent l'essence de la vie intérieure de l'Homme, même si elles concernent sa vie en société¹¹²³ ».

500. Les technologies de l'information et la gouvernementalité algorithmique permettent de mélanger l'art du savoir et du pouvoir par la collecte massive de données, l'élaboration « de nouveaux savoirs et pouvoirs statistiques¹¹²⁴ » tels que le data mining, le profilage, dans « une temporalité actuarielle et préemptive¹¹²⁵ » pour reprendre les mots de Thomas Berns et Antoinette Rouvroy. En parallèle, les activités humaines produisent, manipulent et transforment l'information

¹¹²³ WIENER Norbert, Op. Cit.

¹¹²⁴ ROUVROY Antoinette, BERNS Thomas, Op.Cit., p. 90 - 91.

¹¹²⁵ Ibid. p. 92 - 93.

dont la valeur économique ne cesse de croître. Modification des modes de raisonnement, transformation des modes décisionnels et d'actions, nouvel équilibre des pouvoirs, gestion, prévention, anticipation sont autant de conséquences fines¹¹²⁶ de la surveillance diffuse, et de son appétit pour les informations. Selon André R. Bertrand, « *la dualité données/informations est fondamentale. Nous vivons dans un monde de données, mais les médias nous abreuvent, à longueur de journées, d'informations. Mais, c'est l'interprétation de ces données pour une utilisation particulière qui les transforme en informations. Prenons, par exemple, les cours de la bourse dans un journal : il s'agit d'un tableau de données dont seul un spécialiste financier pourra en extraire une information et en tirer les conséquences qui lui permettront d'agir dans un sens ou dans un autre ; la finalité de l'information étant l'aide à la décision*¹¹²⁷ ». Ce monde de données décrit par Bertrand est le monde révélé par la surveillance diffuse. La surveillance diffuse, par la collecte d'information qu'elle suppose, constitue une aide à la décision.

501. Et, si son affirmation est plus que vraie, on pourrait également dire que la réciproque l'est tout autant, c'est-à-dire qu'une information (technique) peut devenir une donnée (personnelle) à l'image des informations de trafic et de connexion précédemment décrites. Bien que la dualité de ces deux notions soit fondamentale selon certains auteurs de doctrine, cette dualité perd de plus en

¹¹²⁶ On notera ici une conclusion qu'écrivait Christian Laval en 2014 dans le cadre d'un séminaire du Sophiapol, relatif à *Foucault, la surveillance et nous*: « *Je crois que le néolibéralisme sécuritaire fonctionne sur certaines règles assez nouvelles. J'en distinguerai cinq : 1) Le cyberspace est un champ de bataille sur lequel chacun est un ennemi potentiel (ennemi de nouvelles formes de propriété, en particulier de la propriété intellectuelle, ou bien ennemi de la sécurité nationale). 2) On peut dire, écrire, faire ce qu'on veut en démocratie dans les limites des lois, mais à condition d'accepter que tout ce qu'on dit, écrit ou fait librement soit écouté, lu, observé par un pouvoir invisible qui est « officiellement » voué à la sécurité nationale et à l'élimination préventive des terroristes invisibles. 3) Tout ce qu'on dit ou écrit, toutes les traces laissées par nos actes, doivent pouvoir être enregistrés et archivés sinon pour l'éternité du moins pour une longue durée dans des data bases qui serviront « au cas où », afin de remonter jusqu'à chacun en cas de soupçon ou de recherche. 4) Tout ce qu'on dit, écrit ou fait doit pouvoir être traité dans des datas centers par la pratique du data mining (exploitation des données) permettant de donner potentiellement de chaque être humain un « profil » politique et moral permettant de déterminer sa dangerosité potentielle. Chaque personne aura donc une identité fabriquée par les fichiers et évolutive, au fur et à mesure de ses actes. 5) Un nouveau régime de punition se met en place, fondé sur le paradigme de l'élimination sans argument et sans procès. De la même façon que le non recrutement dans une entreprise, le refus de carte de crédit ou d'emprunt, n'ont pas à être justifiés autrement que par la « diminution des risques » pour l'entreprise selon des critères discrétionnaires, le meurtre ciblé du terroriste par le pouvoir de l'administration est admis comme la seule manière de garantir la sécurité nationale et globale. Séries télévisées et films de fiction en fournissent la version esthétique comme le roman noir du XIXe illustre et légitimait à la fois le régime punitif et coercitif des débuts du capitalisme ». (in. LAVAL Christian, *Foucault, la surveillance et nous*, Séminaire du Sophiapol: « Politiques de Foucault », 15 mars 2014, En ligne: <http://questionmarx.typepad.fr/files/foucault-la-surveillance-et-nous.pdf> (dernière consultation: 5 mars 2018)). On ajoutera que le néolibéralisme permet d'obtenir un « apport volontaire, intéressé, naïf, d'informations par l'individu lui-même qui ne voit aucun risque dans la collecte et le traitement de ses données par des tiers qui lui veulent du bien » pour reprendre les mots de Jean Frayssinet précédemment cités. On ajoutera avec lui que « *la valeur de ces dernières est neutralisée: elle est ramenée à la seule valeur d'usage immédiat, les données personnelles ne sont plus porteuses d'autres valeurs, culturelles, idéologiques par exemple. Le traitement des données personnelles est alors forcément ressenti positivement comme permettant une augmentation de la liberté par la capacité accrue d'accès et d'utilisation des services numériques, et non comme un risque pour les libertés personnelles* ». FRAYSSINET Jean, Op. Cit., 2008, p. 71.*

¹¹²⁷ BERTRAND André, *Droit d'auteur*, Editions Dalloz, Collection Dalloz Action, 2010, Point 201.12.

plus de clarté avec la surveillance diffuse. L'auteur poursuit son analyse en donnant plus de précisions sur ces deux notions. Selon lui, « *la donnée, matière brute, peut se présenter sous de multiples formes (chiffres et/ou textes, sur papier ou informatisés...), mais elle est, en tout état de cause, matérialisée ou fixée sur un support (papier, magnétique...). L'information est un message qui peut être transmis oralement ou qui, le plus souvent, résulte de l'interprétation de données. Ce message peut avoir une seule finalité, ou des finalités multiples, dans la mesure où la même information peut être utilisée différemment ou à plusieurs reprises par ceux qui en disposent*¹¹²⁸ ».

502. Appliquée à la surveillance diffuse et au vu des éléments qui précèdent concernant les données de connexion, les données de trafic, les données personnelles et non personnelles, il semble que l'on puisse totalement convenir du fait que l'information représente bien l'essence réelle de la surveillance diffuse. Il apparaît clair également par l'effet de la collecte, l'enregistrement et le traitement de données (personnelles ou non), ces dernières ont de plus en plus vocation à recevoir le qualificatif d'information dans le cadre de la surveillance diffuse. Une théorie juridique de l'information pourrait servir de grille d'analyse efficace pour appréhender ces transformations sociales, mais également pour tenter d'apporter une réponse efficace du droit aux problématiques soulevées par la surveillance diffuse.

2. La notion d'information saisie par le Droit

503. Evoquer la théorie de l'information passe également par l'étude de l'état actuel du discours juridique, que ce soit au travers de la loi ou de la doctrine, sur la notion d'information. La première définition juridique de cette notion apparaît en 1981 dans le cadre d'un arrêté portant sur l'enrichissement du vocabulaire de l'informatique¹¹²⁹. L'information est alors définie comme un « *élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé,*

¹¹²⁸ Ibid. Et de poursuivre: « *En d'autres termes, l'information est un message : - exploitable (à des fins commerciale, politique ou personnelle...) ; - qui perd généralement son intérêt dès qu'elle a été utilisée ou, même en l'absence d'utilisation, qui se périmé par la survenance d'événements ou par sa divulgation. Une information peut ainsi valoir des millions de francs à un instant donné et quelques centimes deux ou trois heures plus tard ; - qui peut être transmise avec ou sans support (information orale/écrite) ou être véhiculée sur un support durable ou altérable (papier/enregistrements magnétiques). La nature de l'information pose le problème de la détermination de sa valeur intrinsèque et de sa matérialité, qui génère des problèmes probatoires tant dans son existence même que lors de sa communication ».*

¹¹²⁹ Arrêté du 22 décembre 1981 - *Enrichissement du vocabulaire de l'informatique*, JORF du 17 janvier 1982, numéro complémentaire, page 624, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000842020> (dernière consultation: 5 mars 2018)

*traité ou communiqué*¹¹³⁰ ».

504. On retrouve dans cette définition des éléments liés à la protection de la donnée personnelle: la conservation, le traitement, la communication. Couplée à l'article 2 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication¹¹³¹, elle peut être des signes, des signaux, des écrits, des images, des sons ou des renseignements de toute nature. De cette brève énumération, on a comme le rappelle Jean-Christophe Galloux l'impression que « *le législateur ne s'est préoccupé que du contenu de l'information, des moyens de sa communication ou de sa diffusion. Au vrai, on retrouve là une attitude assez commune parmi les juristes à l'égard de l'information: le terme « information » est employé dans un sens utilitaire, en considération du contenu du message, car les droits considérés sont destinés à régir les problèmes relatifs au droit et à la liberté d'informer. C'est moins le concept d'information qui importe que les actions dont elle peut être l'objet. On pourrait à ce propos citer l'ensemble des textes relatifs à la protection des informations personnelles (image, voix, souvenirs, correspondances, communications, données médicales ou intimes...)*¹¹³² ». Sans revenir sur les concepts de société de l'information, et les éléments de développement des institutions européennes, la conclusion de Galloux ne peut être que partagée par l'ensemble des juristes. On l'a vu la surveillance diffuse s'est développée autour des notions de communication et d'information. Les législateurs nationaux ou européens se sont d'abord préoccupés d'encadrer les moyens de communication et de diffusion pour ensuite tenter d'appréhender la notion d'information. Il est nécessaire de se tourner vers la doctrine et la pratique pour tenter de concevoir l'information, non plus comme un service, mais bien comme un objet à part entière.

505. La doctrine se partage alors entre plusieurs visions du concept. Soit elle se contente de limiter la qualification de l'information à son contenu¹¹³³; soit elle la limite à sa nature (logiciel,

¹¹³⁰ Ibid.

¹¹³¹ Loi n° 86-1077 du 30 septembre 1986 relative à la liberté de communication, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000512205 (dernière consultation: 5 mars 2018)

¹¹³² GALLOUX Jean-Christophe, *Ebauche d'une définition juridique de l'information*, Recueil Dalloz, 1994, p. 229

¹¹³³ Dans l'article précité, Galloux évoque une « *attitude plutôt utilitariste (qui) consiste à donner de l'information une définition qui dépende de son contenu et non de sa nature, sans d'ailleurs rechercher à connaître cette dernière. (...)*. Ainsi, MM. Aube et Ducos-Ader définissent-ils l'information comme « *... l'action consistant à porter à la connaissance d'un public certains faits ou opinions à l'aide de procédés visuels ou auditifs comportant des messages intelligibles pour le public : l'information est également le résultat de cette action sur les destinataires* ». Si elle englobe la source, le destinataire, le contenu et les moyens de la communiquer, cette définition ne nous enseigne pas ce que l'information peut être en soi. Ce n'est pas sa vocation ».

signe distinctif, donnée, invention, création, savoir-faire)¹¹³⁴. Ces deux approches ne permettent pas là de comprendre l'information comme un objet d'étude saisi pleinement par le Droit. Pourtant, ainsi que le démontre Galloux, « *la catégorisation juridique n'empêche pas de reconnaître au réel sa diversité: que l'on songe à la classification des biens. Le catégorie des meubles regroupe des éléments fort disparates, des animaux aux valeurs mobilières en passant par les toiles aux cimaises du musée Condé*¹¹³⁵ ».

B. La théorie juridique de l'information de Pierre Catala ou la possibilité de comprendre les données comme un bien juridique

506. L'ébauche de la théorie juridique de l'information que Pierre Catala énonçait en 1982¹¹³⁶ présente un intérêt pour permettre de contrer la désinstitution du droit des données personnelles et du droit au respect de la vie privée . S'interrogeant sur ce concept, le Professeur Catala écrit: « *les dictionnaires disent que le verbe « informer » possèdent deux significations: donner forme, structure, signification, d'une part; mettre au courant, faire part, instruire, d'autre part. Sans doutes n'y a-t-il là que les deux étapes d'une unique fonction, le transfert de connaissances. L'information est d'abord expression, formulation destinée à rendre un message communicable; elle est ensuite communiquée, ou peut l'être, à l'aide du signe choisi pour porter le message à autrui*¹¹³⁷ ». L'intérêt principal de la théorie juridique de l'information dégagée par Pierre Catala est qu'elle s'intéresse à l'appropriation de cette dernière. Avant même d'évoquer cette idée d'appropriation, il faut évoquer la théorie du Professeur Catala qui envisage le rapprochement des données et des informations en tant que bien juridique (1). Il faut également enrichir cette recherche d'une nouvelle catégorisation juridique applicable aux données, réduites aujourd'hui à leur valeur informative. La notion de bien commun présente alors un intérêt non négligeable (2).

¹¹³⁴ Galloux évoque à ce propos une « *attitude pragmatique* » qui « *consiste à ne considérer que les « structures d'information », c'est à dire à ne considérer que l'information spécifiée, coulée dans une forme particulière à laquelle le droit positif confère ou est susceptible de conférer une qualification. (...). En dernière analyse, elle est toute forme ayant une valeur économique « en raison du public qui la convoite* ». Il n'est pas nécessaire que le type d'information en cause ait été qualifié par le droit: l'information génétique par exemples considérée comme une information indépendamment de toute qualification positive. Mais de façon significative, en qualifiant cette information, on s'abstiendra de rechercher en quoi elle est une information ».

¹¹³⁵ GALLOUX, op. Cit.

¹¹³⁶ Op. Cit.

¹¹³⁷ CATALA Pierre, *Le droit à l'épreuve du numérique - Jus ex Machina*, Presses Universitaires de France, Collection Droit, Ethique, Société, Première édition, mai 1998, p. 228.

1. L'ébauche de l'application de la catégorie juridique des biens aux données

507. Selon Pierre Catala, l'information est une succession de formulation et de communication reposant sur des outils permettant la communication. L'auteur poursuit d'ailleurs son analyse en anticipant le progrès technologique. Il déclare fort justement que « *dans ce tourbillon de techniques, la définition esquissée plus haut conserve sa validité. aujourd'hui, comme hier, l'article 1 du Droit de l'information pourrait toujours affirmer « tout message communicable à autrui par un moyen quelconque constitue une information. Pourquoi, dès lors, ne pas supposer que les principes propres à encadrer les corps de règles périphériques à l'information peuvent se déduire de ces éléments primaires dont la stabilité est avérée ?*¹¹³⁸ » De là, s'appliquent alors deux types de droits: un droit sur l'information¹¹³⁹ et un droit à l'information¹¹⁴⁰. Ces deux éléments développés par Catala opèrent aux yeux du juriste, par effet miroir, avec la notion de données et plus loin de données personnelles et non personnelles.

508. Pierre Catala, dans son ébauche pour une théorie juridique de l'information, évoque clairement le droit d'obtenir des informations privées. Il écrit alors que « *dans le domaine des informations nominatives, la loi du 6 janvier 1978 a fait franchir un pas important à la théorie juridique. Elle reconnaît aux individus des prérogatives considérables sur les données qui les concernent nommément. (...). Ce sont là des prérogatives de droit réel. Elles consacrent implicitement l'appartenance de la donnée nominative à la personne concernée, légitime titulaire qui peut, en cette qualité, vérifier leur bon usage et leur véracité, sous certaines contraintes et limites que le législateur a édictées pour des motifs d'intérêt général. Il nous paraît donc que la protection accordée par la loi sur l'informatique et les libertés reflète un droit sur l'information personnalisée plutôt qu'un droit à cette information. Aussi est-ce en la personne des tiers et non du sujet qu'il faut rechercher l'existence éventuelle d'un droit aux données nominatives relatives à*

¹¹³⁸ Ibid. p. 229 - 230

¹¹³⁹ Pierre Catala déclare à ce propos: « *considérée dans son objet, l'information est produite par celui qui lui donne forme. Il n'est pas étonnant que tende à s'établir entre l'auteur et l'objet une relation de possédant à possédé, ressortissant au droit réel. On en sera pas d'avantage surpris que cet objet initial, l'information originelle, se prête souvent à transport, dépôt, louage, transfert...* ». Ibid. p. 230

¹¹⁴⁰ Sur ce point l'auteur évoque que « *considérée en fonction de sa destination et non plus de son objet, l'information apparaît promise à la communication, vouée à elle à peine de perdre sa raison d'être. Autrui est son but. La réalisation de ce fut va donc créer une relation entre l'émetteur et le récepteur de l'information. Qui est le maître de ce rapport ? Le détenteur de l'information est-il fondé à la retenir au lieu de la communiquer? Son destinataire potentiel est-il, au contraire, fondé à la réclamer comme un élément du savoir humain dû à chacun, au nom du droit de l'homme à la connaissance ?* ». Ibid.

*autrui*¹¹⁴¹ ».

509. De fait, par ces mots, le Professeur Catala voit dans le droit à la protection des données personnelles un droit sur l'information qu'ont les individus et un droit à l'information qu'ont les tiers (secteur privé ou public). Cette logique paraît rendre plus clair les possibles protections à envisager. Du moins, elle semble donner de l'effectivité à un droit, qui lui, semble en manquer. La conclusion de Catala sur ce droit sur l'information privée est alors fort enrichissante puisqu'elle permet d'éviter le premier problème de la surveillance qui réside dans le manque de conscience de ses enjeux. L'auteur écrit: « *le plus grand nombre d'informations, cependant, ne ressortit pas au statut particulièrement protecteur des données nominatives ou des propriétés intellectuelles. Pourtant si l'on adhère au raisonnement exposé plus haut, une information quelconque ne mérite son nom que si elle a été créée par une opération intellectuelle de formulation, qui emporte appropriation bénéfique du metteur en forme. C'est dire qu'on ne devrait pas juridiquement rencontrer d'information « vacante et sans maître ». De là, procède une conséquence certaine pour ce qui nous occupe ici: il n'existe pas un droit du public à la divulgation d'une information privée, alors même que celle-ci ne constitue pas une création littéraire ni une invention brevetée. (...). Il faut y voir un effet normal de l'appropriation: le droit de rétention s'attache par nature à la possession légitime. L'infériorité de la « propriété ordinaire » de l'information sur les statuts particuliers qui la renforcent est éclatante si on l'observe après la divulgation: elle ne jouit que d'une opposabilité inconsistante et souffre d'une absence de protection utile contre les usurpations. Du moins, cette chétive propriété comporte-t-elle le pouvoir préalable de ne pas divulguer. Par cet attribut négatif mais énergique, le droit du maître sur l'information tient en échec le droit d'autrui à l'information*¹¹⁴² ». Alors qu'aujourd'hui, la valeur libertaire de la protection des données personnelles est neutralisée au bénéfice d'un ressenti positif au traitement des données, vu comme « *permettant une augmentation de la liberté*¹¹⁴³ », il semble plus que nécessaire de voir en la donnée, en la protection des données personnelles, un droit sur l'information conférant une « chétive propriété » aux individus, permettant ainsi à ces derniers « de ne pas divulguer » préalablement ces dernières.

510. Au-delà de cette « chétive propriété », l'ensemble de la démonstration de Pierre Catala est

¹¹⁴¹ CATALA Pierre, Op. Cit., p. 239.

¹¹⁴² CATALA Pierre, Op. Cit., p. 242.

¹¹⁴³ FRAYSSINET Jean, Op. Cit.

axée autour de la notion d'information qui, selon lui, doit être analysée comme suit: « *l'information est un bien créé et non pas donné. C'est un produit de l'activité humaine. Les conditions de son appropriation sont liées à celles de sa genèse: la naissance de l'information est génératrice d'un bien. Une fois créé, ce bien peut donner lieu à un commerce juridique complexe: la vie de l'information est génératrice de contrats*¹¹⁴⁴ ».

2. Recherche d'une catégorie juridique des biens applicable à la notion d'information et potentiellement au droit des données

511. Il faut ici garder en tête les mots de Jean-Christophe Galloux quand il écrit que « *c'est moins le concept d'information qui importe que les actions dont elle peut être l'objet. On pourrait à ce propos citer l'ensemble des textes relatifs à la protection des informations personnelles (image, voix, souvenirs, correspondances, communications, données médicales ou intimes...)*¹¹⁴⁵ ». Ajoutons qu'au vu de la logique de transformation du droit des données et de la vie privée, la conception même des données paraît pouvoir évoluer. Les techniques d'anonymisation se développeront de plus en plus au vu de l'élaboration d'un contrôle a priori par le règlement général de protection des données, mais également au vu de l'ambition de la Commission de créer l'économie fondée sur la donnée.

512. Ces techniques qui permettent de faire entrer dans le champs des données non personnelles, des informations, à l'origine, personnelles, font également perdre au droit des données tout lien avec la protection offerte au titre du droit au respect de la vie privée. Elle permet donc de supprimer le caractère incessible de ces données. Ainsi réduite à une valeur statistique cessible, la donnée doit s'analyser à la lumière du concept d'information, et de son lien avec la catégorie des biens immatériels. La donnée aujourd'hui permet à la surveillance diffuse de connaître l'individu, son identité, son adresse physique et numérique, ses photos, ses contacts, ses habitudes de consommation, ses opinions, son état de santé, ses centres d'intérêts par sa navigation internet et ses

¹¹⁴⁴ CATALA Pierre, Op. Cit., p. 230

¹¹⁴⁵ GALLOUX Jean-Christophe, *Ebauche d'une définition juridique de l'information*, Recueil Dalloz, 1994, p. 229

usages technologiques. Ces informations ont une valeur¹¹⁴⁶ à la fois pour les industries du numérique, mais également pour les individus: le bien être, la liberté, la sécurité, l'accès à la connaissance et à la culture et peuvent alors être assimilées à un bien. Dans cette description se dessine une forme d'utilité publique dans la réduction des données à un bien : utilité de l'économie des données, de la prévision qu'elle porte en son sein, de la connaissance de soi et des autres.

513. Dans leur dictionnaire des biens communs, Marie Cornu, Fabienne Orsi et Judith Rochfeld déclarent que l'utilité publique doit être analysée comme une « *clef de glissement des choses vers les biens*¹¹⁴⁷ ». Dans son versant économique et dans son versant sécuritaire, la surveillance diffuse s'inscrit pleinement dans cette logique d'intérêt public et d'utilité publique. Elle permet également de faire glisser la donnée personnelle (devenue non personnelle) vers la catégorie des biens. Poursuivant leur analyse, les auteures déclarent: « *une lecture propriétaire de l'utilité publique s'impose doublement en matière de communs. Elle s'impose d'abord car elle renvoie à la définition même de ce qu'est la propriété, à savoir la réunion des utilités d'une chose dans le triptyque usus/abusus/fructus, réunion connue depuis les dominia utilia exercées sur la terre romaine, chez Justinien (Saint Victor, 2014). Elle s'impose ensuite car, depuis Ulpien et Javolénus dans le Digeste au VIe siècle (on ne peut proprement appeler biens les choses qui sont plus nuisibles qu'avantageuses* », *Digeste*, 50, 16, 83) jusqu'à Portalis, (« *Les choses ne seraient rien pour le législateur sans l'utilité qu'en tirent les hommes* ») et Demolombe (« *Il n'y a de bien pour nous Jurisconsulte que ce qui peut servir à l'Homme* »), le bien se définit généralement comme la chose susceptible d'appropriation, c'est-à-dire comme la chose dont l'utilité justifie la maîtrise. En ce sens, l'utilité s'entend comme « *ce dont l'usage est ou peut être avantageux, satisfaisant un besoin* » (Littré). C'est ainsi que l'utilité économique, synonyme de richesse et de convoitise, justifiera le plus souvent le passage d'une chose dans la catégorie des biens dans une approche exclusive de la propriété¹¹⁴⁸ ».

514. Au-delà de l'approche patrimoniale, ces mots ne sont pas sans rappeler l'ambition des

¹¹⁴⁶ Voir: The Boston Consulting Group, *The value of our digital identity*, Liberty Global Policy Series, Novembre 2012, Disponible en ligne à l'adresse suivante: <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf> (dernière consultation: 5 mars 2018). Ce rapport déclare que « *la valeur créée par l'identité numérique est impressionnante - taux de croissance annuel de 22% - qui appliqué aux données personnelles peut générer un bénéfice économique annuel de 330 milliards d'euros pour les organisations européennes d'ici 2020. (...) La valeur totale de l'identité numérique combinée pourrait représenter environ 8% du PIB de l'Union européenne des 27* ». (p. 3-4)

¹¹⁴⁷ CORNU Marie, ORSI Fabienne, ROCHFELD Judith (Sous la direction de), *Dictionnaire des biens communs*, PUF / Humensis, Collection Quadrige, 2017, sous la définition de l'utilité publique.

¹¹⁴⁸ Ibid.

institutions nationales et européennes d'envisager l'économie de la donnée et le marché unique numérique. La donnée correspond aujourd'hui à un avantage, à une garantie de prévision, de connaissance et de reconnaissance. L'intérêt général de sécurité et d'économie justifie la volonté de la puissance publique de faire glisser les données progressivement vers la catégorie juridique des biens, et potentiellement des biens communs. La logique inhérente à la création des biens immatériels, ayant trouvé un écho dans le droit de la propriété intellectuelle, a permis par exemple à la puissance publique de protéger l'innovation. Si l'accès à la connaissance, à la culture et à l'innovation est aujourd'hui susceptible d'appropriation, c'est bien du fait de l'intervention de la puissance publique¹¹⁴⁹. L'ensemble des mouvements Open Data, e-démocratie, e-administration peut également être analysé comme des biens communs immatériels, informationnels, ou comme participant de cette logique.

515. Les biens communs désignent originellement des qualités sociétales ou des qualités d'une ressource, d'un patrimoine collectif, nécessaires pour la vie en société et les activités humaines. La surveillance diffuse se fonde sur l'usage des technologies de la communication et de l'information fonctionnant sur les données. Cet usage est présenté, par un ensemble d'acteurs privés et publics, comme nécessaire à la vie en société. Remplir sa déclaration d'impôt, prévention des risques et des menaces, usage d'Internet quotidien sont autant d'éléments présentés comme essentiel aujourd'hui à l'utilité collective, à l'intérêt général. L'ambition d'être tous connectés, et son corolaire le droit à la déconnexion, représentent le parfait aboutissement de cet intérêt général. Nous devons aujourd'hui tous avoir accès aux technologies partout et en tout temps. Nous devons également pouvoir en tirer des bénéfices: culture, connaissance, rentabilité, sécurité.

516. Par référence au premier temps de cette analyse, cet intérêt général est co-produit par les leaders du numérique et la puissance publique. Les individus sont dans cette vision co-producteurs, consommateurs, et fournisseurs de la principale ressource: la donnée, l'information. On comprend également pourquoi la régulation et la gouvernance communautarisée de ces données, de ces informations se sont aussi bien développées, en lieu et place du droit des données personnelles et de la protection de la vie privée. Le règlement général de protection des données personnelles et la proposition de règlement sur la libre circulation des données non personnelles représentent un accord entre la puissance publique et les entreprises sur les conditions d'accès et de circulation de

¹¹⁴⁹ Voir: BOYLE James, *The Public Domain - Enclosing the commons of the Mind*, Yale University Press, New Haven & London, 2008, En ligne: <http://thepublicdomain.org/thepublicdomain1.pdf> (dernière consultation: 5 mars 2018)

cette ressource, ainsi que de sa préservation. Le renforcement de l'obligation de sécurité se situe dans cette logique de préservation de la ressource informationnelle, de la donnée.

Paragraphe 2: L'appropriation des données: un droit chimérique ou une réalité en construction possible au vu de la surveillance diffuse ?

517. Bien que la conception patrimoniale des données n'ait pas été retenue par les institutions nationales ou européennes, cette option aurait pu présenter des intérêts non négligeables pour appréhender autrement le droit des données et envisager de sortir d'une exploitation abusive des données que les nouveaux instruments européens permettent. Au vu des transformations subies par le droit à la vie privée et par le droit des données personnelles, mais également du rapprochement possible des données au concept juridique d'informations, la patrimonialisation des données aurait en effet le mérite de présenter un socle commun de protection par des mécanismes connus. Puisque la liberté qu'est la vie privée semble progressivement disparaître au profit des logiques marchandes et sécuritaires, le droit de propriété appliqué aux données permettrait ainsi que le notait Catala de conférer aux individus un droit réel sur leurs données afin de « *tenir en échec le droit d'autrui à l'information*¹¹⁵⁰ ».

518. En fonction de l'approche choisie entre le rattachement de la donnée à la catégorie des biens susceptibles d'engendrer des contrats (A), et la catégorie des biens communs (B) le droit de propriété peut trouver pleinement ou non application. Dans le premier cas des mécanismes civilistes tels que le droit des contrats et le droit de la consommation peuvent venir en renfort pour appréhender les droits des différents intervenants sur les données. Dans le second cas, il s'agit plutôt de repenser le droit de propriété applicable à ces données autour de leurs usages. Les notions traditionnelles de la protection des données personnelles (consentement et information) peuvent être au coeur de cette logique de patrimonialisation, auxquelles pourraient s'ajouter des éléments du droit civil ou encore du droit pénal, du droit de la consommation, voire même du droit public.

¹¹⁵⁰ Op. Cit.

A. L'appropriation des données par application des mécanismes civilistes du droit des contrats

519. Paradoxalement, les nouveaux instruments européens donnent plusieurs indications sur l'application d'un droit de propriété sur les données personnelles ou non personnelles (1). Les mécanismes civilistes existants permettent alors d'envisager l'organisation d'une protection supplémentaire au titre de ces mécanismes civilistes (2)

1. Des éléments de réponses contenus dans les nouveaux instruments européens

520. En 2013, Jacques Attali écrivait que « *le droit doit être révisé : il faut que les données personnelles soient protégées directement par la loi. Non pas seulement au nom de la protection de la vie privée, mais comme une propriété commerciale. Plus généralement, chacun doit être considéré comme propriétaire de sa vie et de ce qu'il fait; aucune de nos productions ne doit pouvoir être utilisée ou commercialisée par d'autres, sans notre accord pour le donner dans un acte altruiste, ou pour le vendre. Chaque vie est une œuvre; elle est même la plus belle œuvre d'art que toute personne, tout artiste puisse créer. Et chacun doit être considéré comme le légitime propriétaire de cette œuvre-là. On ne parviendra pas à instaurer un tel droit de propriété par la raison, ou par le bon sens. Cela ne viendra que si d'assez nombreux utilisateurs d'internet se coalisent pour négocier ensemble avec les réseaux sociaux, pour reprendre la propriété d'eux-mêmes. Le monde en serait transformé¹¹⁵¹ ».*

521. Le droit a été révisé, et les données personnelles sont protégées aujourd'hui indirectement par la loi au titre de la vie privée. Cette dernière s'effrite au profit des logiques marchandes et sécuritaires prônées par la surveillance diffuse. Il faut effectivement repenser la protection de la vie privée, au titre non pas d'une propriété commerciale, mais d'un droit de propriété reconnu par le droit civil. Les individus doivent en effet être reconnus comme les légitimes propriétaires de leurs données. Sans l'individu, pas de données, ni d'analyse de comportements. La personnalité des données appartient à celui qui les concède. Au regard des mécanismes envisagés par le règlement général de protection des données et la proposition de règlement sur la libre circulation des données non personnelles, l'application de la logique patrimoniale issue du droit des contrats n'est pas si

¹¹⁵¹ ATTALI Jacques, *Etre propriétaire de soi*, 18 Février 2013, L'express, En ligne: <http://blogs.lexpress.fr/attali/2013/02/18/etre-propretaire-de-soi/> (dernière consultation: 5 mars 2018)

insensée. Au-delà des références que ces textes opèrent à la protection de la vie privée, tout se passe comme si les données personnelles étaient soumises aux mécanismes civils du contrat de prêt à usage. Défini à l'article 1875 du Code Civil, « *le prêt à usage est un contrat par lequel l'une des parties livre une chose à l'autre pour s'en servir, à la charge par le preneur de la rendre après s'en être servi* ». Dans le cadre de la consommation de technologies ou de services technologiques, à visée commerciale ou sécuritaire, l'individu livre, à travers son consentement, ses données à l'entreprise ou l'Etat pour que ces entités s'en servent. Le règlement général de protection des données personnelles reconnaît bien des prérogatives de droit réel sur ces données. Ainsi que Catala le mentionnait dans son ébauche d'une théorie juridique de l'information, la législation informatique et libertés reconnaît aux individus des prérogatives telles que « *les droits d'accès et de rectification en particulier. La même loi ouvre aux personnes la faculté de s'opposer, pour des raisons légitimes, à leur inclusion dans un fichier nominatif*¹¹⁵² ». Le règlement général de protection des données personnelles en permettant la limitation de la durée de conservation des données (terme), l'effacement, la portabilité s'insère dans la logique du commodat où le preneur doit rendre la chose au bout d'un certain terme défini par les parties¹¹⁵³. Catala ajoutait également que la législation permet aux individus « *d'exiger des renseignements de celui qui recueille l'information: intéressante innovation, empruntée aux procédés de défense du consommateur, mais qui protège ici le fournisseur. Ce sont là des prérogatives du droit réel. Elle consacrent implicitement l'appartenance de la donnée nominative à la personne concernée, légitime titulaire qui peut, en cette qualité, vérifier leur bon usage et leur véracité, sous certaines contraintes et limites que le législateur a édictées pour des motifs d'intérêt général. Il nous paraît donc que la protection accordée aux individus par la loi sur l'informatique et les libertés reflète un droit sur l'information personnalisée plutôt qu'un droit à cette information* ».

522. Le règlement général de protection des données personnelles s'inspire également de la

¹¹⁵² CATALA Pierre, Op. Cit. p. 239

¹¹⁵³ Bien que les données personnelles ne soient pas à proprement rendues dans le cadre de l'effacement.

protection des consommateurs. Le considérant 42 du règlement général¹¹⁵⁴ évoquant la forme du consentement opère par renvoi à la Directive du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs¹¹⁵⁵. Cet élément peut également donner une autre indication de lecture quant à l'application du droit des contrats aux droits des données personnelles. En effet, cette indication laisse à penser que le législateur cherche à éviter de placer le consommateur de technologies dans une logique contractuelle d'adhésion. Il faut alors s'intéresser ici aux mécanismes des contrats de gré à gré, et c'est dans cette analyse que la problématique de la reconnaissance d'un droit de propriété sur les données au titre du droit civil pose le plus de problèmes.

2. Les moyens possibles d'une organisation civiliste de la patrimonialisation des données

523. Ainsi que Valérie Peugeot s'efforce à le démontrer, il faut dans le cadre des contrats de gré à gré « *sortir des injonctions contradictoires*¹¹⁵⁶ ». Selon l'auteure, la reconnaissance d'un droit de propriété applicable aux données personnelles représente une impasse à plusieurs titres. L'auteure note ainsi « *un problème de conception politique en renvoyant sur l'individu la responsabilité de gérer et protéger ses données* », qui déboucherait sur un « *renforcement des inégalités entre citoyens numériques, entre ceux en capacité de gérer leurs données, de les protéger, les monétiser,*

¹¹⁵⁴ Ce considérant déclare : « *Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement. En particulier, dans le cadre d'une déclaration écrite relative à une autre question, des garanties devraient exister afin de garantir que la personne concernée est consciente du consentement donné et de sa portée. Conformément à la directive 93/13/CEE du Conseil (1), une déclaration de consentement rédigée préalablement par le responsable du traitement devrait être fournie sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples, et elle ne devrait contenir aucune clause abusive. Pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel. Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* ». Considérant 42 du RGPD, P. 8

¹¹⁵⁵ Directive 93/13/CEE du Conseil concernant les clauses abusives dans les contrats conclus avec les consommateurs, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31993L0013&from=FR> (dernière consultation: 5 mars 2018). Au vu du considérant 42, ce renvoi est opéré par rapport à l'article 3 de cette directive qui déclare: « *1. Une clause d'un contrat n'ayant pas fait l'objet d'une négociation individuelle est considérée comme abusive lorsque, en dépit de l'exigence de bonne foi, elle crée au détriment du consommateur un déséquilibre significatif entre les droits et obligations des parties découlant du contrat. 2. Une clause est toujours considérée comme n'ayant pas fait l'objet d'une négociation individuelle lorsqu'elle a été rédigée préalablement et que le consommateur n'a, de ce fait, pas pu avoir d'influence sur son contenu, notamment dans le cadre d'un contrat d'adhésion. Le fait que certains éléments d'une clause ou qu'une clause isolée aient fait l'objet d'une négociation individuelle n'exclut pas l'application du présent article au reste d'un contrat si l'appréciation globale permet de conclure qu'il s'agit malgré tout d'un contrat d'adhésion. Si le professionnel prétend qu'une clause standardisée a fait l'objet d'une négociation individuelle, la charge de la preuve lui incombe. 3. L'annexe contient une liste indicative et non exhaustive de clauses qui peuvent être déclarées abusives* ».

¹¹⁵⁶ PEUGEOT Valérie, *Données personnelles: sortir des injonctions contradictoires*, 13 avril 2014, En ligne: <https://vecam.org/Donnees-personnelles-sortir-des-injonctions-contradictoires> (dernière consultation: 5 mars 2018)

*et ceux qui par manque de littératie, de temps, ou toute autre raison, laisserait faire par défaut le marché*¹¹⁵⁷ ». Ces deux impasses révèlent un même problème: l'apparition d'une vie privée négociée à double vitesse. Or, l'étude du règlement général et de la proposition de règlement démontre que nous sommes, sans même reconnaître un droit de propriété, déjà dans cette situation.

524. Il faut également noter que tous les contrats de droit civil n'ont pas forcément pour contrepartie une valeur monétaire. Dans l'économie de la donnée élaborée par ces deux textes, la reconnaissance d'un droit de propriété à l'individu sur ses données a le mérite de le mettre en face de ses choix. Soit il se place dans une logique performative prônée par l'économie de l'attention, et dans ce cas, il accepte que ses données soient traitées, anonymisées, et ensuite analysée pour un bénéfice de bien être et de sécurité. Soit il ne l'accepte pas. On retrouve ici ce que Pierre Catala entendait par le droit de dire non, le droit à ne pas divulguer ses informations. Valérie Peugeot poursuit son analyse en dénonçant le passage possible « *en régime de propriété intellectuelle*¹¹⁵⁸ » qui supposerait « *que le droit exclusif de l'individu sur ses données soit temporaire*¹¹⁵⁹ ». L'application de la propriété intellectuelle au droit d'auteur pose également le problème de l'apparition d'intermédiaires économiques, tels que la SACEM pour le droit d'auteur¹¹⁶⁰. Bien que l'on puisse partager l'approche de Valérie Peugeot, il ne faut pas réduire l'approche patrimoniale à la contrepartie monétaire des données.

525. Rappelons à nouveau que le premier droit qui découlerait de la logique patrimoniale réside dans le droit de ne pas divulguer ses données. De plus, l'application d'une logique contractuelle, se rapprochant à une sorte de prêt à usage, permettrait d'appliquer à la fois les sanctions du droit civil des contrats (responsabilité civile), du droit pénal, mais également des sanctions extra-contractuelles. Ainsi que le note Pierre Catala, bien que la responsabilité classique de l'article 1382 du Code Civil est assez complexe à mettre en oeuvre du fait des conditions de son application (faute, préjudice, lien de causalité), « *la patrimonialité de l'information nous paraît engagée dans un processus irréversible. Sa réalisation par contrat ne fait aucun doute inter partes. Inversement son opposabilité absolue semblait, naguère encore, une pure chimère, en dehors des cas où le bien-information bénéficiait des monopoles attachés aux propriétés intellectuelles. (...). Qu'on dénomme*

¹¹⁵⁷ Ibid.

¹¹⁵⁸ Ibid.

¹¹⁵⁹ Ibid.

¹¹⁶⁰ Ainsi que le note Valérie Peugeot, « *68 % des sociétaires de la SACEM ne reçoivent aucune rémunération* ».

ou non « propriété » ce nouveau droit en quête d'opposabilité, qu'on appelle ou non « régime primaire » le dispositif qui tend à le réaliser, peu importe au fond, encore que les mots aient une force propre qui opère sur le destin des institutions. Ce qui est captivant pour le juriste est de voir se former, chrysalide encore mais déjà vivant, un nouveau bien consacré aujourd'hui par l'économie et qui portera demain les couleurs du droit¹¹⁶¹ ».

526. La patrimonialité des données doit trouver les moyens de son organisation. La logique contractuelle présente de nombreux intérêts, encore faut-il ne pas vouloir réduire les données personnelles ou leur libre circulation à une simple valeur monétaire.

B. L'impossible appropriation des données entendues comme des biens communs

527. Nous sommes aujourd'hui pleinement entrés dans une économie de la donnée fondée à la fois sur l'attention et la prévention. Une régulation du marché des données peut être envisagée sous couvert des biens communs. Considérer les données comme une ressource collective n'est pas insensé. Cette conception permettrait d'éviter l'application des règles du marché économique édictées par les acteurs privés, mais également d'éviter l'application des règles des biens gérés par la puissance publique. Elle permettrait également d'appréhender d'une manière plus cohérente la vie privée

528. Un amendement, finalement rejeté, à la loi pour la république numérique présente à la fois l'intérêt de comprendre les enjeux de la surveillance diffuse, et le mérite de soulever ces interrogations. Présenté par Delphine Batho et Laurent Grandguillaume, cet amendement était ainsi formulé: « Article 26 - L'alinéa 2 est complété par la phrase suivante :« Les données à caractère personnel, lorsqu'elles forment un réseau indivisible de données liées qui concernent plusieurs personnes physiques, constituent un bien commun qui n'appartient à personne et dont l'usage est commun à tous, dont la protection et l'utilisation sont régies par la présente loi¹¹⁶² ». Notons également, l'exposé sommaire à cet amendement: « La loi informatique et libertés de 1978, dans sa rédaction actuelle, ne considère que les données personnelles solitaires, qui renseignent directement ou indirectement sur une personne. Dans les faits, les données sont aujourd'hui

¹¹⁶¹ CATALA Pierre, Op. Cit., p. 261 - 262

¹¹⁶² BATHO Delphine, GRANDGUILLAUME Laurent, Amendement à l'article 26 de la loi pour une république numérique n°3318), Non soutenu, n°CL125, 6 janvier 2016. En ligne: http://www.assemblee-nationale.fr/14/amendements/3318/CLION_LOIS/CL125.pdf (dernière consultation: 5 mars 2018)

totalemment interconnectées, formant un réseau de données indivisible. Il convient d'adapter le cadre juridique à cette réalité en s'inspirant de l'article 714 du code civil afin d'assurer une protection collective des données en les considérant comme un bien commun ».

529. L'application du régime de l'article 714 du Code civil¹¹⁶³ ne doit pas être compris ici comme étant applicable à chaque donnée personnelle, mais bien au « *réseau de données indivisibles* » que la surveillance diffuse a créée et que les nouveaux instruments européens contribuent largement à légitimer. Si l'application de la propriété privée aux données personnelles paraît délicate, l'application aux données personnelles du statut de bien commun permet de dépasser cette logique. Ainsi que le notait Silvère Mercier « *Ni privé, ni public comment penser des données personnelles en biens communs? Car c'est une piste peu étudiée : celle de faire de ces fameuses données personnelles des biens communs, quelque chose qui appartient à tous et à personne. Ne pas les sanctuariser par la loi, ni les commercialiser sans vergogne mais bien de repenser autour de leurs usages un faisceau de droits*¹¹⁶⁴ ». Cette solution située au-delà de la propriété publique et de la propriété privée permettrait de comprendre la valeur sociale de l'utilité publique du traitement des données. Les traitements de données se développent aujourd'hui dans un paradigme sécurité / marché qui semble impossible à contrer. En terme de protection de la vie privée ce paradigme est dangereux. Mais, ainsi que le rappelait Fabienne Orsi, Judith Rochfeld et Marie Cornu, « *l'utilité publique se situe donc au point de basculement lorsque la valeur « négative » pour un individu devient potentiellement « positive » au regard de l'intérêt général*¹¹⁶⁵ ». Si la dynamique marchande pose problème pour certains, elle est pour d'autres une possibilité d'attention, de compréhension de soi, de réassurance. Peu d'individus voient une dimension négative du traitement des données en vue d'assurer la sécurité¹¹⁶⁶. Dire que nous vivons aujourd'hui dans une culture de la surveillance diffuse c'est d'abord prendre acte de ces positions sociales, c'est aussi faire appel aux forces imaginantes du Droit. Si la surveillance diffuse aujourd'hui est présentée comme d'utilité publique, il y a tout intérêt à voir dans la protection des données personnelles un bien commun qu'il faudrait ériger en intérêt général.

¹¹⁶³ Article 714 du Code Civil: « *Il est des choses qui n'appartiennent à personne et dont l'usage est commun à tous. Des lois de police règlent la manière d'en jouir* ».

¹¹⁶⁴ MERCIER Silvère, *Biens communs et données personnelles: il nous faut inventer* », 12 mars 2014, Disponible en ligne à l'adresse suivante: <http://www.bibliobsession.net/2014/03/12/biens-communs-et-donnees-personnelles-il-nous-faut-inventer/> (dernière consultation: 5 mars 2018)

¹¹⁶⁵ Op. Cit.

¹¹⁶⁶ On s'intéressera par la suite au mythe du je n'ai rien à cacher, rien à me reprocher

530. Si les mouvements actuels d'Open Data, et d'utilisation des logiciels libres prônant le partage d'informations semblent pleinement s'inscrire dans cette logique des biens communs, comment les données personnelles pourraient entrer dans cette catégorie ? Le faisceau de droits décrit par Silvère Mercier, inspiré par Valérie Peugeot, peut ici trouver application. Ce concept est analysé par le mouvement du réalisme juridique¹¹⁶⁷, prônant effectivité du droit et interprétation empirique de ce dernier. Il vise à concevoir la propriété non plus comme relevant « *d'un droit naturel ni d'un droit absolu d'une personne sur une chose mais de relations sociales entre les personnes. La propriété étant un faisceau de droits socialement construit et soumis aux rapports sociaux, elle se décompose et se recompose en fonction des forces sociales en présence. C'est ainsi que, selon certains auteurs, ce changement de perspective pour penser la propriété s'identifie à un programme de « détronement » de la propriété ayant ainsi ouvert la voie à l'État interventionniste¹¹⁶⁸ »*. Et si nous pouvions envisager le droit des données comme un faisceau de droits ? Dans cette vision, certains droits pourraient être garanti à l'individu: consentement aux usages, rectification, suppression et portabilité. D'autres droits pourraient être garantis aux entreprises et aux Etats : collecte de données pour la gestion d'un service. Dans un autre article, Valérie Peugeot énonce la possibilité de clarifier les rôles de chacun des participants aux traitements de données. Elle énonce ainsi que: « *les usages intermédiaires (...) peuvent quant à eux faire l'objet d'un usage par l'entreprise sous deux régimes possibles: une ouverture de la donnée individuelle à un tiers sur base d'une autorisation explicite de la part de l'individu coproducteur, en échange d'un service : j'autorise une marque d'électroménager à accéder à mes données pour me proposer une machine à laver qui correspond à mes besoins, dans une approche dite VRM – Vendor relationship management. (...). Une ouverture de la donnée agrégée et anonymisée à des tiers sous condition de partage limité dans le temps. Sur une très courte période, quand la donnée est « chaude », la plateforme aurait le droit de monétiser celle-ci agrégée à d'autres, mais à l'expiration de cette période, la donnée ne pourrait plus être mobilisée directement ou indirectement par la plateforme productrice. La donnée devrait alors soit être détruite (pas de possibilité de stockage) soit être*

¹¹⁶⁷ Voir: BRUNET Pierre, *Le réalisme n'est-il qu'une théorie de l'interprétation? Réalisme, interprétation, transgression*, 2012, France. Larcier, pp.397-414, 2013, En Ligne: <https://halshs.archives-ouvertes.fr/halshs-00840601/document> (dernière consultation: 5 mars 2018), Voir également JAMIN Christophe, *Le rendez-vous manqué des civilistes français avec le réalisme juridique : un exercice de lecture comparée*, Article Disponible en ligne à l'adresse suivante: <https://spire.sciencespo.fr/hdl:/2441/6ggbvnr6munghes9oc0gmel16/resources/jamin-realisme-juridique.pdf> (dernière consultation: 5 mars 2018)

¹¹⁶⁸ ORSI Fabienne, « Elinor Ostrom et les faisceaux de droits : l'ouverture d'un nouvel espace pour penser la propriété commune », *Revue de la régulation*, 14 | 2e semestre / Autumn 2013, Disponible en ligne à l'adresse suivante: <http://journals.openedition.org/regulation/10471> (dernière consultation: 5 mars 2018)

transférée vers un espace de type cloud personnel où l'individu pourrait la conserver s'il la juge utile, voire la partager s'il le souhaite¹¹⁶⁹ ».

531. Eluder l'application d'une propriété privée et l'application d'une propriété publique, penser une théorie de l'usage partagé des données, une coopération et une dépendance réciproque entre les acteurs, responsabiliser réellement les acteurs du traitement en reconnaissant une place à chacun d'entre eux sont autant de pistes de réflexions que les données - biens communs permettraient de construire, d'envisager, d'élaborer. Cette approche a le mérite de rendre au droit une certaine efficacité, une logique basée sur la réalité des faits sociaux.

¹¹⁶⁹ PEUGEOT Valérie, *Données personnelles: sortir des injonctions contradictoire*, Op. Cit.

Conclusion du Titre

532. L'absence de compréhension de la culture de la surveillance diffuse a engendré le règlement général de protection des données personnelles. Ce texte est incompréhensible à plusieurs titres. Dans sa volonté de contenter les acteurs du marché, et de promouvoir une économie de la donnée, il désinstitue pleinement le droit des données personnelles. La protection de l'individu s'organise non plus autour de mécanismes d'autorisation et de déclaration auprès des autorités de protection, mais bien *a priori* par les entreprises et les entités publiques. Ces acteurs de la surveillance diffuse se retrouvent en charge de la protection de la vie privée, de la vente de leurs services et applications, et de la promotion de la sécurité fondée sur les données. Couplée à la proposition de règlement sur la libre circulation des données non personnelles, les nouveaux instruments européens permettent le passage progressif de la vision d'une vie privée réduite à un argument marketing, à sa véritable marchandisation.

533. Alors que certains juristes tels que Mireille Delmas-Marty en appelle aux « *forces imaginantes du Droit*¹¹⁷⁰ » pour contrer la vague de la mondialisation, on ne peut qu'être surpris de la pauvreté du raisonnement de ces instruments européens censés garantir les droits et libertés fondamentales des individus. Face au phénomène de surveillance diffuse, il faut ainsi que le rappelle Mireille Delmas-Marty, « *se donner les moyens d'élargir le raisonnement juridique, du concept au processus, du statique au dynamique, du modèle au mouvement*¹¹⁷¹ ». L'élargissement du raisonnement juridique passe alors nécessairement par la question du statut juridique des données personnelles. Alors que les textes européens ne sont pas clairs sur ce point, il faut à travers la libre circulation légitimée des données (personnelles et non personnelles) entre-apercevoir la notion d'information, permettant d'appliquer aux données la catégorie juridique des biens. Ces réflexions permettent alors d'envisager la question de l'appropriation des données, question centrale que pose déjà la surveillance diffuse.

534. Les mécanismes civilistes du droit des contrats, de la responsabilité contractuelle et extra-contractuelle représentent une grille d'analyse nécessaire. Ils sont toutefois inefficaces pour redonner au droit des données et au droit à la vie privée, une cohérence qu'ils ont perdu au fur et à

¹¹⁷⁰ DELMAS - MARTY Mireille, *Aux quatre vents du monde -Petit guide de navigation sur l'océan de la mondialisation*, Op. Cit., p. 15.

¹¹⁷¹ Ibid. p. 19

mesure des textes juridiques souhaitant encadrer à la fois un marché, une technologie, une liberté. L'application de l'article 714 du Code Civil reconnaissant l'existence des biens communs présente quant à lui une garantie d'efficacité quant à la lecture de la surveillance diffuse par le droit. La surveillance diffuse est fondée sur une économie capitaliste de l'information, sur la consommation technologique et le brouillage de l'ensemble des notions du droit des données personnelles et de la vie privée. L'absence d'appropriation des biens communs représente un intérêt et une finalité pour un futur encadrement des données. Cette théorie permet également de repenser le rôle et la fonction de chacun des intervenants au traitement, et de les responsabiliser réellement.

535. Ainsi que le rappelle Antonio Casili, la bonne compréhension de l'enjeu social dans lequel évolue ces données est crucial pour conférer une nouvelle force au droit à la vie privée: *« somme toute, ce dévoilement différentiel des informations personnelles n'est nullement un processus monotone, conduisant inévitablement d'un état de plus forte protection de la vie privée à une nouvelle condition de « publitude » généralisée. (...). Autrement dit, les choix des usagers tiennent compte du caractère intrinsèquement plus ou moins appréciable de l'information partagée, ainsi que de la structure et composition de leurs réseaux personnels en ligne, dans chaque type d'interaction. (...). Dans la mesure où les données ne sont pas sensibles par leur nature, mais selon leur pertinence par rapport à un milieu social de choix, le respect de la vie privée revient principalement à vérifier l'adaptation entre l'information dévoilée, l'intention stratégique de son locuteur et le contexte de son dévoilement (à savoir la forme, structure et taille du réseau de contacts avec lesquels elles sont partagées)¹¹⁷² ».*

¹¹⁷² CASILLI Antonio, « Contre l'hypothèse de la « fin de la vie privée » - la négociation de la privacy dans les médias sociaux » *Revue française des sciences de l'information et de la communication*, Disponible en ligne à l'adresse suivante: <http://journals.openedition.org/rfsic/630> (dernière consultation: 5 mars 2018)

Titre 2: La désinstitution du Droit au profit de la nouvelle norme admise: la surveillance diffuse

536. La surveillance diffuse est devenue aujourd'hui une nouvelle norme sociale. Le mot norme évoque la norma, l'équerre de l'architecte. La norme ou la règle¹¹⁷³ se dit d'un modèle de représentation et d'action, ou encore d'une attente standardisée de comportement. Toute régularité comportementale¹¹⁷⁴ ne témoigne pas de l'obéissance à une norme: elle peut seulement traduire d'une forme de routine. Le normatif se compose alors de façons de penser ou d'agir, définies socialement, prescrites et sanctionnables. Toutefois, pour des auteurs tels que Bourdieu, la norme sera plus efficace et mieux intégrée si elle est pleinement intériorisée. La sanction des conduites non conformes passe alors par un jeu de pouvoir et d'inégalité, une sorte de nouvelle domination permettant d'imposer un nouvel ordre social, prescrit et défini par elle-même.

537. A la lecture de cette définition, on voit toute la potentialité négative de la surveillance diffuse: attente de comportement, obéissance, déviance, prescription de règles de conduite, intériorisation de la règle, nouvelle domination. L'ensemble de ces mots doit être analysé de manière consciencieuse. Le Droit a, en principe, le monopole de l'édition des règles de comportements en société. Ce dernier est progressivement désinstitutionné par l'action de la surveillance diffuse. En ce qu'elle a permis une transformation des espaces sociaux, par l'éclatement de la dichotomie publique -privé, tout se passe aujourd'hui comme si le Droit n'avait plus forcément d'espace d'application. Visant à assurer une fluidité de l'économie de marché cette disparition des espaces sociaux influence de manière claire et dangereuse le Droit, la fonction du Droit. La surveillance diffuse doit également être analysée comme une norme en ce qu'elle réduit la société civile à une logique de calcul d'utilité. Elle est en cela fortement influencée par le libéralisme économique, culturelle et politique.

538. Le Droit s'en retrouve modifié. On constate ainsi une hybridation du Droit et de l'Etat de Droit par le libéralisme prôné par la surveillance diffuse (chapitre 1). La surveillance diffuse porte en elle, une attention bienveillante qui modifie également le contrôle social. Puisque la surveillance

¹¹⁷³ Bien que la règle juridique fasse partie des normes sociales, il a toujours été délicat d'appréhender ces notions pour le juriste. Les études de droit sont enseignées de telles manières à être allergique à la norme, à la religion, à la philosophie.

¹¹⁷⁴ Se lever le matin pour aller travailler.

diffuse engendre également diffusion de dispositifs de contrôle et de captation d'attention, il apparaît clairement qu'il faille s'interroger sur les liens qu'entretiennent la surveillance diffuse et le contrôle social, mutés en attention. L'enjeu n'est pas ici de savoir si nos sociétés contemporaines sont soumises à plus ou moins de contrôle social. Il s'agit plutôt de comprendre cette métamorphose pour éclairer l'ensemble des transformations sociales et juridiques à l'oeuvre (Chapitre 2). De l'analyse de ces deux transformations portées par la surveillance diffuse, il faudra alors s'interroger sur la réelle désinstitution du Droit.

Chapitre 1: La surveillance diffuse: entre désinstitution de la fonction du droit et mutation du Droit par la nouvelle norme admise

539. La désinstitution de la fonction droit et sa mutation sont deux phénomènes engendrés par la surveillance diffuse. Mettre en relation ces deux éléments et prendre acte de la nouvelle norme qu'est devenue la surveillance diffuse, c'est tenter de comprendre ce qu'elle est vraiment. L'analyse a jusqu'alors permis d'appréhender la surveillance diffuse comme s'inscrivant dans la continuité d'un projet de société: la société de l'information et de la communication. Développée par un certain nombre d'acteurs, allant du secteur privé au secteur public, en passant par les individus, la surveillance diffuse est parvenue à s'intégrer culturellement dans nos sociétés. Au-delà des conséquences qu'elle engendre en termes de protection des données personnelles au vu de l'évolution juridique de cette notion, il faut comprendre le jeu qu'elle entretient avec le pouvoir, la souveraineté et le Droit, en tant qu'édiction de règles permettant la vie en société. C'est dans ce jeu entre le pouvoir, la souveraineté et le Droit, que la surveillance diffuse devient la nouvelle norme sociale admise..

540. La surveillance diffuse doit alors être analysée comme une nouvelle norme sociale. Elle est à la fois un outil d'influence sur la circulation et la fonction du Droit (section 1), et devient une norme par une rhétorique de l'utilitarisme libéral. Cette rhétorique de l'utilitarisme propre à la surveillance diffuse, influence progressivement le Droit, le faisant prendre en compte les idéaux du libéralisme (section 2).

Section 1: L'influence de la surveillance diffuse sur la circulation et la fonction du droit

541. La surveillance diffuse, en tant que nouvelle norme sociale, entretient des liens avec les notions de pouvoir, de souveraineté et d'économie. En ce qu'elle repose sur une double forme, banale et imposée, la surveillance diffuse tire son pouvoir de son utilité économique, culturelle et sociale (paragraphe 1). En cela, elle influence la circulation et la fonction du droit dans une transformation radicale des espaces sociaux (paragraphe 2). Tout se passe aujourd'hui comme si le Droit circulait dans un espace sans fonction. L'éclatement de la dichotomie publique privé doit être sondée ici, afin de comprendre la circulation et la fonction d'un droit qui n'aurait plus pour ambition d'édicter des règles de conduite dans un espace donné.

Paragraphe 1: La surveillance diffuse: un outil privilégié de l'utilitarisme des sociétés libérales contemporaines

542. Evoquer la conception utilitariste du pouvoir et du droit au regard de la surveillance diffuse, c'est d'abord opérer un questionnement simple: quelle est donc l'utilité d'une surveillance telle que décrite dans ces pages, dans une société prônant régulation du marché et bien-être économique ? (A). C'est également sonder les concepts de biopouvoir et de biopouvoir algorithmique comme transformation des modalités d'exercice du pouvoir et du Droit (B)

A. L'utilité de la surveillance diffuse

543. La surveillance diffuse est aujourd'hui devenue un outil du libéralisme économique, culturelle et politique (1), elle en est même le principal outil (2).

1. La surveillance diffuse et le libéralisme économique

544. La surveillance diffuse, par la multiplication des technologies capables de capter de l'information, par le croisement de ces informations, et par la poursuite du double objectif de préserver la sécurité et le marché économique (des données, du numérique) s'inscrit alors dans cette recherche de maximisation des profits, du bonheur. La société contemporaine est dominée par un discours d'apologie des technologies. Ces dernières rassurent, préservent, protègent, et portent en elles la possibilité de réalisation d'une société quasi-utopique, ou du moins quasi-idéale. Santé, sécurité, rationalité, efficacité sont autant de qualificatifs employés à son égard par les thuriféraires de la surveillance diffuse qu'ils soient du secteur privé, du secteur public, ou encore de simples individus.

545. Alors que la surveillance diffuse se développe grâce et pour une double rationalité - économique et marketing d'une part, sécuritaire d'autre part - l'utilité de sa prolifération, et de son pendant le « data-panoptisme », la mise en données du monde, doit être interrogée. En quoi le principe de visibilité régénéré par la surveillance diffuse est utile à des sociétés qui prônent un libéralisme économique, un libre échange des flux, des personnes ? En 2002, Christian Laval écrivait en postface de l'édition des Mille et une nuits du Panoptique de Bentham, « *comment des sociétés qui aiment se représenter comme d'immenses marchés qui relient tous les points du globe*

sont-elles également des sociétés obsédées de sécurité qui poussent à l'emprisonnement et généralisent la surveillance? Comment le libéralisme triomphant qui rêve d'une société réduite au marché se double-t-il d'un panoptisme généralisé?¹¹⁷⁵ ».

546. Une partie essentielle de la réponse à ces questions réside dans la conception utilitariste du système juridique et politique que prône Jérémy Bentham et qui influe le Panoptique. L'utilitarisme est « *une doctrine ou une attitude morale qui considère que « l'utile ou ce qui peut apporter le plus grand bonheur » doit être le principe suprême de notre action. L'utilitarisme fut soutenu par Bentham qui préconisait une « arithmétique des plaisirs » destinée à comparer méthodiquement la valeur des plaisirs et à augmenter, dans la plus grande proportion, la somme totale du bien être de l'individu, puis par John Stuart Mill et la majorité des penseurs anglo-saxons. Le pragmatisme, qui considère comme « vrai » tout ce qui réussit, perpétue la tradition de l'utilitarisme¹¹⁷⁶ ».* Souvent réduite au dilemme du tramway¹¹⁷⁷, la doctrine utilitariste va beaucoup plus loin qu'une simple éthique de l'utilité, qu'un simple jugement utilitariste. L'utilitarisme correspond bien plus à une logique de maximisation des profits en terme de bonheur pour les individus d'une collectivité. Toute action ou absence d'action doit alors prendre en compte le critère de l'effet bénéfique ou nuisible pour la collectivité des individus. Ainsi que le note Christian Laval pour expliquer l'idée générale qui sous-tend le panoptique, « *selon l'utilitarisme benthamien, l'homme est guidé par la recherche de sa satisfaction personnelle et veut la maximiser toujours et partout. C'est un calculateur qui cherche le maximum de plaisir et le minimum de peine, une petite machine économique qui veut augmenter ses bénéfices et diminuer ses coûts. Sur cette base, c'est toute la société, toutes les institutions, toutes les lois et les normes qui doivent s'adapter à cette donnée: le but de tout l'appareillage institutionnel et l'objectif principal du gouvernement consiste à produire le plus grand bonheur pour le plus grand nombre en réglant et en orientant les conduites afin que les satisfactions des intérêts individuels mènent à la plus grande somme possible de bonheur pour la*

¹¹⁷⁵ BENTHAM Jérémy, *Panoptique*, Mille et une nuits, département de la librairie Arthème Fayard, Septembre 2002, Postface de Christian Laval, *De l'utilité du Panoptique*, p. 46 et suivants, p. 46.

¹¹⁷⁶ « *Il s'oppose au rigorisme moral de Kant, par exemple selon lequel la valeur morale d'une action ne se mesure pas à ses conséquences (à sa réussite), mais à l'intention qui l'anime et au principe sur lequel elle se règle. La tradition de l'utilitarisme remonte à Helvétius, et surtout à Hobbes, elle se recommande de la philosophie d'Epicure dans l'Antiquité* ». JULIA Didier, *Dictionnaire de la philosophie*, Larousse, 1995, p. 293.

¹¹⁷⁷ Pour une relecture contemporaine du dilemme du tramway voir: KAHANE Guy, EVERETT Jim, EARP Brian, FARIAS Miguel, SAVULESCU Julian, *Utilitarian judgments in sacrificial moral dilemmas reflect impartial concern for the greater good*, Cognition, 13 novembre 2014, Disponible en ligne à l'adresse suivante: http://ac.els-cdn.com/S0010027714002054/1-s2.0-S0010027714002054-main.pdf?tid=5e56ce28-5ccd-11e7-9566-00000aacb35e&acdnat=1498742458_c7b59ce690a17e62a9117c5e4c3f8caf (dernière consultation: 5 mars 2018)

*collectivité*¹¹⁷⁸ ».

2. La surveillance diffuse: l'outil principal au service d'un pouvoir utilitariste

547. La surveillance diffuse est aujourd'hui l'outil symbolique d'un pouvoir utilitariste, qui guide, influence et agit sur les conduites individuelles à distance et discrètement, à la fois pour assurer un maximum de sécurité dans les échanges de flux du marché, et un maximum de liberté et de bien-être, dans un intérêt général mis en conformité avec le libéralisme économique¹¹⁷⁹.

548. A l'image de Thomas Hobbes qui qualifiait l'homme de loup pour lui même, Bentham affirme que « *nous sommes tous des délinquants potentiels*¹¹⁸⁰ ». Son idée du panoptique, voire de la démocratie panoptique, permettait ainsi que le rappelle Christian Laval « *d'édifier un système de pouvoir qui laisse les individus libres de faire des choix selon des calculs de maximisation qui leur sont propres, et ce, en conformité avec les principes du libéralisme économique de l'époque, tout en orientant les conduites vers l'intérêt général, ce qui suppose de maintenir constamment à l'œil les « délinquants potentiels »*. Liberté et sécurité sont donc les deux faces de la même pratique politique. (...). On comprend alors l'importance de la surveillance dans ce nouveau pouvoir. Elle est destinée à influencer le calcul des probabilités de l'individu intéressé. Plus nous serons conformes à l'homme économique, plus nous nous croirons libres, mais plus nous devons être surveillés. Tel est le grand message de Bentham. La sécurité est la condition du bonheur général. Le bonheur est le grand but, la surveillance qui conditionne la sécurité est le principal levier pour y parvenir¹¹⁸¹ ».

Ces éléments envisagés pour la société de Bentham semblent avoir trouvé leur pleine application dans la société contemporaine: liberté et sécurité représentent bien les deux faces du pouvoir actuel. Couplé aux analyses de Arendt concernant le philistin cultivé, l'ensemble de l'analyse de Bentham reformulée par Laval prend tout son sens. L'individu devenu homme économique, philistin cultivé numérisé croit en une liberté artificielle créée par le marché: la consommation libre le rend heureux, et le bonheur, le bien-être, tantôt argument marketing, tantôt objectif de politique sociale, est bien

¹¹⁷⁸ LAVAL Christian, « Surveiller et prévenir. la nouvelle société panoptique », *Revue du Mauss* 2012/2 (n°40), p. 47-72, p. 51, En ligne: <https://www.cairn.info/revue-du-mauss-2012-2-page-47.htm#re5no29> (dernière consultation: 5 mars 2018)

¹¹⁷⁹ Cf. Partie 1, et spécialement les analyses développées concernant la banalisation de la surveillance et la gouvernementalité par la peur.

¹¹⁸⁰ Cité par Christian Laval, Ibid. p. 52

¹¹⁸¹ Ibid. p. 52

devenu le « grand but » du pouvoir actuel.

549. Nombre de rapports nationaux ou internationaux consacrent des études au concept de bien-être comme dimension du progrès social, devenant ainsi un indicateur économique de performance des nations. On pourrait citer deux rapports particulièrement éclairants quant aux logiques d'intégration du bien-être comme un axe prioritaire de la performance d'une nation. Le premier est relatif à la stratégie de recherche et d'innovation en matière d'enseignement supérieur et de recherche¹¹⁸². Dans ce rapport, le Ministère fait de « *la santé, le bien être, l'alimentation et les biotechnologies*¹¹⁸³ » un axe prioritaire de la stratégie de la recherche nationale, l'identifiant ainsi comme un enjeu de société, correspondant « *à des domaines économiques émergents et à fort potentiel d'innovation*¹¹⁸⁴ ». Ce rapport identifie le bien être *a contrario* et l'envisage en rapport à des exigences de santé publique¹¹⁸⁵, de la promotion d'une « *alimentation saine et sécurisée (...) qui véhicule d'autres éléments de bien être: respect de l'environnement, aspects organoleptiques, identité culturelle*¹¹⁸⁶ ». Le second de ces rapports est relatif à la mesure des performances économiques et du progrès social¹¹⁸⁷. Le bien-être des citoyens et des populations, ainsi que le bien-être économique, sont envisagés ici comme une dimension du progrès social. Ce concept de bien-être pourrait selon ses promoteurs devenir un élément de mesure au même titre que des outils tels que le PIB ou le PNB, présentant peu d'adéquation avec la société actuelle puisque essentiellement basé sur la notion de production¹¹⁸⁸. Ce rapport vise essentiellement à « *avoir une meilleure vision des indicateurs disponibles ou utiles à construire, afin de concevoir, mettre en oeuvre et évaluer les politiques destinées à accroître le bien-être et à favoriser le progrès social*¹¹⁸⁹ », dans une

¹¹⁸² Ministère de l'enseignement supérieur et de la recherche, *Rapport général sur la stratégie de recherche et d'innovation 2009 - 2012*, 2009, En ligne: http://media.enseignementsup-recherche.gouv.fr/file/SNRI/69/8/Rapport_general_de_la_SNRI_-_version_finale_65698.pdf (dernière consultation: 5 mars 2018)

¹¹⁸³ Ibid. p. 29

¹¹⁸⁴ Ibid. p. 7 et 27

¹¹⁸⁵ Ce rapport déclare clairement que la santé, le bien-être, l'alimentation et les biotechnologies sont un enjeu social majeur. Pour les auteurs: « *la demande croissante de la société vis-à-vis des chercheurs et des professionnels de santé est liée à de nombreux facteurs : allongement de la durée de vie et développement de maladies liées à l'âge, aspiration continue au bien-être, évolution des modes de vie et de consommation, émergence de maladies infectieuses, persistance de pathologies majeures qui touchent une population vieillissant* ». (ibid. p. 29)

¹¹⁸⁶ Ibid. p. 31.

¹¹⁸⁷ STIGLITZ Joseph, SEN Amartya, FITOUSSI Jean-Paul, *Rapport au Président de la République de la Commission sur la mesure des performances économiques et du progrès social*, Ministère de l'économie, de l'industrie et de l'emploi, Septembre 2009, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000427.pdf> (dernière consultation: 5 mars 2018)

¹¹⁸⁸ Ibid. p. 8 - 9

¹¹⁸⁹ Ibid. p. 11.

perspective de soutenabilité¹¹⁹⁰. Un lien fort entre production / consommation et bien-être est mis en avant dans le cadre de la démarche des auteurs. Ces derniers souhaitent déplacer le curseur des indicateurs de bien-être de la production vers la consommation¹¹⁹¹. Afin d'éclairer leurs propos, les auteurs ont recouru à une définition pluridimensionnelle de la notion de bien-être : « *La Commission a répertorié les principales dimensions qu'il convient de prendre en considération. En principe au moins, ces dimensions devraient être appréhendées simultanément: i. les conditions de vie matérielles (revenu, consommation et richesse); ii. la santé; iii. l'éducation; iv. les activités personnelles, dont le travail; v. la participation à la vie politique et la gouvernance; vi. les liens et rapports sociaux ; vii. l'environnement (état présent et à venir); viii. l'insécurité, tant économique que physique. Toutes ces dimensions modèlent le bien-être de chacun; pourtant, bon nombre d'entre elles sont ignorées par les outils traditionnels de mesure des revenus*¹¹⁹² ». On retrouve dans ces lignes l'ensemble des logiques et des glissements que la surveillance diffuse a permis d'opérer dans nos sociétés: de la réglementation à la gouvernance, des logiques de sécurité et de prévention, des notions de risque et de sécurité, de consommation et de sécurité. Ces notions, au coeur de la surveillance diffuse, font aujourd'hui parties de l'élaboration politique du bien-être social.

550. Le concept de bien-être doit donc être entendu comme un nouveau glissement qu'opère la surveillance diffuse: de l'Etat-providence à l'assurance du bien-être des nations¹¹⁹³. Aussi, et à l'image de la notion de sécurité humaine¹¹⁹⁴, il est légitime de s'interroger sur une possible

¹¹⁹⁰ Stiglitz, Sen et Fitoussi écrivent en effet que: « *le rapport établit une distinction entre évaluation du bien-être présent et évaluation de sa soutenabilité, c'est-à-dire de sa capacité à se maintenir dans le temps. Le bien-être présent dépend à la fois des ressources économiques comme les revenus et des caractéristiques non économiques de la vie des gens : ce qu'ils font et ce qu'ils peuvent faire, leur appréciation de leur vie, leur environnement naturel. La soutenabilité de ces niveaux de bien-être dépend de la question de savoir si les stocks de capital qui importent pour notre vie (capital naturel, physique, humain, social) seront ou non transmis aux générations à venir* ». (Ibid. p. 11)

¹¹⁹¹ Ibid. p. 13 et s.

¹¹⁹² Ibid. p. 16 . On citera également les travaux de l'OCDE sur ce point, voir: <http://www.oecd.org/fr/statistiques/mesurer-bien-etre-et-progres.htm> (dernière consultation: 5 mars 2018)

¹¹⁹³ Voir en ce sens: Centre pour la recherche et l'innovation dans l'enseignement, *The Well-Being of Nations: The Role of Human and Social Capital*, Paris, OCDE, 2011.

¹¹⁹⁴ Dont Amartya Sen est le principal promoteur.

émergence d'un droit au bien-être¹¹⁹⁵.

B. La transformation des modalités d'exercice du pouvoir: du biopouvoir de Foucault au biopouvoir algorithmique

551. Le concept de biopouvoir est introduit par Foucault dans sa leçon du 17 mars 1976 consacrée au thème de la défense de la société. Foucault déclare alors que : « *Pendant la seconde moitié du XVIII^{ème} siècle, je crois que l'on voit apparaître quelque chose de nouveau, qui est une autre technologie de pouvoir, non disciplinaire cette fois. [...] Cette nouvelle technique ne supprime pas la technique disciplinaire tout simplement parce qu'elle est d'un autre niveau, elle est à une autre échelle, elle a une autre surface portante, et elle s'aide de tous autres instruments. [...] Après l'anatomo-politique du corps humain, mise en place au cours du XVIII^{ème} siècle, on voit apparaître, à la fin de ce même siècle, quelque chose qui n'est plus une anatomo-politique du corps humain, mais que j'appellerais une « biopolitique » de l'espèce humaine¹¹⁹⁶* ». Cette analyse précise l'étude qu'il a entamé dans *Surveiller et Punir*, et s'inscrit dans son prolongement, tout comme son cours lié au concept des « anormaux¹¹⁹⁷ ». En effet, à l'image de ce que déclare Foucault dans ce dernier cours, « *depuis 1970, la série des cours a porté sur la lente formation d'un savoir et d'un pouvoir de normalisation à partir des procédures juridiques traditionnelles du châtement. Le cours de l'année 1975 - 1976 terminera ce cycle par l'étude des mécanismes par lesquels, depuis la fin du XIX^{ème} siècle, on prétend « défendre la société »¹¹⁹⁸* ».

552. Evoquer la transformation des modalités d'exercice du pouvoir par la surveillance diffuse,

¹¹⁹⁵ Sur l'émergence de la notion de bien-être en droit du travail, voir: CAILLAUD Pascal, « L'action juridique des institutions internationales sur le « travail décent » et la « qualité de l'emploi »: une définition par indicateurs du bien-être du travailleur ? », in. FLORIN Agnès, PREAU Marie, *Le bien-être*, L'Harmattan, 2013, pp. 35 - 59, et, CHAUMETTE Patrick, « La notion de bien-être en droit social. Une notion pleine d'avenir », in. FLORIN Agnès, PREAU Marie, Op. Cit., pp. 193 - 209. Voir également, en matière de développement durable: CHARBONNEAU Alexandre, « La référence au bien-être des gens de mer: entre institutionnalisation d'un service social et approche qualitative des conditions de vie et de travail à bord des navires », in. FLORIN Agnès, PREAU Marie, Op. cit., pp. 117 - 132. L'auteur écrit ainsi « *l'exemple maritime permet de se figurer ce qui pourrait constituer, sur le plan social, le contenu d'un droit du bien-être afin de concrétiser le droit au bien-être, tel qu'il se laisse découvrir dans plusieurs déclarations de droits et constitutions. Sur le plan terrestre, le bien-être inviterait, par exemple, à une réflexion sur la conciliation des temps familiaux et professionnels, à une responsabilisation sociale des employeurs publics et privés qui se concrétiseraient dans les territoires, par le développement de moyens de garde pour les enfants, une mobilité professionnelle plus accompagnée...* » (spécialement p. 132).

¹¹⁹⁶ FOUCAULT Michel, *Il faut défendre la société - Cours au collège de France. 1976*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 1997, p. 215 - 216

¹¹⁹⁷ FOUCAULT Michel, *Les anormaux - Cours au collège de France. 1974-1975*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 1999

¹¹⁹⁸ Ibid. p. 311.

c'est d'abord et avant tout prendre acte d'une modification du biopouvoir de Foucault (1) par une sorte de biopouvoir algorithmique (2).

1. Du Biopouvoir comme technique de pouvoir s'exerçant sur la vie des individus et des populations...

553. L'analyse de Michel Foucault concernant le biopouvoir est particulièrement éclairante des problématiques que traversent la société contemporaine à l'aune de la surveillance diffuse. Là encore les propos de Michel Foucault doivent servir de grille d'analyse utile permettant de décrypter les prémices des liens entre pouvoir, biopouvoir, droit et surveillance diffuse. Ainsi que l'exprimait Foucault, il faut ici s'intéresser à « *la rationalisation de la gestion de l'individu. Mon travail n'a pas pour but une histoire des institutions, mais l'histoire de la rationalité telle qu'elle opère dans les institutions et dans la conduite des gens*¹¹⁹⁹ ». Dans la conception de Foucault, le corps constitue donc la cible privilégiée du pouvoir. Le premier temps d'analyse de la notion de pouvoir par Foucault, se consacre d'abord à l'étude du pouvoir souverain, et à la souveraineté comme dispositif juridique de pouvoir. Ces notions doivent s'entendre au sens décrit par Michel Foucault. Ainsi que le rappelle Bertrand Mazabraud en 2010, « *en ce qui concerne plus spécifiquement la mécanique du droit, l'analytique du pouvoir, qui mobilise la notion de « dispositif », s'avère être un outil précieux. Il ne s'agit pas tant d'interroger « l'épistémè » du discours juridique que d'explicitier le « comment » du droit en rapportant ses discours et ses pratiques aux dispositifs de pouvoir dans lequel il fonctionne. En décentrant le droit de sa production institutionnelle, l'approche foucauldienne désempêtre la doctrine juridique de l'illusion que lui procure son champ disciplinaire : celle d'un caractère « autopoïétique » du droit. Si le droit ne se manifeste invariablement qu'à travers des lois, des contrats et des jugements, le sens de ceux-ci ne s'éclaire que dans leur place stratégique au sein de rapports de forces. Autrement dit, le droit n'est qu'une sorte de signifiant impur se trouvant investi et agencé par des dispositifs de pouvoir*¹²⁰⁰ ». Issue d'un développement historique spécifique et s'appuyant sur des institutions économiques, politiques et individuelles, la surveillance diffuse constitue un dispositif ouvrant des

¹¹⁹⁹ FOUCAULT Michel, « Foucault étudie la raison d'Etat », entretien avec M. Dillon, *The Three Penny Review*, 1ère année, n° 1, hiver printemps 1980, pp. 4. - 5, in. DEFERT Daniel et EWALD François (sous la direction de), *Michel Foucault, Dits et écrits 1954 - 1988, II. 1976 - 1988*, Editions Quarto Gallimard, 2001, texte n° 280, « Foucault étudie la raison d'Etat », pp. 856 - 860, p. 857.

¹²⁰⁰ MAZABRAUD Bertrand, « Foucault, le droit et les dispositifs de pouvoir », *Cités* 2010/2 (n° 42), pp. 127-189, p128 - 129, Disponible en ligne à l'adresse suivante: <https://www.cairn.info/revue-cites-2010-2-page-127.htm> (dernière consultation: 5 mars 2018)

champs de savoir et faisant circuler une nouvelle forme de pouvoir.

554. Pour Foucault, « *par pouvoir, il me semble qu'il faut comprendre d'abord la multiplicité des rapports de force qui sont immanents à un domaine (...) les stratégies dans lesquelles ils prennent effet, et dont le dessin général ou la cristallisation institutionnelle prennent corps dans les appareils étatiques, dans la formulation de la loi, dans les hégémonies sociales*¹²⁰¹ ». Ainsi, le pouvoir est d'abord et avant tout un rapport de domination¹²⁰² qui doit être analysé en fonction des dispositifs¹²⁰³ qui lui permettent de s'établir. De la fin du 17^{ème} siècle jusqu'au milieu du 20^{ème} siècle, les mécanismes disciplinaires qui ont pour but de « *concentrer ; répartir dans l'espace; ordonner dans le temps ; composer dans l'espace-temps une force productive dont l'effet doit être supérieur à la somme des forces élémentaires*¹²⁰⁴ », constituent le fondement de la société disciplinaire. La société astreint l'individu à la norme sociale par « *l'organisation des grands milieux d'enfermement*¹²⁰⁵ », où « *l'individu ne cesse de passer d'un milieu clos à un autre*¹²⁰⁶ ». A l'image du panoptique, décrit précédemment, la société disciplinaire repose sur une maîtrise de l'espace, permettant au pouvoir d'exercer un contrôle omniprésent, « *visible et invérifiable*¹²⁰⁷ » pour reprendre les mots de Foucault, passant par la contrainte des corps au sein d'un espace déterminé. Ainsi, pour Foucault le biopouvoir est constitué par les techniques spécifiques du pouvoir, les dispositifs, qui s'exercent sur les corps individuels et les populations. Ces dispositifs

¹²⁰¹ FOUCAULT Michel, *Il faut défendre la société - Cours au collège de France. 1976*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 1997, p. 172 et suivant. Foucault avait fait précéder l'analyse en prenant appui sur Boulainvilliers et écrivait: « *La loi égalitaire de la nature est faible en face de la loi inégalitaire de l'histoire. Il est donc normal que la loi égalitaire de la nature ait cédé le pas, et définitivement, à la loi inégalitaire de l'histoire. C'est parce qu'il était le droit originaire que le droit naturel n'est pas fondateur, comme disent les juristes, mais forclos par la vigueur plus grande de l'histoire. La loi de l'histoire est toujours plus forte que la loi de la nature. C'est cela que soutient Boulainvilliers lorsqu'il dit que l'histoire est finalement arrivée à créer une loi naturelle d'antithèse entre la liberté et l'égalité, et que cette loi naturelle est plus forte que la loi inscrite dans ce qu'on appelle le droit naturel. La force plus grande de l'histoire par rapport à la force de la nature : c'est cela, finalement, qui fait que l'histoire a recouvert entièrement la nature. La nature ne peut plus parler quand l'histoire commence car, dans la guerre entre l'histoire et la nature, c'est toujours l'histoire qui l'emporte* ». (p. 139)

¹²⁰² Dans son cours du 4 février 1976, il déclare: « *Il n'en reste pas moins que vous voyez là se formuler pour la première fois l'idée que toute loi, quelle qu'elle soit, toute forme de souveraineté, quelle qu'elle soit, tout type de pouvoir, quel qu'il soit, doivent s'analyser non pas dans les termes du droit naturel et de la constitution de la souveraineté, mais comme le mouvement indéfini – et indéfiniment historique – des rapports de domination des uns sur les autres* ». Ibid. p. 76 et suivants

¹²⁰³ Par exemple: la souveraineté, les disciplines, le contrôle, la sécurité

¹²⁰⁴ DELEUZE Gilles, « Post-scriptum sur les sociétés de contrôle », in. *L'autre journal* n° 1, mai 1990, p. 2

¹²⁰⁵ Ibid.

¹²⁰⁶ Ibid.

¹²⁰⁷ FOUCAULT, Op. Cit.

sont hétérogènes aux mécanismes juridico-politiques du pouvoir souverain¹²⁰⁸.

555. La biopolitique, et les mécanismes de sa mise en oeuvre - le biopouvoir - s'appuie donc sur une dimension spatiale, sur le cloisonnement clair entre l'espace public et l'espace privé. Pour rappel, Foucault entend par la notion de biopolitique « *la manière dont on a essayé, depuis le XVIII^{ème} siècle, de rationaliser les problèmes posés à la pratique gouvernementale par les phénomènes propres à un ensemble de vivants constitués en population: santé, hygiène, natalité, longévité, races... On sait quelle place croissante ces problèmes ont occupé depuis le XIX^{ème} siècle, et quels enjeux politiques et économiques ils ont constitué jusqu'à aujourd'hui*¹²⁰⁹ ». Poursuivant cette analyse de la naissance de la biopolitique, Foucault montre bien qu'il ne faut pas « *dissocier ces problèmes du cadre de rationalité politique à l'intérieur duquel ils sont apparus et ont pris leur acuité. A savoir le « libéralisme », puisque c'est par rapport à lui qu'ils ont pris l'allure d'un défi*¹²¹⁰ ». Démontrant que le libéralisme doit s'analyser « *comme principe et méthode de rationalisation de l'exercice du gouvernement - rationalisation qui obéit, et c'est là sa spécificité, à*

¹²⁰⁸ A travers son ouvrage de référence, *Surveiller et punir*, Foucault évoque de manière éparse les mécanismes juridico-politiques. Il écrit par exemple: « *De là l'idée que l'appareil de justice doit se doubler d'un organe de surveillance qui lui soit directement ordonné, et qui permette soit d'empêcher les crimes, soit, s'ils sont commis, d'arrêter leurs auteurs; police et justice doivent marcher ensemble comme les deux actions complémentaires d'un même processus — la police assurant « l'action de la société sur chaque individu », la justice, « les droits des individus contre la société »; ainsi chaque crime viendra à la lumière du jour, et sera puni en toute certitude* » (p. 165). Ou encore: « *Mais si la police comme institution a bien été organisée sous la forme d'un appareil d'État, et si elle a bien été rattachée directement au centre de la souveraineté politique, le type de pouvoir qu'elle exerce, les mécanismes qu'elle met en jeu et les éléments auxquels elle les applique sont spécifiques. C'est un appareil qui doit être coextensif au corps social tout entier et non seulement par les limites extrêmes qu'il rejoint, mais par la minutie des détails qu'il prend en charge. Le pouvoir policier doit porter « sur tout » : ce n'est point cependant la totalité de l'État ni du royaume comme corps visible et invisible du monarque; c'est la poussière des événements, des actions, des conduites, des opinions — « tout ce qui se passe »; l'objet de la police, ce sont ces « choses de chaque instant », ces « choses de peu » dont parlait Catherine II dans sa Grande Instruction. On est, avec la police, dans l'indéfini d'un contrôle qui cherche idéalement à rejoindre le grain le plus élémentaire, le phénomène le plus passager du corps social : « Le ministère des magistrats et officiers de police est des plus importants; les objets qu'il embrasse sont en quelque sorte indéfinis, on ne peut les apercevoir que par un examen suffisamment détaillé » : l'infiniment petit du pouvoir politique. Et pour s'exercer, ce pouvoir doit se donner l'instrument d'une surveillance permanente, exhaustive, omniprésente, capable de tout rendre visible, mais à la condition de se rendre elle-même invisible. Elle doit être comme un regard sans visage qui transforme tout le corps social en un champ de perception : des milliers d'yeux postés partout, des attentions mobiles et toujours en éveil, un long réseau hiérarchisé, qui, selon Le Maire, comporte pour Paris les 48 commissaires, les 20 inspecteurs, puis les « observateurs », payés régulièrement, les « basses mouches » rétribuées à la journée, puis les dénonciateurs, qualifiés selon la tâche, enfin les prostituées. Et cette incessante observation doit être cumulée dans une série de rapports et de registres; tout au long du XVIII^e siècle, un immense texte policier tend à recouvrir la société grâce à une organisation documentaire complexe. Et à la différence des méthodes de l'écriture judiciaire ou administrative, ce qui s'enregistre ainsi, ce sont des conduites, des attitudes, des virtualités, des soupçons — une prise en compte permanente du comportement des individus ».* (p. 381 - 383)

¹²⁰⁹ FOUCAULT Michel, « Naissance de la biopolitique », *Annuaire du Collège de France, 79^{ème} année, Histoire des systèmes de pensée, année 1978 - 1979, 1979*, pp. 367 - 372; In. DEFERT Daniel et EWALD François (sous la direction de), *Michel Foucault, Dits et écrits 1954 - 1988, II. 1976 - 1988*, Editions Quarto Gallimard, 2001, texte n° 274, *Naissance de la biopolitique*, pp. 818 - 825, p. 818.

¹²¹⁰ Ibid.

*la règle interne de l'économie maximale*¹²¹¹ », il déclare alors qu'il « *rompt avec la raison d'Etat*¹²¹² », et qu'il est traversé par le principe : « *on gouverne toujours trop*¹²¹³ ». De cette analyse, on retiendra que le libéralisme comme principe de rationalisation de l'exercice du gouvernement a engendré une modification des règles d'exercice du pouvoir, des espaces sociaux, et des dispositifs de pouvoir.

2.... Au biopouvoir algorithmique comme nouvelle technique de pouvoir engendrée par la surveillance diffuse

556. Digitalisation de la vie, datafication, exploitation des traces des individus en vue de classer et d'anticiper leurs comportements sont les traits principaux de la biopolitique algorithmique. Elle fait concourir les institutions publiques et privées, et les individus, spontanément, volontairement ou non; et elle multiplie ainsi toujours plus l'apparition des traces digitales. Son objectif réel est d'élaborer une interaction inédite entre le savoir et le pouvoir. Pour de nombreux auteurs, tels que François Rigaux, Idriss Aberkane, ou encore Bernard Stiegler cette interaction inédite participe d'un changement radical de la notion de biopolitique comme mode d'exercice de pouvoir.

557. Pour Rigaux, par la « *mise en réseaux du savoir et du pouvoir*¹²¹⁴ » nous sommes passés « *de la noosphère à la noopolitique*¹²¹⁵ ». Opérant par renvoi sélectif à un texte de Pierre de

¹²¹¹ Ibid. p. 819

¹²¹² Ibid.

¹²¹³ Ibid. p. 820. Il conclut d'ailleurs: « *la rationalisation de la pratique gouvernementale, en termes de raison d'Etat impliquait sa maximalisation sous condition d'optimum, dans la mesure où l'existence de l'Etat suppose immédiatement l'exercice du gouvernement. La réflexion libérale ne part pas de l'existence de l'Etat, trouvant dans le gouvernement le moyen d'attendre cette fin qu'il serait pour lui-même; mais de la société qui se trouve être dans un rapport complexe d'extériorité et d'intériorité vis-à-vis de l'Etat. C'est elle - à la fois à titre de condition et de fin dernière - qui permet de ne plus poser la question : comment gouverner le plus possible et au moindre coût possible ? Mais, plutôt celle-ci: pourquoi faut-il gouverner? C'est-à-dire: qu'est-ce qui rend nécessaire qu'il y ait un gouvernement et quelles fins doit-il poursuivre, à l'égard de la société, pour se justifier d'exister. ».*

¹²¹⁴ RIGAUX François, « De la noosphère à la noopolitique. La mise en réseaux du savoir et du pouvoir », in *Liber amicorum Paul Maertens*, Bruxelles, Larcier, 2007, pp. 967-982, En ligne: <http://www.sfdi.org/wp-content/uploads/2014/08/RIGAUXnoos.pdf> (dernière consultation: 5 mars 2018)

¹²¹⁵ Ibid.

Teilhard de Chardin¹²¹⁶, Rigaux écrit « *ce que la noosphère apporte de neuf, c'est une extension planétaire de la connaissance, hissant la pensée à un niveau supérieur. Le cerveau humain s'accomplit dans un « Cerveau des cerveaux ». C'est « la Machine » qui substitue au jeu des fibres nerveuses non pensantes » un « cerveau collectif¹²¹⁷ » » ». Le propos de la noopolitique doit être nuancé car si pour ses thuriféraires elle est la représentation d'une machine libératrice, elle est également la consécration de ce qu'on a pu décrire sous l'expression du Monstre Doux. Bien que certains des éléments de cette noopolitique sont en train d'apparaître et de se dessiner aujourd'hui¹²¹⁸, cette dernière énonce de manière hypothétique, un futur proche s'inscrivant dans une doctrine évolutionniste liée à la technologie et au progrès; mais il ne semble pas que l'on puisse conclure à l'absolue positivité de cette notion. Portant sa réflexion sur la surveillance, et évoquant le concept de société de clairvoyance, Frédéric Neyrat déclare quant à lui que: « *le futur est l'objet direct des sociétés de clairvoyance: ce n'est pas le passé qu'il s'agit de recommencer avec un nouveau moule, ni le présent qu'il faut moduler instant par instant au sein d'une continuité factice, c'est le futur qu'il s'agit de mouler ou moduler avant même qu'il n'ait lieu, de façon préventive grâce à la dataveillance. Si, pour suivre encore le schéma deleuzien, les sociétés disciplinaires avaient le corps pour enjeu (biopolitique), et les sociétés de contrôle l'âme ou l'esprit (noopolitique), alors les sociétés de clairvoyance voudraient identifier la glande pinéale, c'est-à-dire**

¹²¹⁶ Rigaux reprend une citation entière de Teilhard de Chardin: « *la machine libératrice, sans doute, délestant la pensée, tant individuelle que sociale, de tout ce qui alourdirait son ascension. Mais la Machine constructive, aussi, aidant à nouer sur soi, à se concentrer sous forme d'un organisme toujours plus pénétrant les éléments réfléchis de la Terre. Et ici, naturellement, je songe en premier lieu à l'extraordinaire réseau de communications radiophonique et télévisuelle, anticipant peut-être une synchronisation directe des cerveaux au moyen des forces encore mystérieuses de la télépathie, nous reliant déjà tous, actuellement, dans une sorte de co-conscience « éthérée ». Mais je songe aussi à la montée insidieuse de ces étonnantes machines à calcul qui, grâce à des signaux combinés à raison de plusieurs centaines de mille par seconde, non seulement viennent soulager notre cerveau d'un travail fastidieux et épuisant, mais encore parce qu'elles augmentent en nous le facteur essentiel (et trop peu observé) de « la vitesse de la pensée » sont en train de préparer une révolution dans le domaine de la Recherche. Tous ces progrès, et combien d'autres, une certaine philosophie en sourit avec dédain. « Machines commerciales, entend-on répéter, machine de gens pressés, pour gagner du temps et de l'argent ». O aveugles, a-t-on envie de dire, comment n'apercevez vous pas que ces instruments matériels, inéluctablement reliés les uns aux autres dans leur apparition et leur développement, ne sont finalement pas autre chose que les linéaments d'une sorte particulière de super-cerveau, capable de s'élever à la maîtrise de quelque super-domaine dans l'Univers et dans la Pensée! ».* TEILHARD DE CHARDIN Pierre, « Une interprétation biologique plausible de l'histoire humaine: la formation de la Noosphère », *Revue des questions scientifiques*, Louvain, janvier 1947, Cité par RIGAUX, Op. Cit. p 967 - 968. Le problème est qu'il ignore les avertissements de son auteur.

¹²¹⁷ RIGAUX François, Op. Cit. p 967.

¹²¹⁸ Pour Idriss Aberkane « *la géopolitique est l'interaction du pouvoir et de la terre. La spatiopolitique est l'interaction du pouvoir, de l'espace et du temps: dans l'espace, les distances sont des fonctions du temps. La noopolitique est l'interaction du pouvoir et du savoir, du pouvoir et de la sagesse. Elle est la politique et la géopolitique de connaissance. Ses implications sont profondes. Elles expliquent le comportement des princes du passé, leurs erreurs et leurs biais, et permettent aux dirigeants du futur de dépasser ces erreurs. De plus, dans notre monde globalisé, n'importe qui est souverain dans une certaine mesure, ce qui commence déjà par la souveraineté sur soi-même. La noopolitique déclare que cette souveraineté est, à toutes les échelle des organisations humaines, la source de tout bien et la source de tout pouvoir ».* ABERKANE Idriss, *La noopolitique: le pouvoir de la connaissance*, Fondation pour l'innovation politique, novembre 2015, p. 9, En ligne: <http://www.fondapol.org/etude/idriss-j-berkane-la-noopolitique-le-pouvoir-de-la-connaissance/> (dernière consultation: 5 mars 2018)

quelque chose qui n'existe pas (ecto-politique)¹²¹⁹ ».

558. L'ensemble de ces réflexions liées à la noopolitique tendent à éclairer plusieurs points d'analyse concernant la biopolitique algorithmique. Il faut en effet retenir ici la temporalité dans laquelle s'exerce le pouvoir de nos jours, à cheval entre le présent et le moment à-venir. Il faut également souligner cette ambition de la noopolitique à envisager cette stricte équivalence entre savoir et pouvoir. Cette interaction est bien ce que la société de l'information a participé à créer, et ce que la surveillance diffuse permet d'accomplir à l'aide des mécanismes de l'économie néo-libérale. La surveillance diffuse est fondée sur le savoir informationnel, sur l'analyse du comportement des individus, de leurs données personnelles ou non, de leurs informations, leurs traces. Les dispositifs actuels tendent à capter de l'information et des traces, et à les faire parler. Antoinette Rouvroy et Thomas Berns évoque alors le « *nouveau pouvoir statistique*¹²²⁰ ». Ce nouveau type de pouvoir est selon les auteurs « *un régime de visibilité et d'intelligibilité des individus d'une efficacité, d'une finesse et d'une omniprésence jusque-là jamais atteintes, tout en plongeant dans l'ombre, dans l'invisible et dans l'indicible une bonne part de ce qui reste, malgré tout, intraduisible sous forme de données digitales. L'intelligence et l'« efficacité » de ces dispositifs – se présentant à la fois comme des interfaces cognitives et des instruments de gouvernement – consistent dans le fait qu'ils sont capables d'interpréter eux-mêmes les données qu'ils enregistrent en fonction de critères de normalité ou d'anormalité, de désirabilité ou d'indésirabilité, d'intérêt ou d'indifférence*¹²²¹ ». Ce nouveau pouvoir statistique se fonde bien sur les éléments que la surveillance diffuse a permis d'élaborer: « *l'enregistrement massif et systématique de données, le « data mining » et le profilage sont les instruments d'une transformation des rationalités, stratégies et tactiques de gouvernement*¹²²² ». La temporalité dans

¹²¹⁹ NEYRAT Frédéric, Op. Cit., p. 108. Il poursuit l'analyse de cette glande pinéale par une citation de Descartes, tirée de l'article 32 des *passions de l'âme*: « *Et, pour citer un philosophe qui croyait fermement en l'existence de cette glande, on lira avec un drôle de regard ces quelques lignes qui datent du XVII^e ème siècle: « et si on peut aisément concevoir que ces images ou autres impressions se réunissent en cette glande par l'entremise des esprits qui remplissent les cavités du cerveau, mais il n'y a aucun autre endroit dans le corps où elles puissent ainsi être unies, sinon en suite de ce qu'elles le sont en cette glande ».*

¹²²⁰ ROUVROY Antoinette, Berns Thomas, « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événements car constitué de corps « numériques »... », *Multitudes* 2010 / 1 (n° 40), p. 88 - 103, Disponible en ligne à l'adresse suivante: <https://www.cairn.info/revue-multitudes-2010-1-page-88.htm> (dernière consultation: 5 mars 2018)

¹²²¹ Ibid. p. 88.

¹²²² Ibid. Et de poursuivre: « *Cette révolution du pouvoir, tranquille et sans douleur apparente, repose sur l'intensification du phénomène contemporain d'enregistrements systématiques et de « digitalisation de la vie même », à laquelle concourent les institutions publiques et privées, mais aussi les individus eux-mêmes qui, spontanément, volontairement ou non, conservent, publient et multiplient leurs traces digitales »*

laquelle s'exerce ce nouveau pouvoir est « *préemptive et actuarielle*¹²²³ » c'est-à-dire qu'elle se focalise « *sur la prédiction*¹²²⁴ »; et permet au « *gouvernement statistique (de) vise (r) non plus à maîtriser l'actuel, à dompter la sauvagerie des faits, mais à structurer le possible, à éradiquer le virtuel, cette dimension de possibilité ou de potentialité d'où provient que l'actuel tremble toujours un peu d'un devenir « autre » qui constitue, justement, sa singularité et sa puissance, alors même qu'il n'est pas empiriquement connu (et qu'il ne peut, par définition, jamais l'être)*¹²²⁵ ». Le pouvoir statistique s'exerce sur des individus réduit à leur trace¹²²⁶ et permet d' « *anticiper ce que « peuvent » faire les individus*¹²²⁷ », car le pouvoir algorithmique « *tend à proposer des solutions, à travers des applications impliquant des dispositifs de biométrie dynamique, de vidéosurveillance intelligente, d'environnements intelligents, d'informatique ubiquitaire et fonctionnant de manière autonome*¹²²⁸ ». On retrouve ici des caractéristiques de la surveillance diffuse, et plus particulièrement son caractère ubiquitaire. On comprend également le lien entre les descriptions technologiques des auteurs et la conception de la surveillance diffuse comme outil d'un nouveau pouvoir mais également d'un nouveau contrôle social qui dresse et domestique les individus.

559. Couplés à l'analyse de Bernard Stiegler, concernant la « *smartification*¹²²⁹ » de la société automatique, ces mots amènent à penser que la surveillance diffuse est à la fois dispositif et constituant de la biopolitique et du biopouvoir algorithmique. Selon Stiegler, en effet, « *l'infrastructure actuelle évolue à grands pas vers une société d'hypercontrôle fondée sur les équipements mobiles, tel le smartphone, les équipements domestiques, telle la télévision connectée, les habitats, telles la smart house et la smart city, et les équipements de transport, telle l'automobile connectée*¹²³⁰ ». Concluons cette étude avec les mots de Gabriel Tarde qui écrivait : « *la statistique appliquée à tous les aspects de notre vie sociale aboutirait partout à des séries uniformes,*

¹²²³ Ibid. p. 92.

¹²²⁴ Ibid.

¹²²⁵ Ibid. p. 93

¹²²⁶ Les auteurs emploient ici la notion de « *dividualisation* » des sujets de la gouvernementalité algorithmique » (p. 94). Nous évoquerons plus largement la réduction de l'individu à sa trace, et le concept de *dividi* développé par Deleuze, repris par Thomas Berns et Antoinette Rouvroy, dans le cadre du chapitre 3.

¹²²⁷ Ibid. p. 89

¹²²⁸ Ibid.

¹²²⁹ STIEGLER Bernard, Op. Cit., pp. 39 - 44.

¹²³⁰ Ibid. p. 40

horizontalement déroulées et parfaitement comparables aux fameuses « lois de la nature »¹²³¹ ». Et de poursuivre: « par suite, en admettant un perfectionnement et une extension de la statistique poussés à ce point, ses bureaux seraient tout à fait comparables à l'oeil ou à l'oreille. Comme l'oeil ou l'oreille, ils synthétiseraient, pour nous éviter cette peine, des collections d'unités similaires dispersées, et nous présenteraient le résultat clair, net, liquide de cette élaboration¹²³² ». Etonnante acuité prémonitoire de Gabriel Tarde qui présentait déjà dans le pouvoir statistique, la description de la surveillance diffuse, et du biopouvoir algorithmique fondée sur la donnée, l'information, la datafication.

Paragraphe 2: La transformation des espaces sociaux par la surveillance diffuse comme perte de sens du droit ou reconnaissance d'une nouvelle fonction:

560. Evoquer l'organisation de la transparence intégrale dans les espaces sociaux revient à analyser l'éclatement de la dichotomie classiquement admise entre ce qui relève de l'espace public et ce qui relève de l'espace privé (A). Traditionnellement axée autour de la notion de propriété, cette dichotomie n'est plus aussi prégnante aujourd'hui du fait même de la surveillance diffuse. On constate même un renversement de cette dernière par la publicisation du privé et la privatisation du public (B). La smart-city en représente l'aboutissement clair. La fonction du Droit, d'édicter des règles de conduite sociale dans un espace donné s'en retrouve bouleversée. Le Droit conçu sans espace (d'application) se retrouve alors dans l'obligation d'assurer ou de participer à la construction de la transparence totale

A. L'importance de la dichotomie entre l'espace public- espace privé pour le Droit

561. La distinction du public et du privé est primordiale dans la circulation du Droit. Dans sa fonction d'édition de règles de vie en société, le Droit a une importance vitale dans la sphère publique. Il a en revanche une fiction relative dans le cadre de la sphère privée. La dichotomie publique et privé pourrait se résumer ainsi: tout ce qui est public est ouvert à tous, et ce qui est privé relève de la propriété de certains, cet espace est alors fermé pour certains et réservé à d'autres. Au-delà de cette distinction simpliste, il faut comprendre et analyser la circulation et la fonction du Droit dans chacun des deux espaces: l'espace public (1) et l'espace privé (2)

¹²³¹ TARDE Gabriel, Op. Cit., p. 130.

¹²³² Ibid. p. 146.

1. Circulation et fonction du droit dans l'espace public

562. La surveillance diffuse vient redéfinir les contours des sociétés démocratiques, en ce qu'elle bouleverse les conditions de vie de l'individu dans la sphère privée, mais également dans le cadre de l'espace public. Entendu par le droit comme le milieu où s'exercent les prérogatives de puissance publique, l'espace public se voit en réalité redéfinir de nos jours tantôt par l'avènement d'un ordre public sécuritaire, tantôt par l'idéologie utilitariste que sous-tend le néo-libéralisme économique.

563. En réalité, il n'y a que peu de références à ce concept dans la jurisprudence ou dans la loi. En 2010, la loi interdisant la dissimulation du visage dans l'espace public¹²³³ précise en son article 2 que « *l'espace public est constitué des voies publiques ainsi que des lieux ouverts au public ou affectés à un service public*¹²³⁴ ». Cette loi, envisagée pour encadrer l'utilisation de vêtements typiques tels que la burqua, est assez imprécise quant au concept d'espace public. Et, la doctrine et la jurisprudence à ce sujet se sont principalement concentrées sur l'exercice de la liberté de religion. Par la référence aux voies publiques et aux lieux ouverts au public, cet article donne à penser que l'espace public est d'abord un espace physique. Ainsi envisagée, cette notion donne au Droit, la fonction de déterminer les règles de conduite des individus dans un espace physique donné. Le code de la route en est une illustration parfaite: pour conduire sur les voies publiques, l'individu doit passer un examen attestant de ses capacités, et respecter les règles de conduite afin de garantir sa sécurité et celle des autres. Le droit entretient donc ici une relation particulière avec l'espace auquel il s'applique. L'exemple du code de la route permet également de mettre en lumière un second élément de l'espace public. Ce dernier est également un lieu qui met à disposition du public un bien ayant un intérêt public géré par l'Etat ou par le secteur privé. Le Droit s'applique ici pour réguler l'accès, l'utilisation et les restrictions liées à ce bien. L'espace public doit alors être analysé également comme lieu d'exercice de la fonction de régulation publique, d'application du droit, et plus particulièrement du droit public.

564. Si peu d'études juridiques ont été réalisées sur le concept d'espace public, les autres

¹²³³ Loi n°2010-1192 du 11 octobre 2010 interdisant la dissimulation du visage dans l'espace public, JORF n°0237 du 12 octobre 2010, p. 18344, Texte n° 1, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022911670&categorieLien=id> (dernière consultation: 5 mars 2018). Son article 1er déclare: « nul ne peut, dans l'espace public, porter une tenue destinée à dissimuler son visage.

¹²³⁴ Ibid

sciences sociales apportent des éléments de réponses intéressants. Ainsi que le note Hannah Arendt, à propos de la condition de l'homme moderne, « *la distinction entre la vie privée et la vie publique correspond aux domaines familial et politique, entités distinctes, séparées au moins depuis l'avènement de la Cité antique; mais l'apparition du domaine social qui n'est, à proprement parler, ni privé ni public, est un phénomène relativement nouveau, dont l'origine a coïncidé avec la naissance des temps modernes et qui a trouvé dans l'Etat-nation sa forme politique*¹²³⁵ ». A la lecture de ces lignes, il faudrait alors comprendre l'espace public comme l'espace du politique, du débat public. Le Droit est alors également le produit de ce débat. C'est également ce que Jürgen Habermas relève en 1968 lorsqu'il envisage cet espace comme essentiel pour l'élaboration du système juridique, car représentant un espace d'interaction et de relations individuelles¹²³⁶ regroupées en collectif: la société civile. Au delà de ces éléments, relevons avec Hannah Arendt que « *Ce qui nous intéresse ici, c'est l'extraordinaire difficulté (...) à comprendre la division capitale entre domaine public et domaine privé, entre la sphère de la polis et celle du ménage, de la famille, et finalement entre les activités relatives à un monde commun et celles qui concernent l'entretien de la vie: sur ces divisions, considérées comme des postulats, comme des axiomes, reposait toute la pensée politique des Anciens. Dans nos conceptions, la frontière s'efface parce que nous imaginons les peuples, les collectivités politiques comme des familles dont les affaires quotidiennes relèvent de la sollicitude d'une gigantesque administration ménagère*¹²³⁷ ».

565. Cette citation démontre de la clairvoyance de Hannah Arendt à décrire un phénomène qui n'a cessé de s'accélérer. Il apparaît clairement aujourd'hui que la distinction entre ce qui relève de la « polis » et celle du « ménage » s'est encore estompée au bénéfice de la « *sollicitude de la gigantesque administration ménagère* » décrite par Arendt. La notion même de « sollicitude » est ici pleinement à rapprocher de la notion d'attention, de ce nouveau contrôle social qui promeut bien-être, sécurité et liberté. Et la « *gigantesque administration ménagère* » correspond à ce que Hannah

¹²³⁵ ARENDT Hannah, *Condition de l'homme moderne* ; traduit de l'anglais par Georges Fradier ; préface de Paul Ricoeur, Paris, Pocket, 2009, p. 66

¹²³⁶ HABERMAS Jürgen, *L'espace public. Archéologie de la publicité comme dimension constitutive de la société bourgeoise*, Paris, Payot, 1998.

¹²³⁷ ARENDT Hannah, *Condition de l'homme moderne* ; traduit de l'anglais par Georges Fradier ; préface de Paul Ricoeur, Paris, Pocket, 2009, p. 66

Arendt appelle ensuite « *l'avènement du social*¹²³⁸ », de l'Etat-social, et pour reprendre l'analyse précédente, le bien-être des nations. Loin de confirmer, la désinstitution de l'Etat, la modification des espaces sociaux par la surveillance diffuse ont un impact sur la fonction du Droit.

2.Circulation et fonction du Droit dans l'espace privé

566. La distinction du privé et du public est traditionnellement liée au droit de propriété¹²³⁹. La sphère du privé répondait jusqu'à peu à des règles que le (bon) père de famille édictait en sa demeure. Ainsi que le note Maurice Blanc et Jean-Yves Causer, « *on a longtemps considéré que sauf dans les cas extrêmes, les violences infligées aux femmes et aux enfants dans le cadre familial étaient une affaire privée. (...). Cet exemple montre bien l'ambiguïté de la notion de privé, fondée sur la propriété. Dans le droit romain, inspirateur du code napoléonien, l'homme est le chef de famille et il est propriétaire de sa femme et des enfants qu'elle lui donne, ainsi que de l'ensemble des biens familiaux. Le droit de propriété est le droit « d'user et d'abuser », des uns comme des autres. Rousseau n'est pas très éloigné de cette conception, lorsqu'il voit dans la propriété privée une garantie de la liberté du citoyen. Le « contrat social » tel qu'il l'imagine est un pacte entre petits propriétaires*¹²⁴⁰ ».

567. A la lecture de ces lignes, tout se passe comme si le domicile permettait d'entrevoir la frontière entre le public et le privé, le dehors et le dedans. Par la référence au contrat social, et aux conditions de la propriété (l'usus, l'abusus et le fructus), les auteurs démontrent également que le Droit circule dans l'espace privé sous la forme du contrat. Ces mots rappellent également ce que l'étude de Jürgen Habermas démontrait: alors que dans l'espace public la logique du consensus règne, la sphère privée est soumise à la logique de la compromission. La lecture de l'ouvrage de

¹²³⁸ Arendt écrit ainsi que « *l'apparition de la société - l'avènement du ménage, de ses activités, de ses problèmes, de ses procédés d'organisation - sortant de la pénombre du foyer, pour s'installer au grand jour du domaine public, n'a pas seulement effacé l'antique frontière entre le politique et le privé; elle a si bien changé le sens des termes, leur signification pour la vie de l'individu et du citoyen, qu'on ne les reconnaît presque plus. (...). Ce qui paraît plus important encore, c'est que de nos jours le privé s'oppose au moins aussi nettement au domaine social (inconnu des Anciens qui voyaient dans son contenu une affaire privée) qu'au domaine politique proprement dit. Evénement historique décisif: on découvre que le privé au sens moderne, dans sa fonction essentielle qui est d'abriter l'intimité, s'oppose non pas au politique mais au social, auquel il se trouve par conséquent plus étroitement, plus authentiquement lié* ». (Ibid. p. 76 - 77).

¹²³⁹ En ce sens, voir AUBY Jean-Bernard, « Espace public, espaces publics », *Droit administratif*, n°7, Juillet 2009, p. 21: la propriété individuelle est analysée par l'auteur comme « *le moyen essentiel par lequel le Droit rattache des droits et des obligations à des choses et des lieux: en indiquant qui possède, quel type de droits et d'obligations, à un en droit donnée* ».

¹²⁴⁰ BLANC Maurice, CAUSER Jean-Yves, « Privé - Public: quelles frontières ? », *Revue des sciences sociales*, En ligne: <http://www.revue-des-sciences-sociales.com/pdf/rss33-presentation.pdf> (dernière consultation: 5 mars 2018)

Hannah Arendt est également particulièrement éclairante quant à la notion de « domaine privé ». Pour l'auteur, « *dans la pensée antique tout tenait dans le caractère privatif du privé, comme l'indique le mot lui-même; cela signifiait que l'on était littéralement privé de quelques choses, à savoir des facultés les plus hautes et les plus humaines. L'homme qui n'avait d'autre vie que privée, celui qui, esclave, n'avait pas droit au domaine public, ou barbare, n'ait pas su fonder ce domaine, cet homme n'était pas pleinement humain*¹²⁴¹ ». Et d'ajouter que, « *quand nous parlons du privé, nous ne pensons plus à une privation et cela est dû en partie à l'enrichissement énorme que l'individualisme moderne a apporté au domaine privé*¹²⁴² ».

568. De nos jours, le caractère privatif du privé n'est plus, le privé renvoie beaucoup plus à la notion de propriété privée¹²⁴³, et à son corollaire la vie privée. L'espace privé est également le lieu de formation de l'opinion, de l'expression, de la réflexion. En cela, la vie (dans l'espace) privé(e), et le respect du droit à la vie privée est à la fois une garantie pour la libre formation des idées mais également de leur expression. Si la seconde assertion semble ancrée dans nos sociétés au travers de la liberté d'expression, la première semble moins intelligible. La première assertion pourrait s'apparenter à ce que la Cour Constitutionnelle fédérale allemande entendait sous cette expression: « *le pouvoir de l'individu de décider de lui-même sur base du concept d'autodétermination, quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui*¹²⁴⁴ ». Traduit dans le cadre d'un rapport d'information de 2015 comme le droit permettant de « *donner à l'individu l'autonomie informationnelle et décisionnelle nécessaire à son libre épanouissement dans l'univers numérique*¹²⁴⁵ », ce droit à l'autodétermination informationnelle est aujourd'hui dans son application réduite à la seule reconnaissance d'un droit à la maîtrise des données reconnu à l'individu¹²⁴⁶. A cheval entre un réel droit à l'autodétermination et un droit à être

¹²⁴¹ Op. Cit. p. 76 - 77.

¹²⁴² Ibid.

¹²⁴³ Arendt développe cet analyse dans son chapitre 2 de l'ouvrage précité (pp. 59 - 121). voir spécialement: pp. 99 - 109

¹²⁴⁴ FROMONT Michel, Analyse de l'arrêt de la Cour constitutionnelle fédérale allemande du 16 février 1983, *BVerfGE*, tome 62, p. 1, *Revue de Droit public* 1983, p. 954

¹²⁴⁵ PAUL Christian, FERAL-SCHUHL Christiane, Rapport d'information n° 3119 déposé par la Commission de Réflexion et de propositions sur les droits et libertés à l'âge du numérique - *Numérique et Libertés: Un nouvel âge démocratique*, 2015, p. 131, En ligne: <http://www.assemblee-nationale.fr/14/pdf/rapports/r3119.pdf> (dernière consultation: 5 mars 2018)

¹²⁴⁶ Au travers des textes, spécialement de la loi pour la République Numérique, l'autodétermination informationnelle est une consécration de la maîtrise par les individus de leurs données personnelles, au sens du Règlement général de protection des données.

laissé seul¹²⁴⁷, permettant le libre épanouissement de l'individu, la formation libre des idées est permise dans l'espace privé. Qu'elle soit construite sur la doctrine des droits naturels, imprescriptibles et intrinsèques à l'individu¹²⁴⁸, ou sur l'idée du contrat social, qui permet à l'homme de s'arracher de l'état de nature et de vivre en société¹²⁴⁹, la reconnaissance de droits individuels permet de distinguer ce qui relève du privé, et ce qui revient à l'intérêt général, à la société, au public. Ainsi que Wolfgang Sofsky le démontre en opérant quelques « *retours sur le passé*¹²⁵⁰ », c'est avec la Révolution et la construction d'une nouvelle Nation que le privé, et plus particulièrement la vie privée subit « *une attaque d'une ampleur sans précédent dans le monde occidental*¹²⁵¹ ». Interdiction des regroupements privés, tenue vestimentaire qui « *devient une bannière des opinions*¹²⁵² », le tutoiement qui remplace les dialectes (...) sont autant d'exemples que Sofsky évoque comme immixtion de la République et de l'Etat, au nom de la Nation de l'époque.

569. Ses conclusions préliminaires amorcent d'ailleurs l'analyse du pouvoir que Foucault a établi dans le cadre de sa leçon de 1976 concernant le propos de la défense de la société¹²⁵³. Sofsky écrit ainsi que « *l'histoire de la sphère privée n'a jamais suivi un cours linéaire. Elle subit des régressions et fait des bonds en avant, revient parfois à des étapes antérieures et explore des contrées jusqu'alors inconnues. Aux époques de relative liberté succèdent des périodes d'ingérence, de surveillance et d'oppression. La pression du collectif, de la société, de l'autorité n'a jamais cessé de chercher à ramener les sphères privées à de moindres dimensions, jusqu'à ce que les gens se rappellent de nouveau les méthodes qui permettent de saper les exigences officielles et de protéger leurs secrets contre l'indiscrétion organisée*¹²⁵⁴ ». Aujourd'hui, la surveillance diffuse opère une nouvelle immixtion dans le privé et le public conduisant à une transparence totale par la privatisation du public et la publicisation du privé.

¹²⁴⁷ WARREN Samuel, BRANDEIS Louis, *The Right to Privacy*, Harvard Law Review, vol. 4, no. 5, 15 décembre 1890, pp. 193 - 220, En ligne: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> (dernière consultation: 5 mars 2018)

¹²⁴⁸ Grotius

¹²⁴⁹ Hobbes et Rousseau

¹²⁵⁰ SOFSKY Wolfgang, *Le citoyen de verre - entre surveillance et exhibition*, Traduit de l'allemand et préfacé par Olivier Mannoni, Editions de l'Herne, Paris, 2011, pp. 34 - 40.

¹²⁵¹ Ibid. p. 38.

¹²⁵² Ibid

¹²⁵³ Op. Cit.

¹²⁵⁴ SOFSKY, Op. Cit. p. 39

B. La nouvelle fonction du Droit engendrée par la surveillance diffuse: la participation à l'élaboration d'une transparence totale par la privatisation du public et la publicisation du privé

570. Le public influence traditionnellement le privé par des objectifs qu'il détermine. Cet espace public, qui devient de plus en plus social, c'est-à-dire qui fait entrer les préoccupations du privé dans le public, amène à une influence, un pouvoir continu¹²⁵⁵ et bienveillant. La surveillance diffuse se fonde sur cette préoccupation de l'espace public à gagner de plus en plus de terrain sur l'espace privé. Les téléphones, les GPS, les cartes à puces, la technologie RFID, les wifi des espaces commerciaux permettent la détection de nos mouvements, le suivi de personne, la collecte de données, personnelles, financières, de santé, d'échanges électroniques¹²⁵⁶. La fonction du droit se retrouve modifiée. En s'appliquant à des espaces sans caractéristique clair, ni privé, ni public, il participe clairement de l'organisation de la transparence totale (1), la Smart-city en est un exemple parfait (2).

1. L'organisation de la transparence totale prise en charge par le Droit

571. L'organisation de la transparence totale par le Droit est la consécration d'un paradoxe qu'illustraient Wolfgang Sofsky et Hannah Arendt: l'influence de la Nation, de la Société, sur la sphère privée et publique. Ce paradoxe pourrait s'illustrer par la privatisation des lieux publics et la publicisation des lieux privés; mutation fondées sur trois processus de changement essentiel qu'il est nécessaire d'analyser ici.

¹²⁵⁵ Voir en ce sens l'analyse de Foucault, en terme d'espace, relative à la peste et à la surveillance où l'auteur écrit: « Car ce territoire, ce n'était pas le territoire confus dans lequel on rejetait la population dont on devait se purifier. Ce territoire était l'objet d'une analyse fine et détaillée, d'un quadrillage minutieux. La ville en état de peste - et là je vous cite une série de règlements, d'ailleurs absolument identiques les uns aux autres, qui ont été publiés depuis la fin du Moyen-Age jusqu'au début du XVIII^{ème} siècle - était partagée en districts, les districts étaient partagés en quartiers, puis dans ces quartiers on isolait les rues, et il y avait dans chaque rue des surveillants, dans chaque quartier des inspecteurs, dans chaque district des responsables de district et dans la ville elle-même un gouverneur nommé à cet effet, soit encore les échevins qui avaient reçu, au moment de la peste, un supplément de pouvoir. Analyse, donc, du territoire dans ses éléments les plus fins; organisation, à travers ce territoire ainsi analysé, d'un pouvoir continu, et continu dans deux sens. D'une part, à cause de cette pyramide, dont je vous parlais tout à l'heure. Depuis les sentinelles qui veillaient devant les portes des maisons, à l'extrémité des rues, jusqu'aux responsables des quartiers, responsables des districts et responsable de la ville, vous aviez là une sorte de grande pyramide de pouvoir dans laquelle aucune interruption devait avoir place. C'était un pouvoir qui était également continu dans son exercice, et pas simplement dans sa pyramide hiérarchique, puisque la surveillance devait être exercée sans interruption aucune ». in. FOUCAULT Michel, *Les anormaux - Cours au collège de France. 1974 -1975*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 1999, p. 42

¹²⁵⁶ A titre d'exemple illustrant ce propos, on citera l'article suivant: SIGNORET Perrine, *Comment le centre commercial des quatre temps a traqué ses visiteurs ?*, L'express, 15 juillet 2017, Disponible en ligne à l'adresse suivante: http://lexpansion.lexpress.fr/high-tech/comment-le-centre-commercial-des-quatre-temps-a-traque-ses-visiteurs_1927269.html (dernière consultation: 5 mars 2018)

572. Richard Sennett a évoqué dès les années 1970 la privatisation des lieux publics, en proclamant « *la mort de l'espace public*¹²⁵⁷ » emporté par la sphère privée. Selon l'auteur, une nouvelle conception de la visibilité dans l'espace public voit le jour depuis le début des années 1980, par la construction de grands bâtiments de verre. S'appuyant sur des exemples tels que le site de la Défense à Paris, ou encore la Lever House à New York, Richard Sennett, citant Giedion, déclare que ces constructions remplissent deux fonctions de transparence totale et de barrière hermétiques. Il écrit ainsi que: « *cette technologie permet la réalisation de ce que S. Giedion appelle l'idéal du mur perméable, l'optimum de la visibilité*¹²⁵⁸ ». Ainsi, « *l'esthétique de la visibilité*¹²⁵⁹ » et « *l'isolement social*¹²⁶⁰ » que permettent ces constructions, font de l'espace public, non plus le lieu d'échange et de discussion politique qu'envisageait Jürgen Habermas¹²⁶¹ par exemple, mais le conceptualise comme un lieu de passage, un « *dérivé du mouvement*¹²⁶² ». Cette idéologie récente de la transparence totale constitue le premier point d'analyse du processus de privatisation de l'espace public, et engendre un second mouvement: la mise en contrôle de ces espaces et leur normalisation. Multiplication des caméras de vidéosurveillance, des lois anti-mendicité, règles de comportements dans les jardins publics par exemple, interdiction de fumer dans des lieux publics, sont autant d'exemples de la normalisation et de la mise en contrôle des

¹²⁵⁷ Dans son ouvrage *The fall of Public Man*, traduit en français sous le titre suivant *les tyrannies de l'intimité*, Editions du Seuil, 1979; Richard Sennett écrit que « (...) il s'agit de la Lever House qui domine Park Avenue, à New York. Au niveau du sol se trouve un espace ouvert, une cour sur le côté nord de laquelle s'élève une tour; au premier étage, on trouve une structure basse faisant le tour des trois autres côtés. Pour atteindre la cour lorsqu'on vient de la rue, on doit passer sous cette structure; le niveau de la rue lui-même est un espace mort. Aucune activité particulière au rez-de-chaussée: celui-ci n'est guère qu'un lieu de passage vers l'intérieur. La forme de ce gratte-ciel de type « International » est en contradiction avec sa fonction: il y a bien une place publique miniature, mais sa fonction détruit la nature même de la place publique, qui est de mélanger les gens et les activités. Cette contradiction renvoie à un conflit plus important (...). Des parois faites presque entièrement de verre encadré par de minces supports d'acier font qu'intérieur et extérieur de l'immeuble se confondent : cette technologie permet la réalisation de ce que S. Giedion appelle l'idéal du mur perméable, l'optimum de la visibilité. Mais ces murs sont aussi d'hermétiques barrières. La Lever House a été le premier exemple d'une conception architecturale selon laquelle le mur, bien que transparent, coupe totalement l'espace intérieur de l'espace extérieur. Cette conception unit esthétique de la visibilité et isolement social. (...) A la Défense comme à Lever House, cet espace est une surface que l'on traverse, non un lieu où l'on reste. (...). Le niveau du sol, selon les propres mots d'un architecte, sert de « lien support du flot de circulation pour l'ensemble vertical ». Traduit en langage clair, ceci signifie que l'espace public est devenu un dérivé du mouvement ». (p. 29 - 30)

¹²⁵⁸ Ibid.

¹²⁵⁹ Ibid.

¹²⁶⁰ Ibid.

¹²⁶¹ Jürgen Habermas a étudié en 1962 « *le processus au cours duquel le public constitué par les individus faisant usage de leur raison s'approprie la sphère publique contrôlée par l'autorité et la transforme en une sphère où la critique s'exerce contre le pouvoir de l'État* ». in. HABERMAS Jürgen, *L'espace public - Archéologie de la publicité comme dimension constitutive de la société bourgeoise*, traduit de l'allemand par M.B. de Launay, Editions Payot, Paris, 1978, p. 61. A la suite de cette analyse, il démontre comment les logiques de l'Etat providence, fondées sur « *un consensus fabriqué* » - la publicité - porté par des « *intérêts privés privilégiés* » (p. 203), donc par une pression du marché capitaliste, a contribué à pervertir l'espace public.

¹²⁶² SENNETT, Op. Cit.

espaces publics issus de la transparence totale. Enfin, couplé à l'analyse de Arendt et de Sofsky, ce mouvement de transparence rend plus prégnant les problèmes et les demandes issus du « social » : sécurité, liberté et consommation¹²⁶³. Ainsi que le note Arnaud Gasnier: « *c'est aussi aujourd'hui toute une partie de la population qui demande un contrôle social plus virulent aux pouvoirs locaux en réclamant par exemple plus de vigiles, un éclairage plus important la nuit ou encore l'enlèvement d'un mobilier urbain faisant l'objet de modes d'appropriation peu désirés par certains acteurs et groupes sociaux, comme si l'imprévisible, la différence, le non maîtrisable n'avaient plus leur place dans nos sociabilités*¹²⁶⁴ ».

573. Quant à la publicisation des espaces privés, les développements précédents ont déjà permis de démontrer les éléments la constituant: normalisation des nouvelles technologies de l'information et de la communication, de leurs usages, marchandisation de la sécurité, banalisation de la surveillance. Ces deux mouvements de publicisation des espaces privés et de privatisation des espaces publics, ainsi que leurs conséquences, passant de la mise en contrôle des espaces à une mise en norme des espaces, permettent à certains auteurs, tels que Jean-Gabriel Ganascia et Elisabeth Pélegrin - Genel, de tirer le constat de la « *mise en scène de la transparence*¹²⁶⁵ » et de tenter

¹²⁶³ Voir SENNETT Richard, Op. Cit. Voir également: PELEGRIN - GENEL Elisabeth, Op. Cit.. Cette dernière écrit par exemple à propos de ce qu'elle appelle les « *espaces dupliqués* » (p. 61): « *Leur slogan pourrait être celui des Holiday Inn dans les années 1970: « la meilleure surprise est l'absence de surprise ». Centres commerciaux, hangars des entrées de ville, fast-food, espaces tertiaires, motels, hôtels, chaîne de boutiques, stations-service, etc., tous ont en commun d'être reproductibles à l'infini. Conséquence naturelle de la mobilité, ils ne peuvent jamais lui échapper. L'espace dupliqué fait penser à la fonction copier:coller de l'ordinateur avec ses aménagements rigoureusement identiques, interchangeable et juxtaposés à la lisière des villes. Chaque entité répond à une fonction précise, sans vision d'ensemble ou souci de l'environnement. Il en découle un effet d'empilement qui témoigne de l'impuissance des politiques de la ville et donne une transcription spatiale et visible de la mondialisation* » (p. 61 - 62). Et de poursuivre: « *En version plus chic, nous avons le centre commercial. Il répond aux besoins d'une époque perpétuellement en mouvement, habitée par le zapping, qui veut être divertie. « Rien n'est fait pour les encourager à s'arrêter, à se regarder, se parler, à réfléchir, à peser le pour ou le contre, à discuter d'autre chose que des objets en vente ! Il ne faut surtout pas qu'ils occupent leur temps à des choses qui n'aient pas de valeur commerciale », explique Zygmunt Bauman* » (p. 65).

¹²⁶⁴ GASNIER Arnaud, *De nouveaux espaces publics urbains ? Entre privatisation des lieux publics et publicisation des lieux privés*, Revue Urbanisme, Publications d'architecture et d'urbanisme, 2006, pp. 70 - 73, (p. 70)

¹²⁶⁵ PELEGRIN - GENEL Elisabeth, Op. Cit, pp. 109 - 138. Cette dernière entame son analyse ainsi: « *« La vie privée, c'est un espace muré, dans lequel il n'est pas permis de chercher à savoir ce qui se passe dans la maison d'un particulier ». C'est la définition que le dictionnaire donnait de la vie privée il y a cent cinquante ans. Elle est tout à fait désuète aujourd'hui. Le slogan de Nokia au début des années 2000: « je n'ai pas une vie professionnelle et une vie privée, je n'ai qu'une vie » résume ce désir d'unifier toutes les facettes de son existence* » (p. 111). On ajoutera à ce début d'analyse, que cet espace muré que le dictionnaire Littré du français ancien de 1863 sur lequel s'appuie l'auteur, doit être entièrement rapproché de l'analyse de Sennett. Que se passe-t-il quand cet espace muré rendu transparent, par la « vitrification du monde » ? La notion de barrière hermétique développé par Sennett ne semble pas pouvoir s'appliquer à la dynamique de la vie privée. Ainsi que le note Pélegrin - Genel dans la conclusion de son analyse de la transparence, « *Le recours aux dispositifs de vidéosurveillance ne pose quasiment plus de problèmes. Nous sommes habitués à circuler dans des espaces surveillés sans en mesurer les conséquences. Le Panopticon de Bentham n'enferme plus stricto sensu, mais se contente de surveiller les comportements, en utilisant des mécanismes explicites visibles (télé, vidéos, radars, badges) ou invisibles, (cartes magnétiques, fichiers informatiques, GPS, balises de téléphone, etc.)* » (p. 138). Il semble possible d'adopter la même logique pour ce qui est de la transparence, devenue le versant contemporain du principe de visibilité intégrale.

d'appréhender l' « *anatomie de la transparence*¹²⁶⁶ » de nos sociétés contemporaines. Ainsi, concluons avec Jean-Gabriel Ganascia que « *téléphone portable, assistant personnel, réseaux de télécommunication planétaires, carte bancaire ... l'électronique change la vie, nous en convenons tous; elle change aussi la ville, elle change le monde, elle change le pouvoir et le mode de gouvernement. Même l'Etat, ce Léviathan, ce monstre artificiel dont Hobbes nous dit qu'avec ses lois et ses procédures, il nous régit pour nous défendre et assurer notre sécurité, offre aujourd'hui, grâce aux technologies de l'information et de la communication, un visage plus avenant, moins obscur, moins impénétrable qu'auparavant. (...). Tout est plus clair, plus propre, plus neuf car plus lumineux, plus coloré, plus brillant et, surtout, plus transparent* »¹²⁶⁷. Et d'alerter avec lui : « *l'examen de ces aspirations à la nouveauté, en particulier à la transparence et à l'égalité parfaite, demande de la prudence, car ce qu'elles annoncent de prétendument neuf pourrait n'être qu'une résurgence d'idéaux anciens*¹²⁶⁸ ». Cette résurgence d'idéaux anciens est pleinement représentée par l'allégorie de la caverne de Platon. Alors que la surveillance diffuse organise et prend en charge la transparence de l'individu, ce dernier croit avoir accès à la connaissance et à la culture, à la liberté. Il est, en réalité, enchaîné à la doxa de la sécurité et de la consommation, et ne verra bientôt plus que l'ombre de sa liberté.

2.La Smart-City comme illustration de la nouvelle fonction du Droit

574. L'élaboration des Smart City s'inscrit pleinement dans l'allégorie de la caverne de Platon. Elle représente à la fois la mise en place d'une logique implacable de transformation totale des espaces sociaux, et l'aboutissement de l'organisation de la transparence totale par le Droit. Dans la poursuite de l'analyse de la transformation des espaces sociaux, il semble nécessaire de mettre en lumière le propos par la compréhension de la nouvelle cité intelligente. La Smart city et les projets d'édification de ces villes éclosent en effet partout dans le monde. De la Corée du Sud et son quartier de Songdo à Tel Aviv en Israël, en passant par Santander en Espagne et Masdar aux Emirats Arabes Unis, ce concept est en plein essor, et sa mise en oeuvre séduit de plus en plus que ce soit pour de grandes agglomérations, ou des villes plus petites.

¹²⁶⁶ GANASCIA Jean-Gabriel, *Voir et pouvoir : qui nous surveille ?*, Editions Le Pommier, Collection Les Essais, 2009, pp. 64 - 74

¹²⁶⁷ Ibid. p. 64 - 65.

¹²⁶⁸ Ibid. p. 74.

575. Cet attrait pour la ville intelligente s'explique en partie par le discours qui entoure son développement. En 2014, Amel Attour et Alain Rallet évoquent les deux conceptions principales berçant le concept de ville intelligente. Cette dernière est selon les auteurs « *définie à travers sa capacité à améliorer la qualité de son territoire par la numérisation de ses activités économiques*¹²⁶⁹ », et / ou par « *la totalisation de plusieurs vertus (l'innovation, la formation, la gouvernance territoriale, le respect de l'environnement, la mobilité et son engagement dans le développement durable) lui attribuant le label « smart », (...), économiquement compétitive, efficacement gérée et agréable à vivre*¹²⁷⁰ ». La CNIL, quant à elle, vient définir cette notion comme suit: « *la ville intelligente est un nouveau concept de développement urbain. Il s'agit d'améliorer la qualité de vie des citoyens en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. Le périmètre couvrant ce nouveau mode de gestion des villes inclut notamment : infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms) ; transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied, etc.) ; les e-services et e-administrations*¹²⁷¹ ». En réalité, ces définitions regroupent un ensemble de caractéristiques visant la gestion d'une ville, et son mode de fonctionnement. On retrouve ici plusieurs éléments développés précédemment: totalisation numérique, outil au service d'une rhétorique utilitariste, de la « *sollicitude de la grande administration ménagère et l'avènement du social*¹²⁷² » dans le public pour reprendre les termes de Hannah Arendt, privatisation de l'espace public. Totalisation numérique, d'une part, puisque ces villes de demain s'appuient sur un ensemble de capteurs et de technologies mises en oeuvre en vue de capter des informations, personnelles ou non, afin d'inscrire la ville dans le progrès, le développement durable, et de permettre plus de mobilité, de gestion de l'espace public, de bonne gouvernance. Outil d'une rhétorique utilitariste et privatisation de l'espace public, d'autre part, puisque ces villes participent d'une forme aboutie de transparence des individus par la captation de données qu'elles emportent. Elle est également l'aboutissement d'une gestion managériale des espaces par la puissance publique.

¹²⁶⁹ ATTOUR Amel, RALLET Alain, « Le rôle des territoires dans le développement des systèmes trans-sectoriels d'innovation locaux : le cas des smart cities », *Innovations*, 2014, Vol. 1, n°43, p. 253-279

¹²⁷⁰ Ibid.

¹²⁷¹ Définition disponible en ligne à l'adresse suivante: <https://www.cnil.fr/fr/definition/smart-city> (dernière consultation: 5 mars 2018)

¹²⁷² Op. Cit.

576. Il faut convenir ici que les projets de smart city emportent différents traitements de données, ayant des conséquences différentes en terme de risque pour la vie privée. L'une des analyses les plus abouties en terme d'étude des inquiétudes des citoyens liées à la vie privée dans ce genre de projet a été réalisé en 2015 par Liesbet van Zoonen¹²⁷³. Le fondement de l'analyse de l'auteur réside en ces questions: quelles données sont collectées ?; sont-elles des données personnelles ou non ?; quels sont les objectifs de cette collecte ? Van Zoonen décrit alors quatre quadrants de collecte de données: la collecte de données personnelles à des fins de service public (traditionnellement collectées par les collectivités), la collecte de données à des fins de surveillance (mission de police, caméras, transports publics, reconnaissance faciale), la collecte de données impersonnelles à des fins de surveillance (gestion des foules, gestion du trafic automobile), la collecte de données impersonnelles à des fins de service public (gestion des déchets, de l'environnement et développement durable, électricité). Loin des dimensions fictionnelles qu'emportent ce genre d'analyse, l'étude de Liesbet Van Zoonen a le mérite de dresser un paysage des inquiétudes liées à la vie privée dans le cadre des projets Smart city. Elle dénonce également les principales problématiques que posent l'édification de la ville intelligente: développement de la datafication pour reprendre les termes de Sadin; réduction de l'individu à une donnée personnelle ou non, une information, une trace; puissance des algorithmes prédictifs; possibilité de ré-identification des individus malgré l'assurance d'une anonymisation¹²⁷⁴ des données de la part des opérateurs, gestion

¹²⁷³ VAN ZOONEN Liesbet, Privacy concerns in smart cities, Op. Cit.

¹²⁷⁴ Mentionnée au considérant 26 de la directive de 1995 et à l'article 32 IV de la Loi de 1978, l'anonymisation est un traitement de données à caractère personnel effectué dans le but d'empêcher toute identification de la personne concernée. Ce procédé doit être irréversible afin d'empêcher toute ré-identification. Lorsque c'est le cas, l'anonymisation permet de « faire sortir les données anonymisées du champ d'application de la législation sur la protection des données ». Toutefois, dans la plupart des cas, le traitement permettant l'anonymisation des données intervient postérieurement à la collecte des données. Le règlement général de protection des données personnelles consacre l'anonymisation en son considérant 26, et bien définir les données anonymes comme « les informations ne concernant pas une personne physique identifiée ou identifiable; les données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. » En réalité, le terme d'anonymisation est souvent utilisé à tort par les entreprises. Le procédé mis en place par ces dernières relève alors beaucoup plus de la pseudonymisation. La pseudonymisation est une technique « visant à remplacer un attribut par un autre dans un enregistrement ». C'est un avis du G 29 (05/2014) sur les Techniques d'anonymisation adopté le 10 avril 2014, qui indique que « la pseudonymisation n'est pas une méthode d'anonymisation » car « le pseudonymat n'est pas de nature à empêcher qu'une personne concernée soit identifiable et reste donc dans le champ d'application du régime juridique de la protection des données » (En ligne: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (dernière consultation: 5 mars 2018)). L'article 4 du RGPD vient donc préciser la définition, en considérant que la pseudonymisation est un « 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 garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ». Sur le mauvais usage des notions d'anonymisation et de pseudonymisation par les entreprises voir: KITCHIN Rob, *Getting smarter about smart cities: Improving data privacy and data security*, Data Protection Unit, Department of the Taoiseach, Dublin, Ireland, 28 Janvier 2016, En ligne: <http://eprints.maynoothuniversity.ie/7242/1/Smart> (dernière consultation: 5 mars 2018)

managériale des villes par la puissance publique. Enfin, dans la poursuite de cette analyse, le grand nombre d'opérateurs tant publics que privés rend les problématiques de consentement au traitement, au contrôle de la donnée, et à la sécurité de cette dernière très complexe. La possibilité de réutilisation des données pour d'autres finalités que celles préalablement envisagées est certes ici pointée du doigt, mais le manque d'information claire permettant un consentement non vicié l'est tout autant. En 2014, Rob Kitchin démontrait les implications des big data dans des projets d'urbanisme intelligent, et s'inquiétait des politiques menées dans ce cadre, de la possibilité d'une gouvernance technocratique en matière de développement urbain et de la corporatisation/privatisation de la gouvernance des villes. Il concluait également sur les verrous technologiques et signalait la possibilité de voir apparaître des villes « *panoptiques, fragiles, piratables du fait des bugs*¹²⁷⁵ » connus ou non de certaines technologies et / ou capteurs¹²⁷⁶.

577. De fait, la Smart city s'inscrit pleinement dans la rhétorique de l'utilitarisme. Elle partage ses objectifs entre la sécurité, la liberté, le développement économique. Elle est alors pleinement au service de la surveillance diffuse, et entre dans l'idéologie de la transparence totale que porte en son sein la surveillance. Visibilité intégrale, transparence, isolement social des « non-connectés », modèle fondé sur l'analyse de flux d'informations, l'interconnexion des données, possibilité de fabriquer le consentement sous prétexte d'un service public fondé sur la donnée permettant le développement durable, le bien-être, la sécurité et la liberté: voici les traits de la Smart city mis au jour par la surveillance diffuse et la modification du contrôle social qu'elle emporte. En réalité, l'ensemble de cette démonstration liée particulièrement à la Smart City, repose sur ce que nombre d'auteurs¹²⁷⁷ dénoncent quant à la transformation des modalités d'exercice du pouvoir, passant d'une biopolitique à un biopouvoir algorithmique.

¹²⁷⁵ KITCHIN Rob, *The real-time city? Big data and smart urbanism*, GeoJournal, 2014, 79:1 - 14, p. 1, En ligne: <https://pdfs.semanticscholar.org/6e73/7a0e5ef29303760a565ba5e9d98510ab0976.pdf> (dernière consultation: 5 mars 2018)

¹²⁷⁶ Sur les verrous technologiques, et spécialement sur les possibilités de piratages des objets smart, voir: MICHEL Claude, *Un hacker réussit à contourner la sécurité d'une arme à feu intelligente - Et déclencher un tir sans autorisation*, 31 Juillet 2017, En ligne: <https://www.developpez.com/actu/152306/Un-hacker-reussit-a-contourner-la-securite-d-une-arme-a-feu-intelligente-et-declencher-un-tir-sans-autorisation/> (dernière consultation: 5 mars 2018)

¹²⁷⁷ Op. cit.

Section 2: La consécration de la prise en compte par le Droit des objectifs du libéralisme exalté par la surveillance diffuse

578. Les effets de la mutation du pouvoir par la surveillance diffuse sur le Droit sont multiples. Ils résident d'abord dans la modification et l'élaboration lente d'un Droit, d'une philosophie du Droit correspondant à la philosophie du néo-libéralisme à l'oeuvre dans nos sociétés contemporaines. La rhétorique de l'utilitarisme appliquée à la surveillance diffuse, au biopouvoir algorithmique, et l'unité du libéralisme (économique, culturel et politique) ont engendré des effets et des conséquences sur le Droit (Paragraphe 1). Loin de le désinstituer pleinement, la surveillance diffuse semble modifier progressivement le Droit. Pour certains auteurs, tels que Tim O'Reilly¹²⁷⁸, Henri Verdier¹²⁷⁹, ou encore Evgeny Morozov¹²⁸⁰, il faudrait évoquer une controverse fondamentale à l'oeuvre actuellement concernant l'émergence d'une « réglementation algorithmique », traduction contemporaine des mots de Thoreau: « *le gouvernement le meilleur est celui qui gouverne le moins*¹²⁸¹ ». Il serait pourtant préférable, ainsi que le soulignent Morozov, ou de manière plus insidieuse Antoinette Rouvroy¹²⁸² et Bernard Stiegler¹²⁸³, d'alerter quant aux conséquences réellement néfastes de ce programme politique réduit à la technologie, et d'écrire avec Morozov qu'il est aberrant de croire en « un solutionnisme technologique¹²⁸⁴ » intégral (Paragraphe 2).

¹²⁷⁸ O'REILLY Tim, « Open Data and Algorithmic Regulation, in. GOLDSTEIN Brett, DYSON Lauren (éds.), *Beyond Transparency - Open Data and the Future Civic Innovation*, Code for America Press, San Francisco, 2013, pp. 289 - 300, En ligne: <http://beyondtransparency.org/pdf/BeyondTransparency.pdf> (dernière consultation: 5 mars 2018)

¹²⁷⁹ VERDIER Henri, *Gouvernement des algorithmes: une contribution au débat*, 27 octobre 2014, En ligne: <http://www.henriverdier.com/2014/10/gouvernement-des-algorithmes-whats-next.html> (dernière consultation: 5 mars 2018)

¹²⁸⁰ MOROZOV Evgeny, « The rise of data and the death of politics », *The Guardian*, 20 juillet 2014, En ligne: <https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation> (dernière consultation: 5 mars 2018), ou pour une traduction: « La prise de pouvoir des données et la mort de la politique », article paru dans *The Guardian*, 20 juillet 2014, traduit par Guy Weet et republié par Paul Jorion, En ligne: <http://www.pauljorion.com/blog/2014/08/25/la-prise-de-pouvoir-par-les-donnees-et-la-mort-de-la-politique-par-evgeny-morozov/> (dernière consultation: 5 mars 2018)

¹²⁸¹ THOREAU Henry-David, *La désobéissance civile*, Culture Commune, 2014, p. 1.

¹²⁸² Voir en ce sens: ROUVROY Antoinette, « Quand les algorithmes décident à notre place », *Libération*, 10 avril 2014, En ligne: http://www.liberation.fr/evenements-libe/2014/04/10/quand-les-algorithmes-decident-a-notre-place_994175 (dernière consultation: 5 mars 2018), ou encore ROUVROY Antoinette, Berns Thomas, Op. Cit.

¹²⁸³ ROUVROY Antoinette, STIEGLER Bernard, Séminaire Digital Studies, Deuxième Séance, Institut de recherche et d'innovation, Paris, 7 octobre 2014, Compte rendu disponible en ligne à l'adresse suivante: <https://digital-studies.org/wp/seminaire-digital-studies-antoinette-rouvroy-et-bernard-stiegler-paris-07102014/?lang=fr> (dernière consultation: 5 mars 2018)

¹²⁸⁴ MOROZOV Evgeny, *L'aberration du solutionnisme technologique - Pour tout comprendre cliquez ici*, Editions FYP, Collection Innovation, 2014

Paragraphe 1: La surveillance diffuse, le libéralisme, le biopouvoir algorithmique et l'élaboration d'un « Droit libéral »

579. Le biopouvoir algorithmique est donc la technique de pouvoir choisie actuellement pour réguler la vie en société, permettre le bien-être, la sécurité et la liberté, principalement réduite à son versant économique (la consommation). Cette technique de pouvoir tire sa force de la datafication, la mise en données de nos environnements, nos espaces, nos activités, et même de nos propres individualités. Sous prétexte de « smartification » de la vie même, les individus sont prêts à s'insérer dans ce monde de données (personnelles ou non). La surveillance diffuse est le principal dispositif permettant d'atteindre les objectifs précités. Car, en effet, c'est bien au travers de la surveillance diffuse et des techniques algorithmiques, que la masse de données collectées peut être effectivement traitée, et produire un résultat analysable. L'élaboration d'un Droit libéral (B) est fonction de la philosophie prônée par le libéralisme économique, culturel et politique (A).

A. Des interactions entre le Droit et l'ambition du libéralisme à créer une « tyrannie du Bien »

580. La surveillance diffuse obtient sa plénitude d'action et déploie ses traits caractéristiques tels que Jacques Ellul les avait énoncés: « *automatisme du choix technique, auto-accroissement, unicité ou insécabilité, entraînement des techniques, universalisme technique et autonomie de la technique*¹²⁸⁵ ». Rappelons également que pour Ellul, la technique correspond à la philosophie du « *the one best way*¹²⁸⁶ », qu'il met en lumière par les propos suivants: « *lorsque tout a été mesuré, calculé, que la méthode déterminée est, au point de vue intellectuel, satisfaisante, et qu'au point de vue pratique elle se révèle efficiente, plus efficiente que tous les autres moyens employés jusqu'ici ou mis en concurrence au même moment, la direction technique se fait d'elle-même*¹²⁸⁷ ».

581. Cette description de la motivation technique donnée par Ellul, c'est-à-dire de la recherche de la méthode la plus efficace, est exactement ce que représente aujourd'hui la surveillance diffuse aidée par la puissance algorithmique, le pouvoir algorithmique. Selon Jean-Claude Michéa, ce

¹²⁸⁵ ELLUL Jacques, *La Technique ou l'enjeu du siècle*, Op. Cit. pp. 74 - 134

¹²⁸⁶ ELLUL Jacques, *Ibid.* p. 74.

¹²⁸⁷ *Ibid.*

phénomène est permis par l'unité du néo-libéralisme, regroupant politique, culture et économie¹²⁸⁸, qui contribue à créer un « *empire du moindre mal*¹²⁸⁹ ». Il définit cet « *empire du moindre mal* » dès l'introduction de son livre comme suit: « *Winston Churchill disait de la démocratie qu'elle était le pire des régimes « à l'exception de tous les autres ». Il serait difficile de trouver une formule plus appropriée de l'esprit libéral. Autant ce dernier, en effet, manifeste un optimisme sans faille quant à la capacité des hommes de se rendre « maîtres et possesseurs de la nature », autant il fait preuve d'un pessimisme profond dès qu'il s'agit d'apprécier leur aptitude morale à édifier par eux-mêmes un monde décent. Comme on le verra plus loin, ce pessimisme trouve son origine dans l'idée, éminemment moderne, selon laquelle c'est précisément la tentation d'instituer, ici-bas, le règne du Bien et de la Vertu, qui constitue la source ultime de tous les maux qui n'ont cessé d'accabler le genre humain. Cette critique de la « tyrannie du Bien » a, naturellement, un prix. Elle oblige à considérer la politique moderne comme un art purement négatif: celui de définir, en somme la moins mauvaise société possible. C'est en ce sens que le libéralisme doit être compris et se comprend lui-même, comme la politique du moindre mal* ». Par l'imprégnation dans nos sociétés des idéologies sécuritaires, d'un droit potentiel à la sécurité, de la promotion du bien-être, et la liberté de consommation; la protection, la direction, l'influence et la gestion des activités des individus ont été rendu possibles, et, par là, une douce légitimation de la surveillance diffuse.

582. Alors qu'auparavant l'évocation de la surveillance faisait ressortir les traits les plus sombres de l'Histoire (totalitarisme par exemple), ou, s'assimilait à une technique d'exception, la surveillance est aujourd'hui pleinement légitimée. Elle est même devenue l'un des traits caractéristiques de la culture de nos sociétés en crise. L'idéologie de l'empire du moindre mal mise au jour par Jean-Claude Michéa se cache derrière les préoccupations de la surveillance diffuse. Et comme le démontre le Professeur Michéa, le Droit qui s'inscrit dans l'unité du libéralisme, joue, lui aussi un rôle prépondérant.

¹²⁸⁸ MICHEA Jean-Claude, *L'empire du moindre mal - Essai sur la civilisation libérale*, Editions Flammarion, Collection Champs Essai, 2010. Voir spécialement le chapitre 1 de cet ouvrage (pp. 11 - 62). Michéa écrit: « *il ne fait guère de doute que si Adam Smith ou Benjamin Constant revenaient parmi nous (...), ils éprouveraient les plus grandes difficultés à reconnaître la rose de leur libéralisme dans la croix du présent. De là, sous doute, l'incroyable confusion intellectuelle qui règne à présent sans partage quant à l'usage de ce mot. Il conviendrait ainsi, pour beaucoup, de distinguer un « bon » libéralisme politique et culturel et un « mauvais » libéralisme économique; et la critique de ce dernier devrait elle-même être nuancée selon qu'on aurait affaire à un « vrai » libéralisme, à un « néo-libéralisme » ou à un « ultra-libéralisme ».* La thèse que j'entends défendre ici a au moins le mérite de simplifier la question. Je soutiens, en effet, que le mouvement historique qui transforme en profondeur les sociétés modernes doit être fondamentalement compris comme l'accomplissement logique (ou la vérité) du projet philosophique libéral, tel qu'il s'est progressivement défini depuis le XVII^e ème siècle, et, tout particulièrement, depuis la philosophie des Lumières. Cela revient à dire que le monde sans âme du capitalisme contemporain constitue la seule forme historique sous laquelle cette doctrine libérale originelle pouvait se réaliser dans les faits ». (p. 11 - 12).

¹²⁸⁹ Ibid.

B. La consécration d'un Droit Libéral

583. Le Droit Libéral est un instrument au service de la surveillance diffuse, en ce qu'il cherche à parvenir à une forme de méthode la plus efficace pour vivre en société, le « one best-way » décrit par Ellul. Pour l'écrire autrement, par la recherche de la meilleure efficacité en toutes choses, du bien et de la vertu fondés aujourd'hui sur la consommation, la sécurité et le bien-être, le Droit libéral est au service de l'empire du moindre mal décrit par Michéa, et permet de faire passer la surveillance diffuse, le biopouvoir algorithmique, du « souriez, vous êtes filmés » au « souriez, vous êtes gérés ». Perte du sens du droit au profit de la norme qu'est devenue la surveillance diffuse, mise en cause de l'Etat de droit, des idéaux démocratiques au profit de la République et de la Nation sont autant d'éléments sous-tendus par la surveillance diffuse, le nouveau pouvoir algorithmique. Tout se passe aujourd'hui comme si le Droit était réduit à un calcul d'utilité d'où il tire sa source et sa force.

584. Le Droit légitime le recours à la surveillance sous prétexte d'un besoin de sécurité, véhiculé par une gouvernementalité par la peur. Ainsi que Friederich Hegel¹²⁹⁰ le déclarait, « *lorsque quelqu'un marche dans la rue en pleine nuit sans danger, il ne lui vient pas à l'esprit qu'il pourrait en être autrement ; car l'habitude d'être en sécurité est devenue pour nous une seconde nature et l'on ne se rend pas compte que cette sécurité est uniquement le résultat d'institutions particulières. La représentation s' imagine souvent que c'est la force qui assure la cohésion de l'Etat; mais ce qui maintient l'Etat, c'est uniquement le sentiment de l'ordre, partagé par tous*¹²⁹¹ ».

585. Selon cette analyse, l'Etat n'a pas besoin de montrer sa force, son pouvoir de violence légitime, mais simplement de compter sur le sentiment de sécurité, de faire que les citoyens aient la conviction immédiate et irréfléchie qu'ils sont en sécurité, qu'ils n'encourent aucun risque. La surveillance diffuse, et les idéologies qu'elle véhicule, sont le principal outil pour parvenir à cette croyance impénétrable. Le Droit fait également partie de ces « *institutions particulières* » décrites par Hegel. A ce titre, Jean-Claude Michéa écrit ainsi que « *l'axiome de base du libéralisme politique*

¹²⁹⁰ Friedrich Hegel (1770-1831), philosophe allemand. Établissant l'identité du réel et du rationnel, il affirme que la raison et donc l'humanité se réalise progressivement dans l'histoire : derrière l'agitation des passions humaines existe un sens caché de l'histoire tout entière tournée vers la réalisation de l'esprit

¹²⁹¹ HEGEL Friedrich, *Principes de la philosophie du droit*, traduit par R. Derathé, Paris, Vrin, 1986, additif n°268, p. 270

est bien connu. Si la prétention de certains individus (ou associations d'individus, à l'image de l'Eglise) à détenir la vérité sur le Bien est la cause fondamentale qui porte les hommes à s'affronter violemment, alors les membres d'une société ne pourront vivre en paix les uns avec les autres que si le Pouvoir chargé d'organiser leur coexistence est philosophiquement neutre, c'est-à-dire s'il s'abstient, par principe d'imposer aux individus telle ou telle conception de la vie bonne. Dans une société libérale chacun est donc libre d'adopter le style de vie qu'il juge le plus approprié à sa conception du devoir (s'il en a une) ou du bonheur; sous la seule et unique réserve, naturellement, que ses choix soient compatibles avec les libertés correspondantes des autres¹²⁹² ». En deçà de l'évocation du bonheur que le pouvoir doit s'abstenir d'organiser, on retrouve ici la rhétorique de l'utilitarisme précédemment évoqué, où l'individu est comparé à une petite machine économique qui cherche à maximiser son bien-être, et son bonheur. Jean-Claude Michéa poursuit son analyse par l'idée de « la présence - au dessus des individus engagés séparément dans leur recherche de la vie bonne et du bonheur - d'une instance chargée d'harmoniser les libertés à présent concurrentes, et seule fondée, à ce titre, à en limiter le champ d'action en définissant un certain nombre de règles communes. Cette instance est le Droit (dont l'Etat, dans cette optique, n'a plus pour fonction essentielle que de garantir l'application effective)¹²⁹³ ». Pour l'auteur, il faut alors noter un déplacement progressif de l'ambition du Droit passant de « la primauté du Juste sur le Bien¹²⁹⁴ », à une « théorie de l'ajustage ou de l'ajustement. Pour l'essentiel, en effet, il s'agit seulement de mettre au point les combinaisons institutionnelles les plus efficaces, donc de calculer au plus juste le système de poids et contrepoids (checks and balance, disent les philosophes anglo-saxons) qui permettra de maintenir l'équilibre des libertés rivales en leur imposant le minimum d'exigences- en leur garantissant, si l'on préfère, le taux d'imposition essentielle le plus bas possible¹²⁹⁵ ».

586. A travers l'analyse du Professeur Michéa, couplée à l'étude de la rhétorique de l'utilitarisme, il semble que l'Etat lui-même devienne cette petite machine économique décrite par Laval. A tout le moins, il passe bien du gouvernement des hommes à l'administration des choses décrite par Saint-Simon, et de fait, devient un gestionnaire des risques, des menaces, de la

¹²⁹² MICHEA Jean-Claude, Op. Cit, p. 34.

¹²⁹³ Ibid.

¹²⁹⁴ Ibid. p. 35

¹²⁹⁵ Ibid. p. 35 - 36. Michéa écrit : « La théorie de la Justice sur laquelle se fonde la nouvelle autorité du Droit a, en réalité, peu de chose à voir avec ce que la philosophie traditionnelle avait jusqu'alors pensé sous ce nom. Elle ne se soucie plus, en effet, de définir des Idées ou de saisir des Essences, c'est-à-dire de s'exprimer au nom d'une quelconque « Vérité », quel que soit le statut métaphysique de cette dernière. Bien plus que d'une « théorie de la Justice », il conviendrait plutôt de parler à son sujet d'une théorie de l'ajustage ou de l'ajustement ». (p. 35)

sécurité¹²⁹⁶. S'ensuit donc « *la pente logique (...) de s'engager progressivement dans la voie d'une régularisation massive de tous les comportements possibles et imaginables*¹²⁹⁷ ». Ces mots font étrangement écho aux différentes politiques gouvernementales mises en oeuvre ces dernières années. Qu'il s'agisse de l'exhortation du gouvernement, aidé par la technique, à manger-bouger, ou encore de l'interdiction de fumer dans les lieux publics, de la mise en place des Smart-city sous couvert de développement durable et d'innovation, de l'usage des compteurs Linky, on assiste bien là à la régularisation massive de tous les comportements pouvant potentiellement être saisis par le Droit libéral.

587. Jean-Claude Michéa note ainsi que « *aujourd'hui, donc, l'interdiction du tabac; demain, peut être, la légalisation des drogues et, probablement, dans un avenir très proche, les deux en même temps. Certes le climat étrange qui s'installe alors, à la faveur de ces croisades juridiques toujours plus nombreuses (plaisirs troubles de la délation, surveillance généralisée des uns par les autres, multiplication, du coup inéluctable, des censures, des contrôles et des interdits), semble aux antipodes de ce monde paisible et tolérant dont rêvaient les fondateurs du libéralisme: (...) Montesquieu, Constant ou Tocqueville. (...) Mais c'est, toutefois, au nom de leur théorie du Droit et de la Liberté, que ce besoin forcené de légaliser, d'exclure et d'interdire se développe à présent sans limites. A partir du moment où l'Etat libéral se veut, selon l'expression de Pierre Manent, « le scepticisme devenu institution » il n'existe, à son niveau, aucun pare-feu institutionnel cohérent qui puisse prévenir le démontage méthodique de ce qu'Orwell appelait la common decency; ni même cela va de soi, du simple bon sens*¹²⁹⁸ ». La traduction de ces mots se retrouve parfaitement dans la proposition de Règlement de 2017 de la Commission européenne concernant la libre circulation des données non personnelles. En effet, au-delà de son lien avec le marché économique - la libre

¹²⁹⁶ Citant Emmanuel Kant, Michéa va même plus loin en déclarant: « *De ce point de vue, personne n'a, sans doute, mieux formulé cet idéal de neutralité axiologique absolue, qui est au coeur de tout projet libéral, que Emmanuel Kant, lorsqu'il note dans son « Projet de paix perpétuelle », que dans l'hypothèse d'un travail législatif parfait, la seule mécanique du Droit suffirait à assurer la coexistence pacifique même d'un peuple de démons* ». (p. 37)

¹²⁹⁷ Michéa écrit: « *Aucun des premiers libéraux n'aurait célébré comme le terme logique de la liberté l'avènement d'un « peuple de démons ». Le problème c'est que rien, dans la logique du libéralisme politique, ne protège ce dernier contre une telle éventualité. L'autorité du Droit libéral n'est, en effet, légitime, on l'a vu que parce qu'elle se borne à arbitrer le mouvement brownien des libertés concurrentes, sans jamais faire appel à d'autres critères que les exigences de la liberté elle-même; lesquelles se résument, pour l'essentiel, à la seule nécessité de ne pas nuire à autrui. (...) Devant ces questions, multipliables à l'infini, le Droit libéral est obligatoirement en grande difficulté. Si, par hypothèse, il doit s'interdire, pour motiver ses arbitrages, de prendre appui sur des conceptions métaphysiques particulières (par exemple sur une conception déterminée du salut de l'âme, de la décence commune de la dignité humaine), il est, en effet, inévitable, du fait de l'évolution perpétuelle des moeurs (processus que les Modernes s'accordent unanimement à juger « naturel ») qu'il se retrouve confronté à un nombre croissant de « problèmes de société », manifestement impossibles à résoudre de façon cohérente dans le cadre strictement technique qu'il s'est lui-même imparti* ». (pp. 37 - 39)

¹²⁹⁸ Ibid. p. 42 -43.

circulation dans un marché de la donnée des informations - ce projet de règlement, encore en discussion, pourrait prévoir une possibilité pour les autorités compétentes d'accéder aux données non personnelles stockées en Europe mais également par tous les services de cloud computing hors Union européenne en cas d'enquête, ou de suspicion de crimes ou de délits. Selon la Commissaire européenne à la Justice, Vera Jourova, cette possibilité ne sera envisageable qu'à condition de réciprocité avec le gouvernement américain¹²⁹⁹. Alors que le juge européen n'a eu de cesse de se positionner contre la surveillance de masse, ce texte, en tant que véritable traduction d'un Droit libéral, réactive cette problématique.

Paragraphe 2: De la « réglementation algorithmique » à « l'aberration du solutionnisme technologique » : la consécration d'un Etat de Droit Libéral ou la promotion du laissez-faire juridique

588. Le point de départ de cette analyse est d'opérer par effet miroir avec les intentionnalités technophiles et technophobiques citées précédemment. Leurs analyses, dès le départ de cette étude, a permis de comprendre la surveillance diffuse comme un phénomène social et économique. Elle est également, par la prégnance de certains de ces discours, un phénomène juridique à part entière. Ainsi que le note Evgeny Morozov en 2014, *« lorsque nous nous serons affranchis des histoires héroïques, mais insipides que les technologues racontent aux non-initiés pour présenter leur travail, alors pourrions-nous probablement mieux saisir le fonctionnement interne des technologies, leur impact civique ainsi que la manière de les réformer, de les réguler. La rhétorique de Google constitue elle-même un bon sujet d'enquête et pas uniquement du fait de ses références constantes aux miroirs et autres reflets. Google aime en outre invoquer des termes nobles comme la « démocratie » afin de montrer que ce qui est calculé par ses algorithmes n'est pas seulement objectif mais également juste¹³⁰⁰ ».*

589. Les prémices de cette recherche ont permis de s'affranchir quelque peu des discours des technologues. La démonstration qui précède a permis de mettre au jour un nivellement du Droit et

¹²⁹⁹ En ce sens, voir: CHAR Pravin, *Europe seeks power to seize overseas data in challenge to tech giants*, 26 février 2018, Reuters, Disponible en ligne à l'adresse suivante: https://www.reuters.com/article/us-eu-data-order/europe-seeks-power-to-seize-overseas-data-in-challenge-to-tech-giants-idUSKCN1GA0LP?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29 (dernière consultation: 5 mars 2018)

¹³⁰⁰ MOROZOV Evgeny, *L'aberration du solutionnisme technologique - Pour tout comprendre cliquez ici*, Editions FYP, Collection Innovation, 2014, p. 151.

des Libertés par le bas, sous couvert de l'idéologie libérale, et l'élaboration d'un empire du moindre mal. Il faut ici aller un peu plus loin et tentait de donner quelques éléments de définition de cette réglementation algorithmique (A) car cet avenir juridique possible présente des risques (B).

A. De la réalité possible de la réglementation algorithmique

590. La réglementation algorithmique semble être le pendant contemporain des mots de Thoreau: un gouvernement qui gouverne le moins possible du fait même de la surveillance diffuse. Cette définition mérite quelques développements (1). La réglementation algorithmique trouve une traduction dans l'élaboration contemporaine d'un Etat de Droit entièrement tourné vers le capitalisme (2).

1. Tentative de définition de la réglementation algorithmique

591. En 1996, le doyen Carbonnier questionnait la digitalisation et ses conséquences sur le métier du juriste. Il déclarait à cet égard que « *l'informatique en perfectionnant les fichiers a contribué à faire de la jurisprudence un automatisme¹³⁰¹* ». Et d'ajouter que « *en permettant la fondation commerciale de banques de données, elle a bouleversé l'usage et peut-être le contenu de l'oeuvre jurisprudentielle : le praticien ne se livre plus à la recherche artisanale d'arrêts, il achète l'état de la jurisprudence, mais un état établi à travers des mots-clés, dont l'effet réducteur ne peut être éliminé¹³⁰²* ». L'informatique aide à la maîtrise de la connaissance du juriste et donne alors au droit une sorte d'efficacité. Alors qu'il présentait les logiques que sous-tendent l'informatisation de la société, Jean Carbonnier écrit que « *par le gigantisme de ses moyens, l'informatique est capable de saisir des phénomènes de masse à l'action dans les juridictions. (...). Et en les rendant quantitativement visibles, elle leur confère une nouvelle force d'attraction. (...) nous sommes ainsi de plus en plus informés, sauf à nous demander si le flux de l'information n'étrangle pas la connaissance¹³⁰³* ». Sans revenir sur l'analyse de l'informatisation de la société, les arguments de Jean Carbonnier quant à la lecture du Droit par le juriste laissent ses contemporains dans la crainte de ce que peut créer la surveillance diffuse. La possible réglementation algorithmique qu'elle développe se situe en effet dans le prolongement de l'analyse de Carbonnier.

¹³⁰¹ CARBONNIER Jean, *Droit et passion du droit sous la Vème République*, Champs Flammarion, 1996, p. 60

¹³⁰² Ibid.

¹³⁰³ Ibid.

592. Tim O'Reilly, éditeur, capital-risqueur et technophile¹³⁰⁴, dès 2013, élaboré le concept de « réglementation algorithmique¹³⁰⁵ ». Selon lui, « *la réglementation est le croque-mitaine de la politique contemporaine. Nous en avons trop dans la plupart des domaines, nous en avons trop peu dans d'autres, mais surtout, nous n'avons que peu de capacité pour les ajuster lorsque nous en découvrons les résultats inévitables et inattendus*¹³⁰⁶ ». Prenant appui sur des exemples technologiques « smart », il décrit la réglementation algorithmique comme celle qui permet « *une compréhension approfondie du résultat souhaité, la mesure en temps réel du résultat atteint ou non, les algorithmes (c'est-à-dire un ensemble de règles) qui font des ajustements basés sur de nouvelles données, une analyse périodique et approfondie du fonctionnement correct et attendu des algorithmes en question*¹³⁰⁷ ». Pour O'Reilly, la réglementation algorithmique permettrait de se concentrer sur les principaux problèmes de société (sécurité, santé, justice). Elle rendrait alors l'Etat plus performant, plus efficace car rationalisé dans son action et sa prise de décision par la donnée, l'analyse prédictive et comportementale.

593. Dénonçant la réglementation algorithmique prônée par O'Reilly, en s'appuyant sur la « smartification » de la vie quotidienne, Morozov écrit ironiquement « *en plus de rendre nos vies plus efficaces, ce monde intelligent nous met devant un choix politique intéressant. Si tant d'éléments de notre comportement quotidien sont déjà capturés, analysés, pourquoi s'en tenir à des approches non-empiriques de la réglementation? Pourquoi s'appuyer sur les lois quand on a des capteurs et des mécanismes de rétroaction?(...) Ce nouveau type de gouvernance a un nom: la réglementation algorithmique*¹³⁰⁸ ». Des éléments de cette réglementation algorithmique peuvent

¹³⁰⁴ Il popularise le concept du Web 2.0, mais également celui de « government as a platform », une conception de l'Etat conçu comme une plateforme (numérique), visant à améliorer son efficacité.

¹³⁰⁵ O'Reilly Tim, « Open Data and Algorithmic Regulation, in. GOLDSTEIN Brett, DYSON Lauren (éds.), *Beyond Transparency - Open Data and the Future Civic Innovation*, Op. Cit., pp. 289 - 300

¹³⁰⁶ Ibid. p. 289, traduction libre de : « *Regulation is the bugaboo of today's politics. We have too much of it in most areas, we have too little of it in others, but mostly, we just have little ability to adjust the rules or the processes when we discover the inevitable unintended results* »

¹³⁰⁷ Ibid. p. 289 - 290. Traduction libre de : « *1. A deep understanding of the desired outcome; 2. Real-time measurement to determine if that outcome is being achieved; 3. Algorithms (i.e. a set of rules) that make adjustments based on new data; 4. Periodic, deeper analysis of whether the algorithms themselves are correct and performing as expected* ».

¹³⁰⁸ MOROZOV Evgeny, « The rise of data and the death of politics », *Op. Cit.*

déjà apparaître sous couvert de l'uberisation du droit¹³⁰⁹, ou encore de l'uberisation de l'Etat, c'est-à-dire la réduction du travail du juriste à une plateforme, ou encore de l'art de gouverner par plateforme¹³¹⁰. Règlements algorithmique et uberisation du droit sont en réalité les faces d'une même médaille que la surveillance diffuse a permis de créer sous couvert d'une libéralisation d'un marché économique. Déréglementation successive, mutilation du service public, imposition du choix technologique sont autant de phénomènes qu'engendrent l'uberisation du monde et la réglementation algorithmique¹³¹¹. Dans un cadre plus pratique, on pourrait également citer ici les différentes mesures techniques de lutte contre la fraude fiscale aidées par le data mining ou les algorithmes¹³¹². L'ambition sous-jacente au concept de réglementation algorithmique est alors de rendre l'application des lois existantes plus efficaces, et spécialement concernant des sujets de lutte contre la fraude de rationaliser encore un peu plus l'action (économique) de l'Etat, de transformer l'Etat en un manager d'entreprise, un gestionnaire.

¹³⁰⁹ Voir en ce sens: LARRIERE Stéphane, « Uberisation du droit... et ainsi naquit le juriste digital », *Les Affiches Parisiennes*, 15 avril 2016, En ligne: <http://www.affiches-parisiennes.com/uberisation-du-droit-et-ainsi-naquit-le-juriste-digital-6177.html> (dernière consultation: 5 mars 2018). Le directeur juridique d'Atos International écrit ainsi que: « *Après, les libraires, les hôteliers, les chauffeurs de taxi, on fantasme, on glose, on se dit que les juristes pourraient compter parmi les prochaines professions victimes du phénomène schumpétérien de « destruction créatrice » (Capitalisme, socialisme et démocratie, Joseph Schumpeter, Payot), causé par l'apparition d'une application, d'une plateforme ou encore d'un logiciel. (...). Durée interminable hors du temps, monstrueuse réglementation, kafkaïenne justice, dont se dégagent l'individu et l'entreprise grâce à l'essentiel juriste expert qui décrypte et libère l'action à venir (cf. La Loi des Parties, Juriste d'entreprise, qui es-tu ?). La pression de ce droit qui infuse et se diffuse semble créer un besoin de droit chez l'individu qu'il ne peut étancher que par le recours aux juristes, leur assurant ainsi, de confortables jours, que certains, jaloux, qualifient encore de « rente ». Ouf ! Protégé par tous les droits, par son omniscience, le juriste ne semble pas pouvoir être la victime de la destruction créatrice que porte la digitalisation.* ».

¹³¹⁰ O'Reilly, Op. Cit. Voir également: MOROZOV Evgeny, *Noces du Numérique et de l'austérité - Résister à l'uberisation du monde*, Le Monde Diplomatique, Septembre 2015, pp. 1 et 22, En ligne: <https://www.monde-diplomatique.fr/2015/09/MOROZOV/53676> (dernière consultation: 5 mars 2018). Dans cet article, Morozov pose une question essentielle: « *En transformant des particuliers possédant un véhicule en chauffeurs occasionnels sans statut, la société Uber n'a pas seulement suscité la fureur des taxis professionnels : son nom symbolise désormais le lien entre nouvelles technologies et précarisation.?* ».

¹³¹¹ Dans l'article précité, Morozov écrit: « *Le problème est que les villes qui font ami-ami avec Uber risquent de développer une dépendance excessive à ses flux de données. Pourquoi accepter que l'entreprise devienne l'intermédiaire unique en la matière ? Au lieu de la laisser aspirer la totalité des informations relatives aux déplacements, les villes devraient chercher à obtenir ces données par leurs propres moyens. Ensuite, elles pourraient autoriser les entreprises à les utiliser pour implanter leur service. (...). Il ne s'agit pas de prôner un renforcement de la surveillance, mais simplement de souligner qu'Uber se prétend propriétaire de données qui ne lui appartiennent pas* ». Le cas d'Uber qui se prétend propriétaire des données qui ne lui appartiennent pas s'appliquent également pour Google, Facebook ou Amazon. Le fétichisme de ces entreprises envers le choix technologique, et son imposition, conduit à des situations aberrantes de dépendance des villes, des individus, des Etats aux services qu'elles proposent.

¹³¹² Voir en ce sens: « *Bercy : du « data mining » pour lutter contre la fraude fiscale des entreprises* », 2014, En ligne: http://m.lesechos.fr/redirect_article.php?id=021365257320&fw=1 (dernière consultation: 5 mars 2018), NIEDERCORN Frank, « *les algorithmes, pour le meilleur ou le pire* », Les Echos, 10 Mai 2016, En ligne: https://www.lesechos.fr/10/05/2016/LesEchos/22188-045-ECH_les-algorithmes--pour-le-meilleur-ou-le-pire.htm (dernière consultation: 5 mars 2018), et Conseil Général de l'économie, de l'industrie, de l'énergie et des technologies, *Rapport à Madame la Secrétaire d'Etat chargée du Numérique concernant les modalités de régulation des algorithmes de traitement des contenus*, 13 mai 2016, En ligne: [https://www.economie.gouv.fr/files/directions_services/cge/Rapports/2016_05_13_Rapport_Algorithmes\(1\).pdf](https://www.economie.gouv.fr/files/directions_services/cge/Rapports/2016_05_13_Rapport_Algorithmes(1).pdf) (dernière consultation: 5 mars 2018)

594. Dans la conclusion de son article concernant *la prise de pouvoir des données et la mort de la politique*, Evgeny Morozov met en garde contre ce type de réglementation. Il écrit ainsi fort justement: « *il faut dire au crédit de MacBride, qu'il avait tout compris en 1967: « compte tenu des ressources technologiques et techniques de planification moderne », a-t-il averti, « ce n'est vraiment pas très compliqué de transformer même un pays comme le nôtre en une entreprise où le bon fonctionnement de tous les détails de la vie est une fonction mécanique prise en charge ». La crainte de MacBride est devenue le plan directeur de O' Reilly: le gouvernement, écrit-il, devrait être calqué sur l'approche « lean startup » de la Silicon Valley, qui « en utilisant les données produites révisé constamment et affine son approche du marché ». (...). La réglementation algorithmique, quelles que soient ses avantages immédiats, produira un régime politique où les entreprises de technologie et les bureaucrates du gouvernement décident de tout. L'auteur polonais de science-fiction Stanislaw Lem, dans une critique bien vue de la cybernétique, publiée à peu près en même temps que l'Etat automatisé, écrivait: « la société ne peut pas se débarrasser du fardeau d'avoir à décider de son propre sort en sacrifiant cette liberté au bénéfice du régulateur cybernétique¹³¹³ ».*

2. Réalisme de la réglementation algorithmique à travers l'Etat de Droit libéral

595. A partir des travaux de Hannah Arendt et de Antonio Gramsci, André Tosel¹³¹⁴ s'interroge sur la capacité d'assimilation de la société moderne. Ses conclusions sont particulièrement éclairantes quant à la réalité de l'Etat de Droit propre au capitalisme, et participent d'une grille d'analyse intéressante pour la compréhension d'une réglementation algorithmique en construction. Ainsi écrit-il que les sociétés capitalistes démocratiques portent en elles un conformisme de masse. Le principal problème de la reconnaissance d'un Etat de Droit libéral, que la surveillance diffuse a participé à créer, est parfaitement résumé en ces mots.

596. S'appuyant sur les mots de Gramsci, André Tosel écrit que « *La révolution introduite par la classe bourgeoise dans la conception du droit et donc dans la formation de l'État consiste spécifiquement dans la volonté de conformisme (donc éthicité du droit et de l'État). (...). L'État*

¹³¹³ MOROZOV Evgeny, « The rise of data and the death of politics », *Op. Cit.*

¹³¹⁴ TOSEL André, « Libres réflexions à partir de Hannah Arendt - Superfluité humaine et conformisme de l'insujet », in. CALLOZ-TSCHOPP Marie-Claire (dir.), *Lire Hannah Arendt aujourd'hui - Pouvoir, guerre, pensée, jugement, politique*, Actes du colloque international de Lausanne 11 - 12 mai 2007, Université de Lausanne, Institut d'Etudes Politiques Internationales, L'Harmattan, 2008, Paris, pp. 81 - 96

devient éducateur.(...). Une classe qui se pose elle-même comme susceptible d'assimiler toute la société est en même temps capable d'exprimer ce processus, elle conduit à la perfection de l'État de droit; jusqu'au point de concevoir la fin de l'État et du droit devenus inutiles pour avoir épuisé leur tâche et être absorbés dans la société civile¹³¹⁵ ». L'Etat est loin d'être désengagé par le capitalisme et le libéralisme, sa fonction a été modifiée par ces mouvements économiques. Tosel écrit que l'Etat a sacrifié « ses fonctions de protection et de régulation sociales pour se spécialiser dans la gestion des populations dans le sens de l'impératif systémique capitaliste. Cela veut dire simplement que tous les Etats sont pris dans un réseau d'interdépendance, mais que ce réseau fait noeud autour de quelques Etats qui disposent seuls des prérogatives de la souveraineté. (...) Les hommes sont définis de manière abstraite comme propriétaires d'eux-même, de leur « propre », dotés de la liberté fondamentale de contourner tous les obstacles qu'un Etat interventionniste pourrait opposer à leur libre entreprise¹³¹⁶ ». La surveillance diffuse s'inscrit pleinement dans la description que Tossel opère.

597. En ce qu'elle permet la gestion des populations, la surveillance diffuse a modifié la fonction de l'Etat de droit devenu libéral. Tout est organisé dans cet Etat de droit pour promouvoir la consommation et la production. Afin de réaliser ce « *droit de l'homme producteur de soi dans la consommation*¹³¹⁷ », l'Etat de droit n'est plus axé autour de la démocratie mais de la chose publique, des intérêts fluctuants de la Nation. La transformation des espaces sociaux et l'éclatement de la dichotomie publique-privé peuvent être identifiés comme un symptôme de ce glissement. De fait, l'Etat de Droit libéral est a-politique et la société civile de Habermas est transformée en marché. Les nouvelles législations européennes en matière de protection des données personnelles et non personnelles, ou plutôt devrait-on dire des législations concernant la libre circulation de l'information, n'envisagent plus vraiment la garantie de la liberté, mais bien la consommation technologique et la circulation fluide des flux d'informations. Pour Mireille Delmas - Marty, « *la métamorphose juridique de l'Etat de droit démocratique et libéral en état autoritaire, voire totalitaire, se manifeste au confluent du juridique et du politique*¹³¹⁸ ». Depuis le 11 septembre 2001, l'Etat de Droit se réduit à un volet sécuritaire et à un volet de reconnaissance d'un droit à la consommation comme garantie du bonheur et du bien-être des citoyens. Notons avec Mireille

¹³¹⁵ Quaderni del carcere, 8, § 2 ; Gramsci, 1975, p. 937 ; 1983, p. 289, cité par TOSEL André, Op. Cit. p. 82

¹³¹⁶ Ibid.

¹³¹⁷ TOSEL, Op. Cit. p. 85

¹³¹⁸ DELMAS-MARTY Mireille, *Aux quatre vents du monde (Op. Cit.)*, p. 33

Delmas-Marty les dérive que l'Etat de Droit a subi depuis 2001: « *suspension de l'Etat de Droit au nom de circonstances exceptionnelles à la fois urgentes et temporaires; contournement par durcissement de la répression contre certaines cibles et dédoublement du système pénal; enfin le détournement par transfert de pouvoirs, tantôt dans l'Etat (militarisation de la police et/ou de la justice), tantôt en dehors de l'Etat (privatisation de la force publique, qu'il s'agisse de la police ou de l'armée)*¹³¹⁹ ».

598. Les constats établis par André Tosel et Mireille Delmas-Marty font échos à la description de l'utilitarisme par Christian Laval. La consommation et le bien être peuvent se produire uniquement dans un système sécuritaire. Rappelons ici que la surveillance diffuse est le principal outil de la rhétorique de l'utilitarisme, et donc de ce nouvel Etat de droit (hyper) libéral. Concluons en empruntant les mots de Tosse, ce nouvel Etat de Droit libéral, à la fois soft totalitaire, et autoritaire, « *produit un nouveau « corps moral », colonisateur de l'espace politique de la pluralité humaine et de sa faculté de délibération, Etat qui fonctionne politiquement en produisant un apolitisme de masse*¹³²⁰ ».

B. L'aberration du solutionnisme technologique: des risques de la réglementation algorithmique

599. Si les sceptiques peuvent exprimer des réticences quant à l'aboutissement effectif de cette réglementation algorithmique, il est toutefois certain que la biopolitique algorithmique et le nouveau pouvoir statistique sont des réalités contemporaines. Le lien entre l'étude de la discipline et de la biopolitique¹³²¹ d'un côté, et le Droit de l'autre a été initié par Foucault. L'aberration du solutionnisme technologique repose alors essentiellement sur la compréhension de ces mécanismes entre eux, et spécialement à l'aune de la notion de souveraineté. Biopolitique et discipline ont modifié progressivement la souveraineté, dont le rôle consistait à l'origine à enfermer, à faire mourir, en un pouvoir sur la population, « *sur l'homme en tant qu'être vivant, un pouvoir continu, savant, qui est le pouvoir de « faire vivre »*¹³²² ». Le Droit et l'Etat de Droit vise aujourd'hui à gérer

¹³¹⁹ Ibid. p. 33 - 34

¹³²⁰ TOSEL, Op. Cit, p. 87

¹³²¹ Qui ne sont pas exclusive l'une de l'autre

¹³²² FOUCAULT Michel, *Il faut défendre la société - Cours au collège de France. 1976*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 1997

les masses dans une gestion par le calcul d'utilité (2). Cette gestion doit être assimilée à la nouvelle souveraineté de l'Etat de Droit libéral.

1. L'Etat de Droit libéral: une gestion souveraine...

600. Ainsi que le démontre Elisabeth Pélegrin-Genel, nous vivons aujourd'hui dans une ère d'espaces dupliqués à l'infini: du bureau, en passant par les galeries d'art et les galeries marchandes, jusqu'au fast-food. Ces espaces ont en commun leur ouverture au monde, « *sans obstacle, qui induit, facilite et enferme chacun dans une « gestion par le regard ». (...). Le client a un triple rôle: initier la fabrication, surveiller la réalisation mais aussi mettre la main à la pâte*¹³²³ ». Bien que son analyse s'applique aux chaînes de fast food, son analyse de la gestion par le regard rappelle les mots de Giorgio Agamben quant à la notion de souveraineté. Evoquer le concept d'Etat de droit libéral c'est également comprendre la transformation de la souveraineté de l'Etat dans sa vision économique.

601. Ce dernier voit l'exercice du pouvoir de souveraineté s'exercer sur « *la vie nue*¹³²⁴ », c'est-à-dire la vie qui voit l'avènement du social dans la sphère de la *polis*. La souveraineté chez Giorgio Agamben est alors vue de manière très extensive, tout comme la notion de dispositif qui permet de contrôler les conduites, les gestes et les opinions des vivants, « *pas seulement les prisons donc, les asiles, le panoptikon, les écoles, la confession, les usines, les disciplines, les mesures juridiques, dont l'articulation avec le pouvoir est en sens évidente, mais aussi le stylo, l'écriture, la littérature, la philosophie, l'agriculture, la cigarette, la navigation, les ordinateurs, les téléphones portables et, pourquoi pas, le langage lui-même, peut-être le plus ancien dispositif*¹³²⁵ ». Le Droit est ici analysé comme « *un opérateur dans les dispositifs de sécurité ou de gouvernementalité contemporaine*¹³²⁶ ». Cette transformation a été permise par la mise en application du principe de visibilité intégrale, invisible et invérifiable que porte en son sein la surveillance diffuse. Le pouvoir, la souveraineté de l'Etat de Droit libéral passent aujourd'hui de la gestion des territoires, à la vie des

¹³²³ PELEGRIN-GENEL Elisabeth, *Des souris dans un labyrinthe - Décrypter les ruses et manipulations de nos espaces quotidiens*, Editions La Découverte / Poche, n° 377, 2012, p. 132 - 133

¹³²⁴ AGAMBEN Giorgio, *Homo Sacer I, le pouvoir souverain et la vie nue*, Editions du Seuil, Paris, 1997

¹³²⁵ AGAMBEN Giorgio, *Qu'est ce qu'un dispositif ?*, Editions Rivages, Collection Rivage poche, 2014

¹³²⁶ MAZABRAUD Bertrand, « Foucault, le droit et les dispositifs de pouvoir », *Cités* 2010/2 (n° 42), pp. 127-189, pp. 168 - 185, Disponible en ligne à l'adresse suivante: <https://www.cairn.info/revue-cites-2010-2-page-127.htm> (dernière consultation: 5 mars 2018)

individus. Les espaces publics et privés sont entièrement décloisonnés afin de réaliser cet objectif. Le biopouvoir contemporain vise donc à s'insérer dans la doctrine des flux d'informations et de la mobilité: « la vie liquide¹³²⁷ », ce triomphe du consumérisme, selon Zygmunt Bauman. Le rôle du pouvoir se limite alors à jouer les règles du marché, en éradiquant les freins et contraintes possibles au flux et à la mobilité¹³²⁸. Le pouvoir s'exerce aujourd'hui sur un triptyque préalablement dégagé: sécurité, liberté, bien être; et ainsi que le notait Christian Laval « *la sécurité est la condition du bonheur général. Le bonheur est le grand but, la surveillance qui conditionne la sécurité est le principal levier pour y parvenir*¹³²⁹ ».

602. Selon Bertrand Mazabraud, en « *ajoutant et superposant au dispositif juridique et disciplinaire le dispositif sécuritaire*¹³³⁰ » et en les inscrivant dans l'angle d'approche de la gouvernementalité, Foucault démontre que « *la place du droit se trouve modifiée*¹³³¹ ». Et d'ajouter, « *certes le dispositif juridique de souveraineté reste défait et ses appareils ne constituent plus que des rouages au profit des disciplines. Mais Foucault a montré comment le dispositif sécuritaire a lui-même fait fonctionner les disciplines et les appareils juridiques à son profit. Le droit se révèle alors hétérogène à la rationalité économique qui anime les gouvernementalités libérale et néolibérale contemporaines. Néanmoins, cette hétérogénéité peut être réduite et utilisée comme un instrument pour une gouvernementalité économique ou, au contraire, elle peut être accentuée pour la freiner ou y résister*¹³³² ». La souveraineté de l'Etat de Droit libéral n'a pas disparu, elle a été modifiée pour faire correspondre sa tâche et sa fonction aux objectifs du libéralisme: une gestion en vue d'assurer la sécurité du marché, la liberté de consommer, et le bien-être. Ainsi que le rappelle Tosel: « *tous les Etats capitalistes –élite des États souverains États de second rang, États diminués, États fantoches cependant se réorganisent autour du droit pénal et du droit privé, en infléchissant ce dernier dans le sens du droit devenu devoir de produire et de consommer indéfiniment les*

¹³²⁷ Op. Cit.

¹³²⁸ Par exemple, les démarches visant à faciliter l'accès à Internet, les pseudos-nouveaux débats liés à l'éradication des zones blanches (qui pourrait se rapprocher aux débats liés aux luttes contre les discriminations et spécialement les logiques mises en place concernant la discrimination positive), mais également l'ouverture du marché, de la concurrence, l'ensemble des mesures prises pour combattre les freins au marché économique (on pourra s'étonner ici par exemple de la présence des géants du numérique américains aux débats parlementaire liés au Règlement général sur la protection des données personnelles, visant à l'origine à renforcer les droits et libertés, et spécialement la vie privée, dans la société du tout numérique).

¹³²⁹ LAVAL Christian, Op. Cit.

¹³³⁰ Op. Cit. p. 168.

¹³³¹ Ibid.

¹³³² Ibid.

*marchandises*¹³³³ ». Et, de conclure: « *tous les États – souverains, à demi souverains, fantoches, ou simplement nominaux, riches, pauvres – soumettent leurs sujets à l'exigence de ce nouveau conformisme qui en quelque sorte transversalement tente d'homogénéiser des populations oscillant entre le pôle de la misère totale et celui de la surabondance ostentatoire*¹³³⁴ ».

2... L'Etat de Droit libéral ou la gestion des masses par le calcul d'utilité

603. L'individu n'est pas au centre des préoccupations de l'Etat de Droit libéral. La gestion des masses, de la population est dans les faits l'objet de l'exercice de sa souveraineté. Bertrand Mazabraud écrit ainsi que le dispositif sécuritaire, selon Foucault, gère la masse, la population, en se dotant de nouveaux outils statistiques, démographiques; lui permettant d'agir sur le milieu social de l'individu. L'auteur écrit alors que « *le pouvoir sécuritaire agit sur le milieu de celle-ci, prenant en compte toutes les variables environnementales (géographique, climatologique, urbanistique, morale, juridique, etc.). Il travaille donc sur des données qui ne sont jamais totalement réductibles, mais sur des probabilités. (...) le dispositif sécuritaire s'exerce sur une population à travers son milieu selon une rationalité assurancielle : « Une technologie qui vise l'équilibre global (...) la sécurité de l'ensemble par rapport à ses dangers internes (...). Une technologie assurancielle et régulatrice. » Cette rationalité, qui cherche à minimiser les risques tout en les acceptant, est purement économique (bilan coût/avantage). En d'autres termes, le dispositif de sécurité insère les phénomènes (vols, maladies, natalité, etc.) à l'intérieur d'une série d'événements probables, tolère ceux-ci selon une logique de coût et non plus selon une logique du permis/interdit. Ce nouveau dispositif vise donc à « installer des mécanismes de sécurité autour de cet aléatoire qui est inhérent à une population d'êtres vivants. »*¹³³⁵ ». Ces mots traduisent parfaitement la description de la rhétorique de l'utilitarisme de Christian Laval. La surveillance diffuse représente, quant à elle, pleinement cet outil au service de la rationalité assurancielle décrite par Bertrand Mazabraud. Le Droit est alors réduit principalement à ce que Alain Supiot avait déjà dégagé pour le contrat de travail. La loi de l'Etat de Droit est devenu un calcul d'utilité « *qui serait à la fois la source et la mesure de sa légitimité*¹³³⁶ », et l'Etat de Droit libéral est, quant à lui, réduit à un rôle instrumental visant à garantir la fluidité de l'économie du marché. La société civile est quant à elle réduite à une

¹³³³ TOSEL, Op. Cit. p. 83.

¹³³⁴ Ibid. p. 85.

¹³³⁵ Ibid. p. 170 - 171

¹³³⁶ SUPIOT Alain, *Homo juridicus Op-Cit*, p. 174

source de connaissance et de prévisions possibles. La réglementation algorithmique tend alors à réduire la législation, ou comme le déclare Alain Supiot, « leur contenu à un calcul d'utilité, en sorte qu'elles servent « les harmonies économiques qui présideraient au fonctionnement des sociétés humaines¹³³⁷ »

604. On retrouve ici en filigrane les mots de Christian Laval lorsqu'il décrivait la rhétorique de l'utilitarisme propre à la surveillance. Et les conséquences des dispositifs sécuritaires décrites par Bertrand Mazabraud rappelle les propos précédemment développés: « *déterritorialisation du droit par les dispositifs disciplinaires et sécuritaire, reterritorialisation pulvérisée du droit sous le prisme de la biopolitique en de nombreux droits subjectifs¹³³⁸* », « *cheminement d'une régulation externe du pouvoir (en termes de légitimité) à une régulation interne du pouvoir (en termes d'efficacité)¹³³⁹* », « *passage du modèle juridique du pouvoir au modèle économique¹³⁴⁰* », « *l'Etat tire sa légitimité gouvernementale du processus économique, sous l'occurrence suivante: la liberté économique produit la légitimation par un consensus permanent de tous ceux qui participent en tant qu'agents au processus économique (...), comme le droit crée la condition de la liberté économique, l'exercice de cette liberté vient légitimer en retour l'Etat¹³⁴¹* ». L'ensemble de ces éléments tendent à converger vers l'élaboration progressive d'un Droit libéral, d'une liberté réduite à la consommation, à la sécurité et au bien-être, d'un droit désinstitué au profit de l'économie.

605. Si la désinstitution semble une notion forte à appliquer au Droit, il faut néanmoins constater une hybridation de l'Etat de Droit et du Droit par les logiques économiques. Principalement réduite à une règle de calcul d'utilité fondée sur l'analyse de la société civile par la surveillance diffuse, cette nouvelle gouvernance ne vise plus à assurer les droits et libertés fondamentaux classiquement admis, mais bien la liberté de consommer, la sécurité, le bien être. La rhétorique de l'utilitarisme hybride le Droit d'un versant économique, et modifie sa fonction.

¹³³⁷ SUPIOT Alain, *La gouvernance par les nombres - Cours au Collège de France (2012 - 2014)*, Fayard, Collection Poids et mesures du monde, 2015, p. 106

¹³³⁸ Ibid. p. 175, on pense notamment ici au droit à la sécurité, au droit au bien-être

¹³³⁹ Ibid. p. 176. On pense ici notamment à la transformation de l'Etat en manager public, en gestionnaire

¹³⁴⁰ Ibid. p. 178

¹³⁴¹ Ibid. p. 181.

Chapitre 2: La mutation du contrôle social par la surveillance diffuse et ses effets sur le Droit

606. « *Aie confiance, crois en moi, que je puisse veiller sur toi ... (...), fais un somme, sans méfiance, (...), le silence propice te berce, souris et sois complice, laisse tes sens glisser vers ces délices tentatrices*¹³⁴² ». A l'image des paroles du serpent du livre de la jungle, les prosélytes, conquis par l'économie fondée sur la donnée, poussent la société à l'acceptation d'un changement de paradigme: si « *la vie privée n'est plus une norme sociale*¹³⁴³ », acceptons et embrassons la surveillance diffuse. Avec la complicité des individus, la surveillance diffuse s'est intégrée culturellement et socialement.

607. Cette acculturation de la surveillance diffuse emporte des conséquences sur le droit des données personnelles et de la vie privée. Prenant appui sur une société en crise, la surveillance diffuse apparaît aujourd'hui comme le meilleur des remèdes à tous les maux sociaux et individuels. Logique de prévision et de prévention des risques et des menaces, logique performative appliquée aux individus, aux entreprises et aux Etats, rentabilisation des actions et responsabilisation des acteurs sont autant de nouveaux systèmes de décisions, de pensées, et d'effets de la surveillance diffuse. Au-delà de l'intégration culturelle et sociétale de la surveillance diffuse, et des conséquences qu'elle emporte en termes de protection des données personnelles et de la vie privée, ces effets doivent également être analysés comme emportant des conséquences sur le Droit. Si la surveillance diffuse est aujourd'hui la nouvelle norme sociale, c'est principalement du fait d'une hybridation du Droit engendrée par les effets de la surveillance diffuse. Cette hybridation semble pouvoir être analysée également comme une forme de désinstitution, à la lumière du concept de contrôle social.

608. Les analyses Foucaaldiennes, produites voici un quart de siècle, fournissent une grille d'analyse utile du phénomène de surveillance diffuse. Elles donnent, en effet, des indications de méthodes pour l'analyse contemporaine de ce dernier. Elles permettent également de combler, en partie, la défaillance du Droit dans son appréhension du phénomène. Cette grille d'analyse, offerte par la référence au concept de contrôle social et aux études y afférentes, doit nécessairement être enrichie par la mutation même de cette notion, du fait de la surveillance diffuse. Ainsi que le rappelait Michel Foucault, « *ce qui est important, c'est que le travail social s'inscrit à l'intérieur*

¹³⁴² Extrait des paroles de Kaa, Le livre de la jungle, film d'animation de Walt Disney, 1967.

¹³⁴³ On pense ici aux mots de Mark Zuckerberg, précédemment cités, « la vie privée n'est plus une norme sociale ».

d'une grande fonction qui n'a pas cessé de prendre des dimensions nouvelles depuis des siècles, qui est la fonction de surveillance-correction. Surveiller les individus, et les corriger, dans les deux sens du terme, c'est-à-dire les punir ou les pédagogiser¹³⁴⁴ ».

609. Au-delà de la démonstration d'un lien avec le contrôle social, ces mots sont particulièrement éclairant quant à l'influence réciproque que ces deux notions entretiennent. Il apparaît aujourd'hui que nous sommes passés d'une « surveillance-correction », de la fonction de « punir » du contrôle social; d'une vision péjorative donc, à une version positive du contrôle social du fait même de la surveillance: l'attention (section 1). La définition classique de l'action de surveiller emporte nécessairement une observation attentive. Les mécanismes attentionnels mis en place au travers de la surveillance diffuse, en vue d'assurer une nouvelle forme de contrôle, doivent nécessairement être analysés afin d'en comprendre ses effets sur le Droit. Par l'objectivation des individus, la surveillance diffuse semble en effet désinstituer ce dernier dans son rôle de civilisation des relations sociales (section 2).

Section 1: L'avènement d'un contrôle social positivé et pleinement intériorisé du fait de la surveillance diffuse: l'attention

610. Sans revenir sur l'ensemble de l'analyse concernant l'injonction de transparence prônée par la surveillance diffuse, il apparaît nécessaire de comprendre les liens qu'entretiennent le contrôle social et le libéralisme économique. Alors qu'il envisageait les écrits de Bentham, Foucault évoquait l'élaboration d'une économie fondée sur la visibilité (paragraphe 1). Au vu de la rhétorique de l'utilitarisme et du libéralisme, cette économie de la visibilité doit être entendue comme telle, un marché économique guidant le nouveau contrôle social. Alors qu'elle analysait l'ouvrage de Régis Debray concernant le nouveau pouvoir¹³⁴⁵, Mireille Delmas-Marty écrivait qu'au néoprottestantisme décrit par Debray, « *on préférerait « l'esprit protestataire »*¹³⁴⁶ ». Et d'ajouter que « *le nouveau pouvoir (...) semble admettre la justice prédictive mise en place face au*

¹³⁴⁴ FOUCAULT Michel, « Table ronde », (entretien avec J. - M. Domenech, J. Donzelot, J. Julliard, P. Meyer, R. Pucheu, P. Thibaud, J. - R. Tréanton, P. Virillo), *Esprit*, n° 413: Normalisation et Contrôle social (pourquoi le travail social ?), Avril - mai 1972, pp. 678 - 703, in. DEFERT Daniel et EWALD François (sous la direction de), *Michel Foucault, Dits et écrits 1954 - 1988, I. 1954 - 1975*, Editions Quarto Gallimard, 2001, texte n° 107, p. 1199.

¹³⁴⁵ DEBRAY Régis, *Le nouveau pouvoir*, Les éditions du Cerf, Collection Médium - Transmettre pour innover, 2017

¹³⁴⁶ DELMAS-MARTY Mireille, *Au néoprottestantisme, on préférerait l' « esprit protestataire »*, *Le Monde*, 29 août 2017, En Ligne: http://www.lemonde.fr/idees/article/2017/08/29/mireille-delmas-marty-au-neoprottestantisme-de-regis-debray-on-prefererait-l-esprit-protestataire_5177870_3232.html (dernière consultation: 5 mars 2018)

terrorisme, ne craignant pas de s'inspirer d'une société qui porte en elle la possibilité d'un contrôle permanent évoquant les prévisions de Tocqueville sur le « despotisme doux » qui menacerait les démocraties¹³⁴⁷ ». Au coeur même de la définition de la surveillance, l'attention est devenue le nouveau contrôle social (paragraphe 2) au service du despotisme doux de Tocqueville, du monstre doux de Raffaele Simone.

Paragraphe 1: De la mutation du contrôle social par l'élaboration d'une économie de la visibilité

611. La surveillance diffuse porte en elle l'assujettissement de l'individu à la visibilité (A). Cet assujettissement n'est plus le propre d'une forme de contrôle traditionnelle mais bien d'une logique économique qu'il faut comprendre et analyser (B).

A. L'assujettissement de l'individu à la visibilité

612. Si la théorisation par Bentham de l'utilité du regard comme forme essentielle de contrôle social et sa reprise par Michel Foucault sont une part essentielle de la surveillance diffuse, il faut encore traduire cette pensée à la société contemporaine. Ce principe permet la maîtrise de l'espace visuel et le contrôle des personnes qui se trouvent dans cet espace. Ainsi que le soulignait Jérémy Bentham, ce principe d'inspection et de visibilité permet également de réduire le nombre de personnes qui contrôlent, et d'augmenter le nombre de personnes contrôlées.

613. Les technologies de l'information et de la communication ont renforcé cet effet lié au principe d'inspection tendant à faire de la surveillance diffuse un moyen de contrôle invisible et invérifiable pour paraphraser Michel Foucault. L'un des problèmes majeurs de la compréhension de la surveillance contemporaine est de bien comprendre son lien avec la notion de contrôle social, et, plus avant, avec la notion de pouvoir. En effet, le principe de visibilité décrit par Bentham et Foucault semble être passé d'un moyen de contrôle social et de pouvoir à une véritable norme sociale. L'analyse de ces questions sur les évolutions du regard dans nos sociétés modernes à l'aune de la surveillance diffuse et du contrôle revient à mettre en évidence ce que Michel Foucault appelait « *l'économie de la visibilité dans l'exercice du pouvoir*¹³⁴⁸ ». Ce dernier a étudié le déclin

¹³⁴⁷ Ibid.

¹³⁴⁸ FOUCAULT Michel, *Surveiller et punir - Naissance de la prison*, Op. Cit., p. 334.

des institutions dominantes au profit des sociétés de contrôle. A travers ses analyses concernant la bureaucratie, la rationalisation du pouvoir, et les concepts de savoir et pouvoir, de discipline, de biopolitique et de gouvernementalité, Foucault a mis en évidence l'apparition de nouvelles pratiques engendrant l'auto-gouvernance des individus et des populations. Par la mise en place d'un pouvoir disciplinaire fondé sur la surveillance et la décentralisation des pouvoirs étatiques, Foucault constate une transformation claire de la nature et de l'exercice du pouvoir.

614. En 1975, il écrit alors: « *l'examen intervertit l'économie de la visibilité dans l'exercice du pouvoir. Traditionnellement le pouvoir, c'est ce qui se voit, ce qui se montre, ce qui se manifeste, et de façon paradoxale, trouve le principe de sa force dans le mouvement par lequel il la déploie. Ceux sur qui il s'exerce peuvent rester dans l'ombre; ils ne reçoivent de lumière que de cette part de pouvoir qui leur est concédée, ou du reflet qu'ils en portent un instant. Le pouvoir disciplinaire, lui, s'exerce en se rendant invisible; en revanche il impose à ceux qu'il soumet un principe de visibilité obligatoire. Dans la discipline, ce sont les sujets qui ont à être vus. Leur éclairage assure l'emprise du pouvoir qui s'exerce sur eux. C'est le fait d'être vu sans cesse, de pouvoir toujours être vu, qui maintient dans son assujettissement l'individu disciplinaire*¹³⁴⁹ ». Le contrôle social est influencé par l'économie de la visibilité. L'influence des logiques économiques sur le pouvoir mais également sur le contrôle social sont les principaux traits aujourd'hui de la surveillance diffuse.

B. La mutation du contrôle social par le libéralisme contemporain

615. Les analyses liées au pouvoir disciplinaire, frappent l'esprit lorsqu'on les rapproche à la situation actuelle dominée par la surveillance diffuse. Guy Debord en 1967¹³⁵⁰ insiste sur la mutation du contrôle social par la domination spectaculaire. Gilles Deleuze, quant à lui, poursuit et complète l'analyse de Foucault concernant la discipline, et l'enrichit par le recours au concept de société de contrôle. Dans son analyse, nul recours au principe de visibilité, ni même à l'importance du regard; mais une étude des mécanismes de contrôle enrichissante permettant de traduire des enjeux de pouvoir et de domination. Deleuze écrit ainsi que: « *il est facile de faire correspondre à chaque société des types de machines, non pas que les machines soient déterminantes, mais parce qu'elles expriment les formes sociales capables de leur donner naissance et de s'en servir. (...). Les sociétés de contrôle opèrent par des machines de troisième espèce, machines informatiques et*

¹³⁴⁹ Ibid. p. 219 - 220.

¹³⁵⁰ DEBORD Guy, *La société du spectacle*, Editions Champ Libre, Paris, 1971

ordinateurs dont le danger passif est le brouillage, et l'actif, le piratage et l'introduction de virus. Ce n'est pas une évolution technologique sans être plus profondément une mutation du capitalisme¹³⁵¹ ».

616. Au-delà de ce rapprochement entre la mutation du contrôle social et la mutation de nos sociétés liées au capitalisme, Gilles Deleuze analyse le principe du contrôle qui complète l'enfermement disciplinaire. *« Ce sont les sociétés de contrôle qui sont en train de remplacer les sociétés disciplinaires. « Contrôle », c'est le nom que Burroughs propose pour désigner le nouveau monstre, et que Foucault reconnaît comme notre proche avenir¹³⁵² ».* Et de poursuivre: *« L'étude socio-technique des mécanismes de contrôle, saisis à leur aurore, devrait être catégorielle et décrire ce qui est déjà en train de s'installer à la place des milieux d'enfermement disciplinaires, dont tout le monde annonce la crise. Il se peut que de vieux moyens, empruntés aux anciennes sociétés de souveraineté, reviennent sur scène, mais avec les adaptations nécessaires. Ce qui compte, c'est que nous sommes au début de quelque chose. (...). Ce sont des exemples assez minces, mais qui permettraient de mieux comprendre ce qu'on entend par crise des institutions, c'est-à-dire l'installation progressive et dispersée d'un nouveau régime de domination¹³⁵³ ».* L'ensemble de ces analyses ont en commun de mettre en avant un nouveau régime de domination qu'il soit organisé par le spectacle, par des machines et mécanismes de contrôle, par un pouvoir disciplinaire organisé autour d'un principe de visibilité intégrale. Elles démontrent un déclin des institutions classiquement établies lorsqu'on évoque la question du pouvoir, qu'il s'agisse de l'Etat, du pouvoir politique, ainsi que du sujet de ce pouvoir: le sujet de droit. Ces citations ont également le mérite plus subtile d'interroger l'individu sur son rapport à la visibilité, au contrôle social, au pouvoir.

617. Pour opérer un rappel avec les développements précédents et spécialement ceux consacrés à la gouvernementalité par la peur, Michel Foucault écrivait : *« Si on prend la question du pouvoir, du pouvoir politique, en la remplaçant dans la question plus générale de la gouvernementalité (...), si on entend par gouvernementalité un champ stratégique de relations de pouvoir, dans ce qu'elles ont de mobile, de transformable, de réversible, (...) cette notion de gouvernementalité ne peut pas ne pas passer, théoriquement et pratiquement, par l'élément d'un sujet qui serait défini par le rapport de soi à soi. Alors que la théorie du pouvoir politique comme institution se réfère d'ordinaire à une*

¹³⁵¹ DELEUZE Gilles, « Post-scriptum sur les sociétés de contrôle », in. *L'autre journal* n° 1, mai 1990, p. 5.

¹³⁵² Ibid. p. 2

¹³⁵³ Ibid. p. 6 - 7.

*conception juridique du sujet de droit,(...) l'analyse du pouvoir comme ensemble de relations réversibles- doit se référer à une éthique du sujet défini par le rapport de soi à soi.¹³⁵⁴ ». Ces mots ne sont pas sans rappeler ceux de Pierre Bourdieu, et les analyses développées précédemment concernant la culture du narcissisme. Le principe de visibilité intégrale de la surveillance diffuse emporte satisfaction d'un désir, pour l'individu, de reconnaissance. Ainsi que Bourdieu le fait remarquer, le vu et l'image d'un groupe social est une réalité sociologique. En 1979, Bourdieu écrit: « *La représentation que les individus et les groupes livrent inévitablement à travers leurs pratiques et leurs propriétés fait partie intégrante de leur réalité sociale. Une classe est définie par son être perçu autant que par son être, par sa consommation - qui n'a pas besoin d'être ostentatoire pour être symbolique - autant que par sa position dans les rapports de production (même s'il est vrai que celle-ci commande celle-là)*¹³⁵⁵ ».*

618. Ainsi que le déclare Alain Damasio, « *ce que Foucault sent, c'est que le pouvoir va devoir procéder autrement, beaucoup plus doucement, insidieusement, et en faisant une sorte d'échange : on troque une partie de notre liberté au nom d'une vie plus fluide. Il anticipe le fait qu'on passe d'un régime disciplinaire à un régime plus normatif. (...). Ce n'est plus Big Brother, c'est Big Mother, il s'agit d'un pouvoir maternant, couvant qui anticipe et répond à nos besoins*¹³⁵⁶ ». Avec les notions de contrôle, de gouvernementalité, de pouvoir, Michel Foucault avait pressenti le passage d'un régime disciplinaire aux sociétés de contrôle. Son analyse du panoptique, couplée à son étude du contrôle social, permet de rendre compte d'une réalité contemporaine: le panoptique et son principe de visibilité intégrale se sont exportés à la société toute entière. La surveillance diffuse, qui régénère le principe de visibilité intégrale, a permis progressivement d'intérioriser l'idéologie de cette forme de contrôle qu'elle est devenue une norme, une auto-discipline, un auto-contrôle. En parallèle, la thèse de Zygmunt Bauman concernant « la société liquide¹³⁵⁷ » éclaire quant à l'émancipation des individus face à la loi, au pouvoir, aux institutions classiques, et au nouvel ordre promu par les mécanismes de la consommation.

¹³⁵⁴ FOUCAULT Michel, *L'herméneutique du sujet - Cours au collège de France, 1981 -1982*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 2001, p. 241 - 242

¹³⁵⁵ BOURDIEU Pierre, *La Distinction - Critique sociale du jugement*, Les éditions de Minuit, Collection Le sens commun, Paris, 1979, p. 563 - 564

¹³⁵⁶ ROPERT Pierre, *Interview d'Alain Damasio à l'occasion du 30^{ème} anniversaire de la mort de Michel Foucault dans le cadre d'un dossier relatif à la société de surveillance de Foucault*, France Culture, 13 juin 2016, En ligne: <https://www.franceculture.fr/philosophie/la-societe-de-surveillance-de-foucault> (dernière consultation: 5 mars 2018)

¹³⁵⁷ Op. Cit.

Paragraphe 2: L'avènement d'un contrôle social positif et pleinement intériorisé du fait de la surveillance diffuse: l'attention

619. Bien-être, sécurité, liberté, libéralisme économique et utilitarisme sont autant d'éléments factuels de nos sociétés contemporaines qui participent à l'élaboration d'une théorie empirique de la surveillance diffuse, du « data-panoptisme » pour reprendre l'expression de Sadin, et du contrôle social que cette dernière engendre. L'ensemble de ces facteurs est d'autant plus présent aujourd'hui que le néo-libéralisme conduit à une remise en question de l'Etat-providence - passant du Welfare State au Well-Being des nations - à une promotion toujours plus croissante de l'économie de marché fondée sur le développement économique et la liberté de l'individu-consommateur; mais également à une autorégulation des acteurs du marché engendrant une disparition progressive du secteur public au profit du secteur privé. Foucault avait pressenti l'effet du panoptique comme machine de pouvoir, en l'interprétant à la lumière des notions de gouvernementalité, mais également du néolibéralisme. Il écrivait que « *l'efficace du pouvoir, sa force contraignante sont, en quelque sorte, passées de l'autre côté – du côté de sa force d'application. Celui qui est soumis à un champ de visibilité, et qui le sait, reprend à son compte les contraintes du pouvoir ; il les fait jouer spontanément sur lui-même ; il inscrit en soi le rapport de pouvoir dans lequel il joue simultanément les deux rôles il devient le principe de son propre assujettissement*¹³⁵⁸ ». Dès *Surveiller et Punir*, Foucault analyse donc la surveillance comme un moyen de gouverner les individus à distance, tout en les faisant intérioriser les contraintes du pouvoir, créant ainsi, un nouveau mode d'assujettissement. La surveillance diffuse dominée par un néo-libéralisme prônant bien-être et sécurité, fonctionne quant à elle sur des moyens d'assujettissement relativement nouveaux. Il faut, en effet, d'une part démontrer l'avènement d'un contrôle social totalement positif, qui pourrait se résumer sous le concept de l'attention (A). D'autre part, l'intériorisation quasi-parfaite de ce nouveau contrôle social mène à l'acceptabilité, l'acceptation sans résistance aucune de la surveillance diffuse, conduisant à l'analyse du mythe répandu dans les sociétés contemporaines du « je n'ai rien à cacher, je n'ai rien à me reprocher », voire même à l'inversion de ce dernier. En réalité, l'ensemble de cet analyse tourne autour de la question de la fabrique du consentement à la surveillance diffuse (B).

¹³⁵⁸ FOUCAULT Michel, *Surveiller et punir*, Op. Cit., p. 363

A. L'attention: une nouvelle forme de contrôle social positif

620. L'attention de la surveillance diffuse est exactement ce que les auteurs tels que Mireille Delmas-Marty, Tocqueville, et Raffaele Simone évoquent sous les expressions de monstre doux et de despotisme doux. Cette attention opère un dressage, une domestication des individus en douceur (1). Le caractère ubiquitaire de la surveillance diffuse, comme outil principal d'un nouveau contrôle social, participe alors d'une totalisation d'un contrôle social positif et muté en attention (2).

1. Le dressage et la domestication des individus

621. Les analyses de Jacques Ellul, de Michel Foucault, de Hannah Arendt et de Christian Laval ont permis de mettre au jour la totalisation technologique que le système économique a élaboré de manière conjointe, tant par le secteur privé que par le secteur public. Ces études ont permis de démontrer les modifications des relations sociales que la totalisation technologique et le système économique néo-libéral ont engendrées: brouillage des classes sociales préalablement établies¹³⁵⁹, volonté de s'insérer dans une « vie de consommation¹³⁶⁰ », et de réduire l'individu et sa liberté à cette seule action. Ces éléments engendrent le développement de la surveillance diffuse permise par une gouvernance, voire une gouvernementalité, fondée sur la peur du terrorisme et des insécurités, et sur la promotion du bien-être, voire d'un potentiel droit au bien être. Du point de vue du contrôle social, ce dernier se modifie également; passant d'un contrôle de type bureaucratique à une forme plus douce, plus positive. A l'image de ce que décrivait Foucault concernant la crise des sociétés de discipline dans les pays industrialisés, reconnaissant qu'il allait falloir « *se séparer dans l'avenir de*

¹³⁵⁹ Cf. Hannah Arendt

¹³⁶⁰ Nous empruntons cette expression à Zygmunt Bauman qui décrit la vie de consommation comme suit: « *les êtres humains sont tous, depuis toujours, des consommateurs, et le rapport de l'homme à la consommation n'a rien de nouveau. Il précède certainement à l'avènement de la variété « liquide » de la modernité. (...) Il est au contraire nécessaire de se concentrer sur une vraie nouveauté qui est essentiellement de nature sociale, et ensuite de nature psychologique ou comportementale: la consommation individuelle conduite dans le cadre d'une société de consommateurs. Une « société de consommateurs » ne vaut pas que la somme des consommateurs; c'est une totalité comme dirait Emile Durkheim, « supérieure à la somme de ses parties ». Il s'agit d'une société qui (pour employer une vieille notion autrefois popularisée sous l'influence d'Althusser) « interpelle » ses membres surtout, voire exclusivement, en tant que consommateurs; une société qui juge et évalue ses membres presque uniquement d'après leurs capacités et conduite relatives à la consommation. L'expression « société de consommateurs » fait bien plus que simplement traduire en paroles cette observation banale d'après laquelle, ayant trouvé la consommation agréable, ses membres passent le plus clair de leur temps à essayer d'en augmenter les plaisirs, et y emploient l'essentiel de leurs efforts. Cette expression indique en sus que la perception et le traitement de presque toutes les parties du cadre social et des actions qu'elles suscitent et encadrent tendent à être guidées par le « syndrome consumériste » de prédispositions cognitives et évaluantes. La « politique de vie », comprenant la Politique avec un « P » majuscule autant que la nature des relations interpersonnelles, tend à être refaçonée à l'image des moyens et des objets de consommation, et suivant les lignes qu'implique le syndrome consumériste ». in. BAUMAN Zygmunt, *La vie liquide*, Fayard / Pluriel, 2013, p. 130 - 131*

*la société de discipline d'aujourd'hui*¹³⁶¹ », le contrôle social classique semble muter en auto-contrôle permanent, pleinement intériorisé, rendu possible par et pour la surveillance diffuse.

622. De fait, ce n'est pas le triomphe d'un individu et d'une société de liberté que la mutation du contrôle social a permis. Bien que libéré d'un conformisme social disciplinaire et d'un pouvoir étatique contraignant, l'individu, ou pour reprendre les mots de Christian Laval « l'homme-économique » est au contraire sommé de se rendre visible et de se placer dans le champ d'observation de la surveillance diffuse, devenant ainsi ubiquitaire. Cette mutation du contrôle social revêt deux aspects fondamentaux. Ainsi que l'écrit fort justement Philippe Vion - Dury en 2016, « *du fait de l'éclatement successif de tous les milieux d'enfermement, de la contestation de toutes les normes et de la déconstruction de tous les mythes et traditions; l'implacable vague du libéralisme socio-culturel et économique a balayé un par un les corps et espaces intermédiaires institués entre l'individu et le Marché, dont les espaces d'enfermement. Sans ceux-ci, plus de discipline possible. Sans enceintes pour les contenir et leur donner leur force, les disciplines vont se métamorphoser et se fondre « à l'air libre », dans le champs social lui-même. Le dressage des individus est dès lors immanent: il est présent partout, de manière diffuse, presque imperceptible, mais néanmoins actif, agissant à travers les relations sociales, les représentations, les signes. Sans institutions, les normes se multiplient et se diffusent, mais ne sont plus énoncées, tout comme les techniques pour les inculquer. Coutumes, habitudes et pratiques ne sont plus enseignées, elles sont suggérées par les modèles que produit la société*¹³⁶² ». Et d'ajouter, « *fini le fantasme du Big Brother incarné dans quelques instances diabolisées, la structure du Panoptique a éclaté et a fusionné avec notre environnement*¹³⁶³ ». Ces quelques réflexions de l'auteur amènent des précisions quant à l'étude de la modification du contrôle social. Les mots de l'auteur tendent à prouver la fusion totale du panoptique, du data-panoptisme, plus globalement de la surveillance diffuse avec nos sociétés. Elle n'est alors plus conçue comme un outil de coercition et de contrôle; mais bien plutôt comme un outil ubiquitaire du dressage des individus.

623. Le contrôle social glisse donc vers ce dressage des individus, ou comme le notait Peter

¹³⁶¹ FOUCAULT Michel, « La société disciplinaire en crise », *Asahi Jaanaru*, 20ème année, n° 19, 12 mai 1978, (Conférence à l'institut franco-japonais de Kansai, à Kyoto, le 18 avril 1978, in. DEFERT Daniel et EWALD François (sous la direction de), *Michel Foucault, Dits et écrits 1954 - 1988, II. 1976 - 1988*, texte n° 231, pp. 532 - 534 Editions Quarto Gallimard, 2001

¹³⁶² VION-DURY Philippe, *La nouvelle servitude volontaire - Enquête sur le projet politique de la Silicon Valley*, FYP Editions, 2016, p. 220 - 221.

¹³⁶³ Ibid.

Sloterdijk, vers la domestication¹³⁶⁴ de ces derniers. Il ne s'agit plus aujourd'hui d'enserrer le contrôle social dans des logiques d'enfermements des corps, mais bien de le penser comme une action continue et diffuse sur les esprits. Cet élément de compréhension amène certains auteurs à recourir à nouveau à la fiction et à la métaphore en analysant la situation contemporaine par un glissement de la figure du « Big Brother vous surveille » à la figure de « Big Mother veille sur vous »¹³⁶⁵. On comprend dès lors que la dénotation négative, que revêtait jusqu'alors le contrôle social, puisse recevoir aujourd'hui une connotation positive, du fait même de la surveillance qui veille sur les individus, les incite, les influence, les gère, les protège tout en les analysant.

2. La totalisation d'un nouveau contrôle social: l'attention

624. Le caractère ubiquitaire de la surveillance diffuse, comme outil d'un nouveau contrôle social qui dresse et domestique les individus, participe de la totalisation du contrôle social. A l'image de ce que décrivait Marcel Mauss relativement aux faits sociaux totaux, qui « *mettent en branle dans certains cas la totalité de la société et de ses institutions (...) et dans d'autres cas, seulement un très grand nombre d'institutions, en particulier lorsque ces échanges et ces contrats concernent plutôt des individus*¹³⁶⁶ », ce nouveau contrôle social total cristallise croyance collective, fonctions institutionnelles, pouvoir, économie, droit et normes sociales. L'argument d'un contrôle social total sous-tendu par les nouvelles technologies, popularisé par Gary Marx en 1985¹³⁶⁷, n'est certes pas nouveau; mais son mode d'action renforcé par la surveillance diffuse l'est. Les institutions du pouvoir, qu'elles soient économiques ou politiques, ne s'appuient plus sur une forme de discipline

¹³⁶⁴ SLOTERDIJK Peter, *Règles pour le parc humain, suivi de La domestication de l'Etre*, Editions Fayard, Milles et une nuits, 2010.

¹³⁶⁵ Outre l'auteur de science-fiction Alain Damasio, on citera à l'appui de ce glissement des auteurs tels que Michel Schneider, ou encore Philippe Vion-Dury. Voir: SCHNEIDER Michel, *Big Mother, Psychopathologie de la vie politique*, Odile Jacob, 2002; VION - DURY Philippe, Op. Cit.

¹³⁶⁶ Et de poursuivre: « *Tous ces phénomènes sont à la fois juridiques, économiques, religieux, et même esthétiques, morphologiques, etc. Ils sont juridiques, de droit privé et public, de moralité organisée et diffuse, strictement obligatoires ou simplement loués et blâmés, politiques et domestiques en même temps, intéressant les classes sociales aussi bien que les clans et les familles. Ils sont religieux : de religion stricte et de magie et d'animisme et de mentalité religieuse diffuse. Ils sont économiques : car l'idée de la valeur, de l'utile, de l'intérêt, du luxe, de la richesse, de l'acquisition de l'accumulation, et d'autre part, celle de la consommation, même celle de la dépense pure, purement somptuaire, y sont partout présentes, bien qu'elles y soient entendues autrement qu'aujourd'hui chez nous* ». In. MAUSS Marcel, *Essai sur le don - Formes et raisons de l'échange dans les sociétés primitives*, édition électronique réalisée par Jean-Marie Tremblay, professeur de sociologie au Cégep de Chicoutimi, 2002, En ligne: <http://anthropomada.com/bibliotheque/Marcel-MAUSS-Essai-sur-le-don.pdf> (dernière consultation: 5 mars 2018), p. 102 - 103

¹³⁶⁷ MARX Gary, « The Surveillance Society: The Threat of 1984-Style Techniques », *Futurist*, Juin 1985, n° 19, pp. 21 - 26. A travers cet article l'auteur insiste sur le fait que les nouvelles technologies participent à créer des situations où les derniers gardes-fous contre un contrôle social total s'effritent.

et de contrainte pour exercer le contrôle; mais bien plutôt sur des logiques bienveillantes, quotidiennes, diffuses qui se résument parfaitement sous la dénomination d'attention.

625. L'économie fondée sur l'attention comme capital social n'est pas une notion récente¹³⁶⁸. L'acquisition, la captation de l'attention et sa distribution, permettrait d'entretenir, d'accumuler des ressources, principalement fondées sur l'information. Le sociologue allemand, Georg Franck, a systématisé très tôt l'approche de l'économie de l'attention. Dès l'introduction de son article fondateur, un lien clair peut être opéré entre l'attention, l'économie, et sa potentialité de rapprochement à la notion de contrôle social. Georg Frank écrit ainsi: « *qu'y a-t-il de plus plaisant que de voir d'autres personnes tourner vers nous un esprit bienveillant ? D'avoir l'assurance de leur empathie compulsive ? Qu'y a-t-il de plus inspirant que de parler à des oreilles éprises ? De faire l'expérience de sa propre puissance de fascination ? Qu'y a-t-il de plus excitant que les regards de toute une salle fixés sur soi ? Les applaudissements à tout rompre ? Enfin, quoi de plus enchanteur que faire l'objet du regard charmé de ceux sous le charme desquels nous sommes nous-mêmes ? L'attention d'autrui est la plus irrésistible des drogues. Son acquisition éclipse toute autre sorte de revenu. Ainsi la gloire prime sur le pouvoir; ainsi la richesse s'estompe devant la prééminence¹³⁶⁹ ».* Cette économie de l'attention représente l'aboutissement de la logique utilitariste préalablement développée: elle porte en elle la promotion du bien-être, de la bienveillance, de la

¹³⁶⁸ Herbert Simon écrivait en 1971 que : « *Dans un monde riche en information, l'abondance d'information entraîne la pénurie d'une autre ressource : la rareté devient ce que consomme l'information. Ce que l'information consomme est assez évident : c'est l'attention de ses receveurs. Donc une abondance d'information crée une rareté de l'attention et le besoin de répartir efficacement cette attention parmi la surabondance des sources d'informations qui peuvent la consommer* ». in. GREENBERGER Martin, *Computers, communications, and the public interest*, Baltimore, MD, The John Hopkins Press, 1971, En ligne: <http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=33748>, p. 40, (dernière consultation: 5 mars 2018).

¹³⁶⁹ FRANCK Georg, « Economie de l'attention », in. CITTON Yves (sous la direction de), *L'économie de l'attention - Nouvel horizon du capitalisme ?*, Editions La Découverte, Paris, 2014, pp. 55 - 72. L'auteur ajoute plus loin, « *si la capacité de l'attention humaine à assimiler de l'information se transfère aux machines, cela signifie que le développement des médias n'est pas le seul à se diriger vers la colonisation des espaces virtuels. (...). La transformation dans l'ensemble dépasse de loin ce que laisse entrevoir le discours habituel sur la « société de l'information » (...). L'attention est loin de n'être qu'une aptitude à traiter des informations. Être attentif, c'est par définition, être dans un état conscient, aussi bien au sens de l'existence consciente de soi que de la présence d'esprit. Être attentif, c'est être dans le milieu {Medium} par quoi tout doit passer afin de devenir expérience effective pour nous. Chaque être attentif est le centre de son propre monde individuel. (...). Le fait d'être attentif est, en lui-même, d'un degré ontologique supérieur par rapport à tout objet qui apparaît dans l'attention. L'être attentif fait part de la dignité qui est la sienne à celui auquel s'adresse son attention. Rien que pour cette raison, le fait de recevoir de l'attention {Zuwendung} bienveillante compte parmi les biens les plus précieux pour les êtres qui sont eux-mêmes attentifs. Recevoir de l'attention {aufmerksame Zuwendung} signifie avoir part au monde d'un autre* ». Ibid. p. 70 - 71

sécurité et de la liberté¹³⁷⁰. Elle fonctionne principalement sur la captation de l'attention via des mécanismes publicitaires, des prédications, du storytelling¹³⁷¹. Son principal carburant réside dans l'information que les individus lui permettent de capter, d'analyser, de croiser à l'aide des nouvelles technologies. Elle est systématique, concentrée sur ce but, et routinière; et permet en dernier lieu d'influencer, de gérer, de diriger, voire de protéger les individus d'eux-mêmes et des autres¹³⁷². L'attention, en tant que nouvelle forme de contrôle social, correspond alors pleinement à l'émergence d'un contrôle social total, puisque pleinement positif dans ses objectifs, et dans sa nature même qui s'intègre pleinement à la vie liquide décrite par Zygmunt Bauman. Cette construction positive, indirecte, douce et bienveillante d'une nouvelle forme de contrôle social n'est pas sans rappeler les mots de Pierre Bourdieu qui déclarait que « *toute intervention directe et consciente, du moins lorsqu'elle vient de l'Etat, par quelque biais que ce soit, est discréditée d'avance*¹³⁷³ ». Ici, nul besoin d'intervention directe et nul discrédit jeté sur cette forme d'intervention, qui n'intervient pas. Par l'attention, le contrôle et le pouvoir sont réglés à distance, par captation, traitement, collecte et appairage d'informations; et engendre la possibilité du contrôle social total envisagé par l'Etat, et les entreprises du secteur privé.

626. L'attention comme nouveau mode de contrôle social s'inscrit alors pleinement dans les analyses foucaaldiennes de la modernité en occident. Et couplée aux analyse d'Arendt, Ellul, Lasch

¹³⁷⁰ Gabriel de Tarde, dans son ouvrage concernant les lois de l'imitation présentait également l'avènement d'une économie de l'attention. Il écrivait alors: « *Quand on voit une personne curieuse de n'importe quoi dont on se souciait naguère comme d'un fétu, aussitôt on devient désireux de connaître cette chose, et ce mouvement se propage très vite, et, à mesure qu'il se propage, l'intensité de ce désir croît en chacun par l'effet du mutuel reflet. Chaque fois qu'une nouveauté quelconque, en fait de prédication religieuse, de programme politique, d'idées philosophiques, d'articles industriels, de vers, de romans, de drames, d'opéras, apparaît dans un endroit bien visible, c'est-à-dire une capitale, il suffit que l'attention de dix personnes soit ostensiblement fixée sur cette chose pour que bientôt cent, mille, dix mille personnes s'y intéressent et s'y passionnent. Parfois, le phénomène revêt les caractères d'une névrose* », in. TARDE Gabriel, *Les lois de l'imitation – Étude sociologique*, 7ème édition, Paris, Librairie Félix Alcan, 1921, p. 214. On pourrait totalement faire correspondre les mots de Tarde à notre société. En guise d'exemple de la névrose attentionnelle que décrit Tarde, on pourrait évoquer l'application Pokemon GO, qui capte l'attention par l'ambition de la chasse d'animaux virtuellement créés, apparaissant dans les villes, créant des mouvements de foules et parfois d'hystérie (ex.en Chine). Cette application redistribue l'attention en créant par des placements de produits (les Pokemon qu'il faut chasser) situer proche de commerces, de nouveaux besoins, de nouvelles attentions. Cette application correspond bien au phénomène de curiosité attentionnelle que Tarde décrit. Les logiques discursives, les prédications commerciales et politiques provoquent l'installation de cette application vantant son mérite à « manger », « bouger » et « chasser des pokemon ». Voirs: ROY Soline, *Si Pokemon GO ne vous tue pas, il vous rendra (un peu) plus fort*, Le Figaro, 25 août 2016, En ligne: <http://sante.lefigaro.fr/actualite/2016/08/25/25326-si-pokemon-go-ne-vous-tue-pas-il-vous-rendra-peu-plus-fort> (dernière consultation: 5 mars 2018). L'auteur reprend les mots d'un tweet de Marisol Touraine, alors ministre de la Santé, qui écrivait: « *A tous les dresseurs: sortez, marchez, c'est bon pour la santé !* ».

¹³⁷¹ Voir en ce sens: CITTON Yves, *Mythocratie - Storytelling et imaginaire de gauche*, Editions Amsterdam, Paris, 2010.

¹³⁷² Voir en ce sens: CITTON Yves (sous la direction de), *L'économie de l'attention - Nouvel horizon du capitalisme ?*, Editions La Découverte, Paris, 2014; et KESSOUS Emmanuel, *L'attention au monde, sociologie des données personnelles à l'ère du numérique*, Editions Armand Colin, Collection Recherches, 2012

¹³⁷³ BOURDIEU Pierre, *Contre-feux - Pour un mouvement social européen*, Raisons d'Agir, 2001, p. 30.

et Bauman, elle reconfigure les mécanismes disciplinaires à l'oeuvre. Ainsi que le note Jonathan Crary à l'occasion d'une contribution à l'ouvrage de Yves Citton consacré à l'économie de l'attention comme nouvel horizon du capitalisme, « *au début du XX^{ème} siècle, le sujet attentif s'inscrit dans un processus d'internalisation des impératifs disciplinaires, qui implique que les individus soient rendus plus directement responsables de leur propre utilisation efficace et profitable au sein des divers dispositifs sociaux. Et il est certain que les tentatives de détermination des limites d'une attention « normative », à la fin du XIX^{ème} siècle, prenaient part à cette transformation*¹³⁷⁴ ». Et d'ajouter en s'appuyant sur Foucault et Guy Debord¹³⁷⁵, « *Debord et Foucault définissent tous deux des mécanismes de pouvoir diffus, par lesquels des impératifs de normalisation ou de conformité infiltrent la plupart des couches de l'activité sociale pour être subjectivement internalisés. C'est dans ce sens que la gestion de l'attention - qu'elle passe par des formes précoces de culture de masse à la fin du XIX^{ème} siècle, ou qu'elle passe plus tard par la télévision ou l'ordinateur (tout au moins dans leur forme les plus massivement répandues) - a peu à voir avec le contenu visuel de ces écrans, et bien davantage avec une stratégie plus large de gestion des individus. (...). L'attention devient la clef de l'opération des formes de pouvoir non coercitives. (...). La télévision et l'ordinateur personnel, même s'ils convergent maintenant vers un unique modèle de fonctionnement machiniste, sont des processus antinomiques visant à fixer et à strier. Ce sont des méthodes de gestion de l'attention qui utilisent le cloisonnement et la sédentarisation, rendant les corps contrôlables et utiles simultanément, même lorsqu'ils simulent l'illusion du choix et de l'« interactivité »*¹³⁷⁶ ».

627. Ces propos ne sont pas sans rappeler l'ensemble de l'étude liée au Panoptique, et à la rhétorique de l'utilitarisme précédemment développée. La surveillance diffuse est à la fois architecture de pouvoir, et optique de pouvoir. Elle inverse quelque peu l'analyse du Panoptique par Foucault, dans le sens où l'individu n'est plus simplement objet de l'attention, il est à la fois l'acteur principal de ce nouveau contrôle social - son émetteur - , son objet, - le récepteur - mais il est également son principal messageur - le consommateur. L'attention, par les nouvelles technologies qu'elle utilise, le « cloisonne et le sédentarise », le rend « contrôlable et utile », influençable.

¹³⁷⁴ CRARY Jonathan, « Le capitalisme comme crise permanente de l'attention, in. CITTON Yves (sous la direction de), *L'économie de l'attention - Nouvel horizon du capitalisme ?*, Editions La Découverte, Paris, 2014, pp. 35 - 54, p. 52

¹³⁷⁵ Spécialement son ouvrage sur la société du spectacle, où il décrit le spectacle comme un « comportement hypnotique », donc en quelque sorte, comme une captation de l'attention. DEBORD Guy, *La société du spectacle*, Editions Gallimard, Paris, 1992.

¹³⁷⁶ CRARY Jonathan, Op. Cit. p. 53 - 54.

B. Du mythe « je n'ai rien à cacher, je n'ai rien à me reprocher » comme pleine intériorisation du contrôle social

628. L'analyse du mythe « je n'ai rien à cacher, je n'ai rien à me reprocher » (1) est particulièrement éclairante quant à l'intériorisation de l'attention comme nouveau contrôle social (2) Elle permet de démontrer la prégnance d'une forme d'auto-contrôle engendrée par l'attention.

1. L'analyse du mythe « je n'ai rien à cacher je n'ai rien à me reprocher »: ou la crédulité des individus ?

629. Face à la surveillance diffuse, il n'est pas rare que l'opinion publique affirme être prête à délaissier un peu de liberté au bénéfice de la sécurité et de la lutte contre le terrorisme, ou encore qu'il n'est pas gênant que des réseaux sociaux ou des moteurs de recherche puissent collecter des données les concernant puisqu'ils n'ont globalement rien à cacher. Ces éléments sont souvent résumés sous le mythe, ou le syndrome du « rien à cacher, rien à se reprocher », et est assez bien envisagé sous la plume d'Alex Türk. En 2011, alors Président de la CNIL, ce dernier écrit: *« parmi ceux que nous avons appelés plus haut les « naïfs » se trouvent d'abord les usagers qui sont parfaitement conscients des capacités des acteurs du réseau à identifier, capter et manipuler leurs données, et donc analyser leurs comportements, cerner leurs goûts et ainsi établir leurs profils. Mais, disent-ils, cela ne leur pose aucun problème car « ils n'ont rien à cacher ni rien à se reprocher ». Précisions que ce syndrome du « rien à cacher rien à me reprocher » peut concerner aussi bien les familiers des moteurs de recherche et des réseaux sociaux que les personnes susceptibles de faire l'objet d'une prise de vue ou d'une géolocalisation, à leur insu ou non. Et il s'agit d'un des plus redoutables adversaires d'une institutions, telle que la CNIL, chargée d'assurer l'équilibre entre la protection des données personnelles et de la vie privée et le développement des nouvelles technologies de l'information¹³⁷⁷ ».*

630. Bien que le propos général soit séduisant, il semble qu'il soit hâtif de voir en l'individu un être *« naïf (...) parfaitement conscient (s) des capacités des acteurs du réseau »*, et ce au regard de la surveillance diffuse, et de son double objectif: sécurité et liberté (de consommation). Les

¹³⁷⁷ TURK Alex, *La vie privée en péril. Des citoyens sous contrôle*, Paris, Odile Jacob, 2011, p. 125.

affirmations de deux PDG d'entreprise de la Silicon Valley donnent le ton de cette affirmation. En 2009, dans le cadre d'une interview, le président de Google, Eric Schmidt déclare : « *S'il y a quelque chose que vous voudriez que personne ne sache, peut être que vous devriez commencer par ne pas la faire*¹³⁷⁸ ». Un an plus tard, Mark Zuckerberg, PDG de Facebook, déclare: « *les gens ont pris l'habitude non seulement de partager plus d'informations de toutes sortes, mais ils le font de façon plus ouverte et avec plus de gens*¹³⁷⁹ », et de poursuivre sur le fait qu'il avait contribué à établir un changement de vision des individus sur leur vie privée, concluant que cette dernière n'est plus « *une norme sociale*¹³⁸⁰ ». Malgré la compréhension des réseaux sociaux et des moteurs de recherche, et de la volonté de ces deux personnages publics de rester cachés, et donc de protéger âprement leur vie privée¹³⁸¹, Eric Schmidt a décidé de ne plus accepter d'interview avec certains journalistes, à la suite de révélations concernant des informations personnelles, telles que son salaire, ses voisins, ses hobbies¹³⁸². Il semble, dans un premier temps, qu'il faille donc conclure à l'impossibilité de vivre caché dans nos sociétés contemporaines.

631. Bien que la surveillance diffuse a contribué à rendre le monde contemporain transparent, ces deux exemples montrent bien que des personnes souhaitant préserver leur vie privée, ne le peuvent plus vraiment. Au syndrome du « je n'ai rien à cacher, je n'ai rien à me reprocher », il faudrait ajouter: « puisqu'aujourd'hui tout se sait ». Tout ce qu'on dit, écrit, l'ensemble des traces que nous laissons, peuvent être repérés, enregistrés et archivés pour une durée plus ou moins longue dans des data center qui pourront servir si l'occasion se présente. Les technologies de l'information et de la communication aident clairement cette situation, et le peu de clarté et la lourdeur de certaines

¹³⁷⁸ SCHMIDT Eric, PDG de Gogle, à propos de la vie privée, interview donnée à la chaîne CNBC, Disponible en ligne: <https://www.youtube.com/watch?v=A6e7wfdHzew> (dernière consultation: 5 mars 2018)

¹³⁷⁹ JOHNSON Bobbie, *Privacy no longer a social norm, says Facebook founder*, The Guardian, 11 janvier 2010, En ligne: <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> (dernière consultation: 5 mars 2018)

¹³⁸⁰ Ibid.

¹³⁸¹ Zuckerberg, a également acquis les quatre propriétés adjacentes pour ne pas être dérangé, ou encore 144 hectares d'une île hawaïenne. Schmidt, quant à lui, s'est offert un appartement avec ascenseur particulier sans concierge pour, là aussi, protéger sa vie privée... Voir: FOURMY Marc, *Mark Zuckerberg s'offre un bout d'île à Hawaï*, Le Point, 3 octobre 2014, En ligne: http://www.lepoint.fr/people/mark-zuckerberg-s-offre-un-bout-d-ile-a-hawai-03-10-2014-1869024_2116.php (dernière consultation: 5 mars 2018), AMIRA Dan, *Inside Google Chairman Eric Schmidt's Lavish Sex Palace*, Daily Intelligencer, 25 juillet 2013, En ligne: <http://nymag.com/daily/intelligencer/2013/07/eric-schmidt-penthouse-new-york-photos-apartment.html> (dernière consultation: 5 mars 2018)

¹³⁸² Voir en ce sens: WESTHOVEN Jennifer, *CNET: We've been blackballed by Google*, CNN, 5 août 2005, En ligne: http://money.cnn.com/2005/08/05/technology/google_cnet/ (dernière consultation: 5 mars 2018). Ce qui amène à l'ironie de certains journalistes, et spécialement Cory Doctorow qui écrit: « *Hey, Eric: if you don't want us to know how much money you make, where you live, and what you do with your spare time, maybe you shouldn't have a house, earn a salary, or have any hobbies, right ?* » in . DOCTOROW Cory, *Google CEO Says privacy doesn't matter. google blacklists CNet for violating CEO's privacy*, 9 décembre 2009, En ligne: <http://boingboing.net/2009/12/09/google-ceo-says-priv.html> (dernière consultation: 5 mars 2018)

conditions générales d'utilisation et politique de confidentialité de ces sites Internet¹³⁸³ contribuent à la prolifération inconsciente d'informations personnelles. Entre absence de consentement réellement éclairé, ainsi que le droit privé l'impose, et prolifération technologique¹³⁸⁴; l'argument de la naïveté des individus est quelque peu mis à mal.

2.L'affirmation d'un auto-contrôle des individus par l'intériorisation de l'attention

632. Le néolibéralisme économique et sécuritaire, fondé sur une rhétorique de l'utilitarisme, souhaite tout voir, tout savoir, et ce, dans un triple objectif: la sécurité, la liberté, et la satisfaction d'intérêt personnel dans une société de consommation. Couplés à l'analyse de l'attention comme nouveau contrôle social, ces éléments ne sont pas sans évoquer la pensée de Michalis Lianos qui déclarait que: « *le contrôle périoptique est un effet de l'organisation efficace que la société des institutions impose à ses sujets. Ce n'est pas le contrôle qui se désocialise mais la socialité qui s'institutionnalise; ce n'est pas la surveillance qui s'approfondit et s'étend mais la demande pour des systèmes et des réseaux favorisant la fluidité atomisée qui se propage; ce n'est pas la liberté qui régresse mais son contenu qui se déplace; ce n'est pas la stratification qui disparaît mais sa dépendance des jonctions institutionnelles qui augmente; ce n'est pas la norme et sa fonctionnalité socialisante qui s'effondrent mais leur fondement en dehors des valeurs intériorisées qui se construit*¹³⁸⁵ ». Le contrôle périoptique décrit par Michalis Lianos organise les possibilités d'action de l'individu autour de l'action effectivement contrôlée, c'est-à-dire celle qui est déjà envisagée comme possible. Les nouvelles technologies permettant de comprendre à l'avance le choix d'action du sujet, de l'orienter, de l'inciter, les possibilités d'action de l'individu doivent alors correspondre. Il s'agit ici de séduire l'individu, pour opérer ensuite une coordination utile de son action. La

¹³⁸³ Pour preuve, on citera un commentaire remarquable de l'Electronic Frontier Foundation qui retrace les étapes importantes de la politique de confidentialité de Facebook, pointant du doigt ses modifications quasiment chaque année depuis 2005. OPSAHL Kurt, *Facebook's eroding privacy policy: a timeline*, Electronic Frontier Foundation, 28 avril 2010, En ligne: <https://www.eff.org/deeplinks/2010/04/facebook-timeline/> (dernière consultation: 5 mars 2018)

¹³⁸⁴ Dont les API (interface de programmation applicative qui permettent à des (sociétés) tiers de se connecter à un service ou à ses données pour proposer d'autres services), les social bar, le like universel. Voir en ce sens: PISANI Francis, *La nouvelle plateforme Facebook : séduisante et dangereuse*, 4 mai 2010, Le Monde, En ligne: <http://pisani.blog.lemonde.fr/2010/05/04/la-nouvelle-plateforme-facebook-seduisante-et-dangereuse/> (dernière consultation: 5 mars 2018), et sur les API: un article concernant *l'open-graph de Facebook (qui) distribue les données privées des utilisateurs*, du 17 janvier 2011, En ligne: <http://www.commentcamarche.net/news/5853945-l-open-graph-de-facebook-distribue-les-donnees-privées-des-utilisateurs> (dernière consultation: 5 mars 2018), ou encore, GUILLOUX Michael, *Geofeedia a surveillé les utilisateurs de Twitter; Facebook et Instagram pour la police - la start-up avait un accès commercial à leurs données*, 12 octobre 2016, En ligne: <https://www.developpez.com/actu/105233/Geofeedia-a-surveille-les-utilisateurs-de-Twitter-Facebook-et-Instagram-pour-la-police-la-startup-avait-un-acces-commercial-a-leurs-donnees/> (dernière consultation: 5 mars 2018)

¹³⁸⁵ LIANOS Michalis, *Le nouveau contrôle social - Toile institutionnelle, normativité et lien social*, Editions L'Harmattan, Collection Logiques Sociales, 2001, p. 201

caméra de vidéosurveillance est devenue banale car elle donne aux individus un sentiment de sécurité. Par sa dynamique propre de reproduction du regard et de la visibilité, elle force les individus à se conformer aux attentes du lieu dans lequel ils se trouvent filmés.

633. Selon Michalis Lianos, le nouveau contrôle social permet d'exercer une sorte de pouvoir sur le choix individuel, choix qu'il rapproche de la notion de liberté¹³⁸⁶. Aussi, par une logique « *d'inspection* », de « *socio-cognition* », voire plutôt d'attention¹³⁸⁷, on « *préconise au sujet de ce comportement une voie d'action entre des limites bien définies*¹³⁸⁸ ». Ces limites bien définies, Lianos les constate dans ce nouveau mode de contrôle qui « *ne s'oriente pas vers la surveillance mais vers la motivation autonome et différentielle*¹³⁸⁹ ». Au vu des éléments développés concernant la rhétorique de l'utilitarisme et les logiques attentionnelles que contient la surveillance diffuse, il est possible de réfuter la première partie de l'assertion de l'auteur. Pour autant, la motivation autonome et différentielle décrite par le Professeur Lianos semble pleinement s'inscrire dans le projet de la surveillance diffuse, et dans la définition qu'opère David Lyon à ce sujet¹³⁹⁰. L'influence, la gestion, la direction et la protection sont bien les buts essentiels de ce nouveau contrôle social, mais également de la surveillance diffuse. Aussi, et comme le note Michalis Lianos, la surveillance apparaît dans des circonstances où « *le sujet post-industriel est inondé de messages institutionnels qui lui indiquent constamment des façons de penser et d'agir privilégiant des projets*

¹³⁸⁶ Voir en ce sens l'ensemble de l'introduction du livre précité, où Lianos démontre bien que le nouveau contrôle social ne s'exerce plus par une forme de coercition, de contrainte, mais bien plutôt par une fusion de la contrainte et de la liberté, permettant d'orienter les choix comportementaux. Il écrit ainsi que « *le contrôle post-industriel consiste en de nouvelles façons de générerait d'imposer des prescriptions comportementales* ». (Ibid. p. 30)

¹³⁸⁷ Sur la possibilité de rapprocher les notions de socio-cognition et d'inspection au coeur du nouveau contrôle social développé par Lianos, ce dernier écrit: « *ce n'est plus la force brutale d'un centre inculquant la conformité qui contrôle les sujets contemporains, mais la capacité d'attirer leurs regards qui, par cette focalisation commune mais atomisée, établit et légitime leur point de convergence comme un centre de facto de normativité.(...). L'institution devient un périoste, c'est-à-dire un point de focalisation multiple, et par là-même un lieu de socialisation, sans l'avoir souhaité et sans s'intéresser à cette fonction. Qu'il s'agisse d'une star hollywoodienne, d'un conglomérat industriel, d'un moteur de recherche sur Internet ou d'une chaîne de grands magasins, les regards et les pratiques individuels convergents ne sont ni proposés, ni reçus sur un fondement moral ou même axiologique; ils représentent tout simplement une utilité massive dans un capitalisme libéral. De ce point de vue, le contrôle périodique approfondit la désocialisation de la norme en se propageant par des cercles toujours plus étendus et rompt très clairement avec toute coercition* ». (p.32 - 33). L'auteur développe ensuite les moyens d'action de ce nouveau contrôle social, c'est-à-dire « *le socio-cognitif: (la) légitimité, (l') inspection, (la) technologie* » voir pp. 33 - 42. L'ensemble de ces éléments tend à s'insérer pleinement dans les propos développés précédemment concernant l'attention, la rhétorique de l'utilitarisme et le Panoptique. Nous soulignons notre désaccord avec Lianos lorsqu'il s'emploie à amoindrir les effets et l'ambition de la surveillance diffuse. La surveillance est dans la rhétorique utilitariste de la gouvernance néo-libérale, que Lianos pointe du doigt, le principal outil pour parvenir à ce qu'il appelle l'inspection, le socio-cognitif, et le modelage des choix des individus. Rappelons ici, les propos de Christian Laval: « *La sécurité est la condition du bonheur général. Le bonheur est le grand but, la surveillance qui conditionne la sécurité est le principal levier pour y parvenir* ». (Op. Cit.)

¹³⁸⁸ Ibid. p. 37

¹³⁸⁹ Ibid. p. 31

¹³⁹⁰ Cf. Introduction générale.

*d'actions préfabriqués. la prolifération vertigineuse des choix, mais toujours des choix d'adhésion, représente la science actuellement établie de la liberté*¹³⁹¹ ». Et de poursuivre : « *loin de la surveillance centralisée, le contrôle social émerge dans ces circonstances comme un apprentissage à la conformité autour de plusieurs pôles en compétition*¹³⁹² ». Ces propos s'inscrivent pleinement dans la logique du syndrome du « je n'ai rien à cacher je n'ai rien à me reprocher ». A partir de l'exemple de la vidéosurveillance, de la vidéoprotection, et plus globalement des nouvelles technologies sécuritaires, il est possible de faire apparaître la logique des choix d'adhésion pointée du doigt par le Professeur Lianos. Les approches de types socio-criminologiques, prônées par quelques « experts », visant à démontrer l'effet dissuasif des caméras installées sur la voie publique contre la délinquance¹³⁹³, tendent à participer à l'acceptabilité de la vidéosurveillance. Plus loin encore, les approches socio-politiques qui analysent les ambitions implicites de ce dispositif¹³⁹⁴ conduisent à rendre la vidéosurveillance conforme à son but affiché, et non, à y renoncer. L'ensemble des discours liés à la question de l'efficacité de cette technologie, aux buts explicites et implicites de cette dernière, contribue dans les faits, et au delà de l'acceptabilité sociale¹³⁹⁵ de ces dispositifs, à rendre, aux yeux de l'opinion publique, légitime leur usage.

634. Plus globalement, la même logique peut être retrouvée dans la construction de la société de l'information, et plus tard de la surveillance diffuse. Sous couvert d'un storytelling prônant les bénéfices d'une vie ultra-connectée, les individus n'ont pas eu d'autres choix que d'adhérer à

¹³⁹¹ Ibid. p. 32

¹³⁹² Ibid.

¹³⁹³ Rapport Bauer précédemment cité, ainsi que l'étude de Le Goff et Heilmann concernant ce rapport (Op. Cit), LECLERC Jean-Marc, *Videosurveillance: le rapport qui prouve son efficacité*, Le Figaro, 21 août 2009, En ligne: <http://www.lefigaro.fr/actualite-france/2009/08/21/01016-20090821ARTFIG00361-videosurveillance-le-rapport-qui-prouve-son-efficacite-.php> (dernière consultation: 5 mars 2018)

¹³⁹⁴ Giorgio Agamben écrit: « *J'appelle dispositif tout ce qui a, d'une manière ou d'une autre, la capacité de capturer, d'orienter, de déterminer, d'intercepter, de modeler, de contrôler et d'assurer les gestes, les conduites, les opinions et les discours des êtres vivants* ». In. AGAMBEN Giorgio, *Qu'est ce qu'un dispositif?*, Editions Rivages, Collection Rivage poche, 2014, p. 31

¹³⁹⁵ La notion d'acceptabilité sociale est devenue omniprésente dans les discours et débats publics, dans les conduites de projet touchant à la sécurité et aux nouvelles technologies. Ce terme, à l'image de la notion de « responsabilité sociale » qui se répand de nos jours, ne revêt que peu de sens puisque « *malléable et manipulable à toutes fins, utilisée de façon pragmatique, sans références explicites à des fondements conceptuels et théoriques rigoureusement établis* » (in. BATTELIER Pierre, *Acceptabilité sociale, cartographie d'une notion et de ses usages*, Cahier de recherches, 2015, UQAM : les publications du Centr'ERE, p. i). Cette notion revêt une multitude d'acceptions, et implique de nombreux concepts sous-jacents qui viennent ajouter à la complexité des termes. Ce concept souffre d'un problème de perception, chaque acteur ayant sa propre perception de la notion. Le terme accepter revêt une dualité de dimension : positive et proactive, et négative et passive. La conditionnalité qu'emporte l'acceptabilité est largement dépendante de la mise en scène du construit technologique, c'est-à-dire à la fois du risque d'attaques malveillantes ou terroristes, plus globalement de la notion de droit à la sécurité, mais également des technologies envisagées. Voir également: BOISSONADE Jérôme (sous la direction de), *Mettre à l'épreuve l'acceptabilité sociale*, Vertigo, Volume 15 numéro 3, décembre 2015, En ligne: <https://vertigo.revues.org/16679> (dernière consultation: 5 mars 2018)

l'utilisation d'Internet, des smartphones, et bientôt à la Smart-city¹³⁹⁶. En réalité, couplé au discours de l'opinion publique et au mythe du « je n'ai rien à cacher, je n'ai rien à me reprocher », l'ensemble de ces éléments tend moins à dénoncer la naïveté des individus, pour reprendre les termes de Alex Türk, que d'explorer une double dimension correspondant d'une part à ce que Norbert Elias évoque sous le terme d'auto-contrôle¹³⁹⁷, voire plus globalement, à ce que Walter Lippmann¹³⁹⁸, Harold Lasswell¹³⁹⁹, Jacques Ellul¹⁴⁰⁰, et Noam Chomsky¹⁴⁰¹ évoquent sous le nom de propagande technologique et de fabrique du consentement.

¹³⁹⁶ Ces mots rappellent à nouveau l'utilitarisme de la surveillance diffuse dans une économie néo-libérale. Les conséquences du discours néo-libéral, et son effet de lissage des comportements individuels avait déjà été démontré par Pierre Bourdieu. Ce dernier écrivait: « *De cette sorte de faute originelle, inscrite dans le mythe walrasien de la « théorie pure », découlent tous les manques et tous les manquements de la discipline économique, et l'obstination fatale avec laquelle elle s'accroche à l'opposition arbitraire qu'elle fait exister, par sa seule existence, entre la logique proprement économique, fondée sur la concurrence et porteuse d'efficacité, et la logique sociale, soumise à la règle de l'équité. Cela dit, cette « théorie » originellement désocialisée et déshistoricisée a, aujourd'hui plus que jamais, les moyens de se rendre vraie, empiriquement vérifiable. En effet, le discours néolibéral n'est pas un discours comme les autres. (...). Au nom de ce programme scientifique de connaissance, converti en programme politique d'action, s'accomplit un immense travail politique (déné puisé, en apparence, purement négatif) qui vise à créer les conditions de réalisation et de fonctionnement de la « théorie » ; un programme de destruction méthodique des collectifs » BOURDIEU Pierre, *L'essence du néolibéralisme*, Le Monde Diplomatique, Mars 1998, p. 3, En ligne: <http://www.monde-diplomatique.fr/1998/03/BOURDIEU/3609> (dernière consultation: 5 mars 2018)*

¹³⁹⁷ La surveillance diffuse doit être comprise comme un dispositif étatique et économique qui participe du processus de « *civilisation des moeurs* » décrit par Elias. A travers les oeuvres de Norbert Elias, la « *dynamique de l'Occident* », nos sociétés contemporaines sont caractérisées par l'aboutissement historique et sociologique du passage d'une contrainte imposée de l'extérieur (le monopole étatique de la violence), à une forme d'auto-contrainte rendue possible par l'intériorisation du contrôle des comportements, des émotions, des pulsions (la maîtrise de soi). Norbert Elias note ainsi, « *qu'au mécanisme de contrôle et de surveillance de la société correspond ici l'appareil de contrôle qui se forme dans l'économie psychique de l'individu* » (in. ELIAS Norbert, *La dynamique de l'occident*, Editions Calmann-Lévy, 1975, p. 210. Voir également du même auteur, *La civilisation des moeurs*, Editions Calmann-Lévy, Collection Pocket, 1973; *La société des individus*, Editons Fayard, Collection Agora, 1991).

¹³⁹⁸ Voir: LIPPMANN Walter, *Public opinion*, New York, Harcourt, Brace and Company, 1922; et, du même auteur, *The Phantom Public*, New York, Harcourt, Brace and Company, 1925. Dans le premier ouvrage, Lippmann écrit : « *the symbols of public opinion, in times of moderate security, are subject to check and comparison and argument. (...). There is, after all, just one human activity left in which whole populations accomplish the union sacrée. It occurs in those middle phases of a war when fear, pugnacity, and hatred have secured complete dominion of the spirit, either to crush every other instinct or to enlist it, and before weariness is left* » (p. 11). Nous soutenons ici que par le recours toujours plus englobant au droit à la sécurité, à la lutte contre le terrorisme, l'opinion publique a pu être forgée, « *dominée* » et préparée à la banalisation de l'implémentation de dispositifs socio-techniques. Il écrit ensuite que: « *within the life of the generation now in control of affairs, persuasion has become a self-conscious art and a regular organ of popular government. None of us begins to understand the consequences, but it is no daring prophecy to say that the knowledge how to create consent will alter every political calculation and modify every political premise. Under the impact of propaganda, not necessarily in the sinister meaning of the word alone, the old constants of our thinking have become variables. It is no longer possible, for example, to believe in the original dogma of democracy; that the knowledge needed for the management of human affairs comes up spontaneously from the human heart*». (p. 248 - 249). Dans le second ouvrage, Lippmann peaufine son analyse en s'intéressant aux effets de la fabrique du consentement, et écrit que le citoyen contemporain est un homme désenchanté. Plus précisément: « *the private citizen today has come to feel rather like a deaf spectator in the back row, who ought keep his mind on the mystery off there, but cannot quite manage to keep awake. He knows he is somehow affected by what is going on. Rules and regulations continually; taxes annually and wars occasionally remind him that he is being swept along by great drifts or circumstance* » (p. 3).

¹³⁹⁹ Voir en ce sens: LASSWELL Harold, *Propagande technique in the World War*, Alfred Knopf Inc., New York, 1927 (et plus particulièrement son introduction où il évoque la mobilisation de l'opinion (p. 14))

¹⁴⁰⁰ Voir les trois ouvrages fondateurs de la pensée de Jacques Ellul concernant la Technique (Op. Cit.)

¹⁴⁰¹ Voir : CHOMSKY Noam, HERMAN Edward, *La fabrication du consentement - De la propagande médiatique en démocratie*, Editions Agone, Collection Contre-feux, 2008

635. Le lien entre la surveillance diffuse et le contrôle social n'est plus à démontrer. Depuis les analyses de Bentham et Foucault, il est admis que la surveillance participe du contrôle social. Néanmoins, par la démonstration de la double nature de la surveillance diffuse, il a été possible de démontrer non pas qu'il existe aujourd'hui plus ou moins de contrôle, mais bien de prouver une mutation de ce dernier. Par l'économie de l'attention, le discours néo-libéral fondé sur la rhétorique de l'utilitarisme, le contrôle social est aujourd'hui pleinement intériorisé et positif. Il n'est plus l'enjeu de l'enfermement des corps, mais de la discipline des esprits, réunissant contrainte et liberté. Notons avec Michalis Lianos que le « *danger se trouve*¹⁴⁰² » aujourd'hui « *dans la fusion totale entre liberté, satisfaction et contrôle et la passivité volontaire qui peut s'ensuivre*¹⁴⁰³ ». Rappelons également avec Jean-Jacques Rousseau que « *il n'y a point d'assujettissement si parfait que celui qui garde l'apparence de la liberté, on capture ainsi la volonté même. Le pauvre enfant qui ne sait rien, qui ne peut rien, qui ne connaît rien, n'est-il pas à votre merci? Ne disposez-vous pas, par rapport à lui, de tout ce qui l'entourne? N'êtes-vous pas le maître de l'affecter comme il vous plaît? Ses travaux, ses jeux, ses plaisirs, ses peines; tout n'est-il pas dans vos mains sans qu'il le sache? Sans doute, il ne doit faire que ce qu'il veut; mais il ne doit vouloir que ce que vous voulez qu'il fasse; il ne doit pas faire un pas que vous ne l'ayez prévu, il ne doit pas ouvrir la bouche que vous ne sachiez ce qu'il va dire*¹⁴⁰⁴ ».

Section 2: L'objectivation des individus par la surveillance diffuse: transformation des sujets de droit et désinstitution du Droit

636. Le questionnement lié à l'objectivation des individus a très vite été central dans les études liées à la société de l'information. François Rigaux déclarait ainsi que ce « *phénomène est aussi ancien que le passage de l'humanité à une vie sociale organisée. (...). Toute société humaine a été depuis l'origine et n'a pas cessé d'être une « société de l'information », celle-ci étant l'expression même du lien social. Que l'individu ait besoin de protection dans une société de l'information (...),*

¹⁴⁰² LIANOS Michalis, Op. Cit, p. 204

¹⁴⁰³ Ibid.

¹⁴⁰⁴ ROUSSEAU Jean-Jacques, *Oeuvres complètes - Tome deuxième - La nouvelles héloïse, Emile, Lettre à M. de Beaumont*, Chez Furne, Librairie - Editeur, Paris, p. 460.

suscite une interrogation fondamentale¹⁴⁰⁵ ». Et de poursuivre: « La liberté d'expression et la liberté contractuelle ont été le terrain de nouvelles méthodes d'exercice du pouvoir des grandes entreprises. Celles-ci maîtrisent des informations nombreuses et diversifiées qui leur permettent de donner au marché les orientations qui leur conviennent et elles tiennent aussi à jour une information personnalisée sur les choix, les goûts, le genre de vie de leurs clients. Si l'on ajoute que les principaux moyens d'information — une presse de plus en plus concentrée et les organes audiovisuels — sont aujourd'hui privatisés, la société de l'information met face à face des entreprises puissantes et des individus largement transformés en simples objets d'informations ou de données qui leur sont personnelles et dont ils ont perdu la maîtrise¹⁴⁰⁶ ».

637. La surveillance diffuse a permis l'aboutissement de la transformation de l'individu en simple objet d'information. Bien que Rigaux poursuit son analyse en portant son raisonnement sur les raisons d'une protection spécifique de l'individu dans la société de l'information, la construction d'un droit libéral se rapportant aux données et à la vie privée n'était, à l'époque de son analyse, pas encore abouti. De fait, l'objectivation des individus (paragraphe 1) engendre une forme nouvelle de désinstitution du Droit, ou, à tout le moins d'une transformation de ce dernier. Par la normalisation constante des comportements des individus, le Droit passe d'une volonté de régler à une fonction de régulation, de gouvernance des risques et des menaces. S'il n'est pas désinstitutionné, le Droit est au moins en perte de symbolique. Ce n'est plus forcément le Droit qui régule, mais la surveillance diffuse qui normalise, homogénéise les comportements, et engendre un conformisme social. Plus encore, on constate l'apparition de nouvelles formes de régulation propres à la surveillance diffuse. La technique des nudges doit ici être interrogée afin de comprendre pleinement la perte de symbolique du Droit, voire sa désinstitution totale (paragraphe 2)

Paragraphe 1: La surveillance diffuse ou l'objectivation des individus

638. La surveillance diffuse permet la réalisation du passage du gouvernement des hommes à l'administration des choses. Plus que le fait de dire que la surveillance diffuse participe à la création de profils les plus individualisés possibles, il faut ici comprendre l'ambition de ces profils à vouloir créer un savoir objectif sur les individus. L'individu échange son caractère subjectif (A) au profit

¹⁴⁰⁵ RIGAUD François, *L'individu, sujet ou objet de la société de l'information*, Groupe d'études Société de l'information et vie privée, p. 122, En ligne: <https://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr6.pdf> (dernière consultation: 5 mars 2018)

¹⁴⁰⁶ Ibid. p. 124

d'un corps statistique (B).

A. Du sujet de Droit ...

639. Evoquer le sujet de droit revient à interroger la fonction du droit au regard des individus. Le droit institue tout d'abord l'individu en tant que sujet de droit (1). Il permet, interdit et juge la conformité des comportements individuels en fonction de règles de droit prescrites par la loi (2).

1. L'institutionnalisation par le Droit de l'individu en tant que sujet de Droit

640. La fonction première du Droit est de permettre à l'individu d'être reconnu dans la société comme un sujet de droit. Ainsi que le rappelle Alain Supiot, « *le sujet de droit est certes un sujet souverain, c'est-à-dire un être qui naît « libre et doué de raison », qui peut donc se gouverner lui-même et se soumettre le monde des objets. (...). Mais il n'accède à cette liberté que dans la mesure où il demeure un sujet au sens étymologique et premier du mot, c'est-à-dire un être assujetti au respect des lois (sub-jectum: jeté dessous), qu'il s'agisse des lois de la Cité ou des lois de la science. Promouvoir ce sujet à deux faces est notre manière d'instituer l'Homme, d'en faire un sujet de droit qui puise dans l'hétéronomie de la loi les moyens de son autonomie¹⁴⁰⁷ ».*

641. Ce n'est pas le lien du sang de la naissance qui permet à l'individu d'être vu et analysé comme un sujet de droit au sein de la société. De part sa naissance, sa filiation est reconnue par l'autorité publique, il naît alors sujet de droit par sa reconnaissance à l'état civil. Par là, il devient alors sujet de la loi et détenteur de devoir vis à vis de cette même société. François Ost décrit cet individu entrant dans la société « *en assumant sa place dans la lignée et en acceptant le principe de dissymétrie qui la caractérise¹⁴⁰⁸ »* comme « *un relais de la loi* », ou comme le voyait Rousseau un co-contractant du contrat social. Par la reconnaissance de la personnalité juridique à la naissance, le Droit reconnaît à l'individu son aptitude à être titulaire de droit subjectif et redevables de droits. Le droit objectif est un ensemble de règles tendant à la régulation des comportements humains et qui bénéficie du monopole de la contrainte étatique. Les droits subjectifs sont quant à eux les prérogatives individuelles, les droits individuels que certaines règles du droit objectif reconnaissent à une personne (la propriété, la vie privée par exemple). La particularité essentielle du Droit est

¹⁴⁰⁷ SUPIOT Alain, *Homo juridicus Op. Cit.*, p. 55

¹⁴⁰⁸ OST François, *Le temps du Droit*, Odile Jacob, Novembre 1999, Paris, p. 65.

qu'il se réfère à un sujet, le sujet de droit, qu'il considère autonome, libre et doué de raison. L'Etat est garant de la reconnaissance souveraine de la personnalité juridique des individus.

642. Cette personnalité juridique doit être approfondie. Si le droit reconnaît la capacité d'un individu à entrer dans la Cité, c'est bien parce qu'il le considère comme un esprit pensant, un être doué de raison. La Déclaration Universelle des Droits de l'Homme rappelle d'ailleurs ce principe dès son article 1er: « *tous les êtres humains naissent libres et égaux en dignité et en droits. Ils sont doués de raison et de conscience et doivent agir les uns envers les autres dans un esprit de fraternité* », et de confirmer en son article 6 que « *chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique* ». La personnalité juridique est, au travers l'esprit de ce texte (article 29), un moyen de garantir à l'individu, sujet de droit, « *le libre et le plein développement de sa personnalité* ». La fiction juridique du sujet de droit et de la personnalité juridique s'appuie sur une dimension anthropologique claire. Comme le démontre Alain Supiot: « *la personnalité est ainsi le concept générique qui permet de faire tenir ensemble le corps et l'esprit. Elle transcende la nature mortelle de chaque homme pour le faire participer à l'immortalité de l'esprit humain. (...). la personnalité juridique (...) est comme une page blanche sur laquelle il lui appartient d'apposer la marque de son esprit*¹⁴⁰⁹ ». La personne - sujet de droit - n'est pas une chose en ce qu'elle est capable d'autonomie, de pensées, de raison. Bien que ce propos doive quelque peu être nuancé, au vu de la réforme du statut juridique des animaux les reconnaissant comme « *des êtres vivants doués de sensibilité*¹⁴¹⁰ », il reste que seul l'individu dispose de droits et est soumis à des devoirs

2.L'imposition par le Droit de la conformité des comportements à la loi

643. Le principal devoir que l'individu - sujet de droit a, est celui de respecter la loi, en ce qu'elle permet et interdit, et/ou oblige et interdit des comportements. Ainsi que le rappelle Foucault, la loi participe d'une normativité: « *cette normativité de la loi, fondatrice peut-être de la loi, ne peut en aucun cas être confondue avec ce qu'on essaie de repérer sous le nom de procédures, techniques de normalisation (...). Si la loi se réfère à une norme, la loi a donc pour rôle et fonction de codifier une norme (...), j'essaie de repérer comment, en dessous, dans les marges et peut-être même à*

¹⁴⁰⁹ SUPIOT Alain, *Homo juridicus*, Op. Cit. P. 58

¹⁴¹⁰ Le nouvel article 515-14 du Code civil déclare: « *Les animaux sont des êtres vivants doués de sensibilité. Sous réserve des lois qui les protègent, les animaux sont soumis au régime des biens* ». Pour une analyse intéressante de ce sujet voir: CHANTEUR Janine, *Du droit des bêtes à disposer d'elles-mêmes*, Editions du Seuil, Collection Couleur des idées, 1993

contresens d'un système de la loi se développent des techniques de normalisation¹⁴¹¹ ». La normativité de la loi ne doit pas être entendue de la même manière que la normativité du contrôle social attentionnel, la loi permet la réglementation de problèmes de société, de faire entrer le social ou des pratiques sociales, dans le droit. La norme sociale précède la loi, et la loi lui donne forme et force juridique. On pourrait par exemple citer ici la reconnaissance en France d'un droit à l'interruption volontaire de grossesse en 1975.

644. Ainsi qu'Antoinette Rouvroy le mentionne le droit *« s'éprouve, dans le processus de subjectivation juridique que déclenche l'interpellation qu'elle lance aux individus, la manière qu'il a de s'adresser à eux. En réponse à l'interpellation du droit, les individus se positionnent comme sujets d'un droit qu'ils « éprouvent » en y mesurant leurs « raisons » et « motivations », et en reconnaissant leurs actes comme les leurs propres¹⁴¹² ». La loi et le Droit sont à la fois reconnaissance d'une action possible ou obligatoire, mais également technique de l'interdit et de la sanction. S'appuyant sur les analyses de Jérémie Bentham, l'auteur analyse l'action possible, obligatoire ou interdite comme suit: « « gouverner » avec de la loi consiste à produire une certaine régularité dans les comportements en incitant les individus à choisir, parmi toutes les conduites possibles, c'est-à-dire parmi toutes les choses qu'ils peuvent (qu'ils ont la possibilité de) faire ou qu'ils peuvent s'abstenir de faire, celles qui sont les plus compatibles avec les intérêts de la communauté¹⁴¹³ ». Et, c'est entre cette direction qu'elle adresse aux sujets de Droit, et la crainte de la sanction (la technique de l'interdit), que le sujet de Droit s'inscrit dans la société. La technique de l'interdit se résume en réalité à deux éléments cruciaux du droit: la fonction d'interprétation du droit et la fonction de dire le droit principalement garantie par le juge. Le juge est le gardien de la Constitution et la justice, la gardienne du droit. Ces deux fonctions représentent la principale garantie d'une vie en société démocratique. Ainsi que les propos de Alain Supiot le rappellent: « le Droit est ainsi devenue une technique de l'Interdit. C'est une technique parce que son sens n'est pas enfermé dans la Lettre d'un Texte sacré et immuable (...). Mais c'est une technique de l'Interdit, qui interpose, dans les rapports de chacun à autrui et au monde, un sens commun qui les dépasse et l'oblige, et fait de lui un simple maillon de la chaîne humaine. Le Droit peut donc servir des fins diverses et changeantes, aussi bien dans l'histoire des systèmes politiques que dans celle des sciences et des technique , mais il les sert en subordonnant le pouvoir et la technique à une raison*

¹⁴¹¹ FOUCAULT Michel, *Sécurité, territoire, population*, Op. Cit, p. 59

¹⁴¹² ROUVROY Antoinette, « Pour une défense de l'éprouvant inopérationalité du droit (...) », Op. Cit., p. 148

¹⁴¹³ Ibid. p. 146

*humaine*¹⁴¹⁴ ».

645. Le Droit et la loi ne sont pas réductibles à une simple technique permettant de normaliser les comportements ou de rendre compte d'une norme par la loi. Le droit a une signification ou une capacité à la signification, à donner sens à la vie en société démocratique. Le sujet de droit en est le relais, et le juge le principal gardien. Le Droit soumis à la raison humaine ne se résume pas à ce que la surveillance diffuse est en train d'élaborer: la réduction de toutes règles de vie à un calcul d'utilité, une raison humaine remplacée par la vertu des algorithmes.

B. ... Aux corps statistique: la réduction du sujet de Droit à un objet

646. Ainsi qu'Hannah Arendt le décrivait à propos des origines du totalitarisme, « *le premier pas essentiel sur la route qui mène à la domination totale consiste à tuer en l'homme la personnalité juridique*¹⁴¹⁵ ». En ce que la surveillance diffuse réduit l'individu à des profils de plus en plus individualisés, les mots de Arendt s'imposent à l'esprit. L'étude de cette notion de profil individualisé démontre en effet que l'individu est principalement réduit à une statistique, à un corps statistique. On constate en réalité que sous couvert des concepts de profils, de statistiques, de corps statistiques, se cachent un in-sujet, et la réduction de l'individu à un objet.

647. Alors qu'il se pose la question de savoir à quoi sert le Droit, François Ost opère un détour anthropologique afin de comprendre à quel homme s'adresse le Droit aujourd'hui¹⁴¹⁶. En prenant appui sur les remarques de Antoinette Rouvroy et Thomas Berns¹⁴¹⁷ concernant l'élaboration d'un nouveau pouvoir statistique et la production de corps statistiques¹⁴¹⁸, François Ost écrit que « *à chacun de ces trois stades du datamining est évacuée la prise en compte du sujet envisagé tant dans son individualité (il est décomposé en séquences comportementales), que dans son intentionnalité signifiante (les « profils » résultent de simples corrélations algorithmiques), ou encore dans sa*

¹⁴¹⁴ SUPIOT Alain, *Homo juridicus Op. Cit.*, p. 26.

¹⁴¹⁵ ARENDT Hannah, *Les origines du totalitarisme (Op. Cit.)*, p. 185

¹⁴¹⁶ OST François, *A quoi sert le Droit ? - Usages, Fonctions, Finalités*, Editions Bruylant, Collection Penser le Droit, 2016, voir spécialement son interlude: « *quel homme pour quel droit ?* », p. 248 -326

¹⁴¹⁷ ROUVROY Antoinette, Berns Thomas, *Le nouveau pouvoir statistique (Op. Cit.)*.

¹⁴¹⁸ Ibid. p. 98 - 99.

*capacité d'action délibérée (on le traite à l'aide de stimuli/réponses réflexes)*¹⁴¹⁹ ». La surveillance diffuse désinstitue le sujet de droit aussi bien dans sa faculté d'autonomie et de délibération, d'individualité, que dans son intentionnalité, c'est-à-dire dans sa capacité à se subjectiver et à se percevoir. L'ensemble de ces références font écho au concept de vie privée précédemment développé. La capacité d'être laissé seul, de penser et de s'exprimer librement, la possibilité pour l'individu de construire son raisonnement librement, et de prendre des décisions au vu de ces raisonnements. Le concept de corps statistiques doit être entendu comme produisant une objectivation de l'individu. Antoinette Rouvroy et Thomas Berns analysent ce concept comme la suite logique de la « *dividualisation des sujets*¹⁴²⁰ ».

648. Cette objectivation touche aussi bien son corps physique, que sa capacité à penser. La vision de l'individu passe alors progressivement à l'être libre, doué de raison, d'entendement et de volonté à une chose docile. Antoinette Rouvroy et Thomas Berns complètent ces éléments en écrivant que « *la gouvernementalité algorithmique ne fonctionnerait plus tant à la domestication, à la disciplinarisation des corps, à leur assujettissement à la norme et à la subjectivation par la norme, qui la domestication de la norme par le corps (statistique) et donc à même les corps, à la faveur d'une confiscation ou d'une absorption par la technologie du processus d'élaboration des normes*¹⁴²¹ ». Si la production d'une nouvelle normalisation est intéressante¹⁴²², il semble bien qu'il faille comprendre ce phénomène comme dépendant de l'objectivation du corps, l'objectivation de soi¹⁴²³, et plus loin des individus. L'analyse d'Antoinette Rouvroy du sujet de droit transformé par

¹⁴¹⁹ OST François, *Op.Cit.*, p. 308. Pour Ost, il faut entendre par datamining un ensemble de dispositifs dont le fonctionnement se décompose en trois étapes: « *la récolte de quantités massives de données* », « *la phase de traitement de ces données* », « *l'usage managérial de ces profilages en vie d'obtenir la réaction souhaitée ou d'éviter les comportements à risque* » (p. 307-308)

¹⁴²⁰ ROUVROY et BERNNS, *Op. Cit.*, p. 94. Les auteurs écrivent que: « *la mesure de toute chose est « dividuelle », à la fois infra- et supra-personnelle, rhizomatique, constituée d'une multitude de représentations numérisées, potentiellement contradictoires entre elles et en tout cas hétérogènes les unes aux autres. C'est cet « être » numérique constamment décomposé, recomposé, composite, qui intéresse à présent directement le pouvoir: l'instabilité du « dividu », cette unité dépourvue de for intérieur, correspond à l'absence de projet et d'hypothèse du gouvernement. Dans un régime de gouvernementalité algorithmique, il n'est plus attendu du sujet qu'il soit d'un seul bloc, ni qu'il fasse preuve de l'intériorisation des normes en s'identifiant et en rendant compte de soi auprès d'un pouvoir identifiable; le « pouvoir » - ou ce qu'il en reste - tolère d'autant mieux les irrégularités, les contradictions, les incohérences des individus, qu'il produit leurs corps statistiques non plus en fonction de a manière dont les individus se perçoivent, s'assujettissent ou se subjectivent, mais en fonction de ce que ces corps pourraient faire, en fonction des virtualités dont ils sont porteurs ».*

¹⁴²¹ Ibid. p. 98

¹⁴²² Nous évoquerons ce point par la suite de notre analyse

¹⁴²³ Par la quantification par exemple. Objectivation de soi mais également de soi par rapport aux autres. En ce sens, voir: PHARABOD Anne-Sylvie, NIKOLSKI Véra, GRANJON Fabien, « *La mise en chiffres de soi. Une approche compréhensive des mesures personnelles* », *Réseaux*, 2013/1 (n° 177), p. 97-129, En ligne: <https://www.cairn.info/revue-reseaux-2013-1-page-97.htm> (dernière consultation: 5 mars 2018)

la dividualisation technologique en corps statistique peut également s'assimiler à ce que Arendt analysait sous les régimes totalitaires comme la « *préparation de cadavres vivants qu'est le meurtre en l'homme de la personne morale*¹⁴²⁴ », c'est à dire de sa capacité d'interaction avec autrui. Car en effet, toute interaction humaine est aujourd'hui (en)cadrer par les technologies, et pas la surveillance diffuse.

649. Et puisque aujourd'hui l'objectivation du sujet de Droit se produit dans un Etat de Droit libéral, il faut rejoindre ici l'analyse d'André Tosel lorsqu'il évoque l'in-sujet comme nouveau sujet juridique¹⁴²⁵. L'auteur repère également une mutation du sujet juridique. Il écrit ainsi que « *l'individu humain n'est même plus considéré comme citoyen, titulaire d'une égale liberté qu'il partage avec les autres et qui lui permet de prendre part avec ses concitoyens au pouvoir commun de délibérer et de décider des affaires communes. La nouvelle forme sujet ne s'identifie plus au droit républicain d'avoir des droits de cité, mais au droit d'avoir le droit de consommer. Les sujets sont en relation qualitative de coexistence concurrentielle où ils se distinguent les uns des autres par le pouvoir quantitatif de consommer, selon leur inégale solvabilité. L'inégalité réelle des sujets est structurale dans la mesure où les sujets sont unifiés par la même possession de la même forme qui se déploie quantitativement*¹⁴²⁶ ». Et d'ajouter que : « *la force de ce droit subjectif réside dans son lien immédiat au désir et à sa capacité d'écraser ce désir sur lui-même: le sujet est désir individuel de droit privé solvable. Ce sujet a perdu toute identité parce qu'il est une partie qualitativement homogène d'une masse humaine qui désire la quantité indéfinie des biens et services consommables. Les sujets ne se distinguent que par leur solvabilité*¹⁴²⁷ ». On retrouve ici l'état de désir décrit précédemment quant à l'analyse du mythe de Narcisse. L'individu contemporain en quête d'attention est objectivé par la rhétorique de l'utilitarisme. Réduit lui aussi à un calcul d'utilité, soumis à un contrôle social attentionnel, et à la promotion du bien-être et de la sécurité, l'objet individu n'a d'autre choix que celui de la consommation technologique, et de laisser toujours plus d'informations le concernant dans les mains des entreprises et des Etats.

650. Que l'on y voit la production d'un corps statistique, ou dans sa version plus aboutie, la production d'un in-sujet, le libéralisme par le contrôle social attentionnel qu'il porte en son sein a

¹⁴²⁴ ARENDT, Op. Cit, p. 190.

¹⁴²⁵ TOSEL André, Op. Cit., spécialement p. 91 et suivants

¹⁴²⁶ Ibid. P. 87

¹⁴²⁷ Ibid.

permis l'objectivation de l'individu. Cet homme objet, réduit à une utilité, est privé de sa capacité de penser. Ainsi que le note André Tosel, « *il est mis dans l'impossibilité de réfléchir sur les finalités de l'agir humain dans le contexte de l'Etat hyperlibéral. C'est l'homme en sa conscience immédiate qui s'interdit la réflexion sur les fins et qui ne pense qu'aux moyens de satisfaire son droit de consommer le droit de consommation*¹⁴²⁸ ». Cette assertion explique pour partie le mythe de nos sociétés du « rien à cacher, rien à se reprocher ». Elle est également parfaitement représentée dans les mots de Snowden « *prétendre que votre droit à une sphère privée n'est pas important parce que vous n'avez rien à cacher n'est rien d'autre que de dire que la liberté d'expression n'est pas essentielle, car vous n'avez rien à dire*¹⁴²⁹ ». Partageons ici une des conclusions d'Antoinette Rouvroy concernant l'individu et la nécessité de sa subjectivation: « *Cette conception d'un sujet processus plutôt que phénomène nous place dans la perspective antihumaniste déjà bien balisée par Althusser (les sujets sont constitués à travers et par l'interprétation idéologique qui leur est adressée, et ne préexistent pas à cette interpellation), Butler (les sujets se constituent en rendant compte d'eux-mêmes, et ne préexistent pas à ce geste de « rendre compte »), Foucault (les sujets ne préexistent pas à leur co-construction à travers les discours de vérité construits à leur endroit et les rapports de pouvoir dans lesquels ils sont pris) ou Derrida (selon qui le Droit présume et construit le sujet de droit. On se présente devant la loi avec nos volontés et imaginations, mais sans le droit nous ne serions pas des sujets.)*¹⁴³⁰ ».

Paragraphe 2: L'apparition d'une nouvelle forme de régulation par la surveillance diffuse: la technique des nudges comme symptôme de la perte de symbolicité du Droit et de sa désinstitution progressive

651. La surveillance diffuse et le contrôle social attentionnel privent l'individu de sa capacité de penser, d'entendement, de volonté. Ils réduisent sa possibilité d'agir ou de ne pas agir, d'obéir ou de ne pas obéir. Dans ce système d'objectivation des corps, le droit et la loi n'ont que peu de prises. Ainsi que le notait, Foucault « *alors que les systèmes juridiques qualifient les sujets de droit, selon des normes universelles, les disciplines caractérisent, classifient, spécialisent ; elles distribuent le*

¹⁴²⁸ Ibid. p. 88

¹⁴²⁹ in. MEILLASSOUX Marc, Nothing to Hide, Film Documentaire, 2017, Disponible en ligne à l'adresse suivante https://www.youtube.com/watch?time_continue=385&v=djwzEIV7gE (dernière consultation: 5 mars 2018)

¹⁴³⁰ ROUVROY Antoinette, « Pour une défense de l'éprouvante inopérationnalité du droit face à l'opérationnalité sans épreuve du comportementalisme numérique », *Dissensus*, Avril 2011, n° 4, pp. 127 - 149, p. 144 - 145, En ligne: <https://popups.uliege.be/2031-4981/index.php?id=1269&file=1&pid=963> (dernière consultation: 5 mars 2018)

long d'une échelle, répartissent autour d'une norme, hiérarchisent les individus les uns par rapport aux autres, et à la limite disqualifient et invalident¹⁴³¹ ».

652. Dans sa double volonté de réduction de toutes choses à un calcul d'utilité, et de réduction de l'individu à un in-sujet, la surveillance diffuse engendre une perte de symbolique du Droit, et même, plus loin une véritable désinstitution (B) et la loi par la production d'une nouvelle régulation normative (A).

A. La production par la surveillance diffuse et le contrôle social attentionnel d'une nouvelle forme de normalisation: les nudges

653. La réduction des sujets de Droit à des in-sujets, des corps statistiques permet au contrôle social attentionnel et à la surveillance diffuse d'introduire une nouvelle forme de normalisation. Principalement aidée par la mise en données du monde et le traitement de toutes informations sur les individus, la surveillance diffuse élabore un savoir sur les individus. Assimilée à un « *comportementalisme numérique¹⁴³²* » par Antoinette Rouvroy et Thomas Berns, cette régulation nouvelle permet un « *management des risques et des opportunités (et) vise à orienter l'action des individus, sans exercer de contrainte directe et explicite, et en faisant l'économie d'une étude de leurs motivations et de leurs intentions. l'action s'exerce plutôt sur leur environnement, qui s'adapte en temps réel, et obtient la réaction souhaitée du sujet, par voie de stimuli et de signaux d'alarme suscitant des réactions réflexes, plutôt que par la voie d'injonctions appelant une action réfléchie¹⁴³³* ».

654. La technique des nudges s'inscrit dans cette nouvelle forme de régulation douce, sans contrainte. Elle en représente même l'aboutissement dans nos sociétés se situant entre la normalisation par responsabilisation, par incitation, par persuasion douce, et manipulation (1). Deux exemples pratiques contemporains permettront de mettre en lumière ce propos. Les péages inversés et les compteurs Linky représentent deux exemples qui, par leur possibilité de rétroaction,

¹⁴³¹ FOUCAULT Michel, *Surveiller et Punir, Op.Cit.*, p. 435

¹⁴³² Les auteurs définissent ce concept comme suit: « *rationalité (a) normative ou (a)politique reposant sur la récolte, l'agrégation et l'analyse automatisée de données en quantité massive de manière à modéliser, anticiper et affecter par avance les comportements possibles* » in. ROUVROY Antoinette, BERNIS Thomas, « Gouvernamentalité algorithmique et perspectives d'émancipation », *Réseaux*, 2013/1, n° 177, pp. 163 - 196, p. 173, En ligne: <https://www.cairn.info/revue-reseaux-2013-1-page-163.htm>

¹⁴³³ OST François, *A quoi sert le Droit?, Op. Cit.*, p. 308

influencent, responsabilisent par la vertu et non par la raison, les individus (2).

1. Le nudge comme technique de normalisation manipulatrice des in-sujets

655. Le nudge, encore appelé par ses partisans¹⁴³⁴ le paternalisme libertarien, devrait être analysé comme une méthode douce permettant d'inspirer aux individus la bonne décision. Le comportement individuel s'altère quelque peu, dans un sens prévisible, du fait d'une incitation douce mise en place par des acteurs publics ou privés. On oriente alors l'individu vers des choix, des actions d'intérêt individuel ou collectif. Les nudges ont été théorisés comme une réponse au manque de rationalité des individus, et s'inscrivent dans le cadre plus global des théories de l'économie comportementale. Aidé par les technologies numériques les nudges participent de ce que Rouvroy et Berns envisagent sous couvert du recours au concept de comportementalisme numérique.

656. La technique de normalisation par les nudges doit être analysée avec objectivité. Des auteurs tels que François Ost et Philippe Vion-Dury rappellent d'ailleurs que ces techniques doivent plutôt être perçues comme opérant une « *guidance inconsciente grâce à des procédures par défaut (tablant sur le fait que, le plus souvent, le sujet ne choisit pas), ainsi que des dispositifs topographiques induisant, comme pour des cobayes dans un labyrinthe, le parcours souhaité, ou encore diverses stratégies visuelles stimulant ou dissuadant les conduites*¹⁴³⁵ », mais également comme créant un « *écosystème de manipulation*¹⁴³⁶ ». L'individu est, en effet, dans ce système de moralisation, soumis à une analyse constante afin de produire un comportement attendu dans telle ou telle situation. Pour François Ost, il est alors sommé d'agir selon une « *moralité collective*¹⁴³⁷ », « *la raison et la moralité algorithmique apparaissent comme des forces extraordinairement conservatrices, vouées à l'exécution mécanique de leur programme, dans le déni et la peur de la créativité qui est le propre de l'homme, et aussi des sociétés qui sont le produit de leur créativité*

¹⁴³⁴ Voir: THALER Richard, SUNSTEIN Cass, *Nudge - Improving Decisions about Health, Wealth and Happiness*, Penguin Books, 2012. On précisera que ces auteurs sont tous deux des universitaires américains: le premier est économiste à la Chicago University, le second est professeur de droit à Harvard.

¹⁴³⁵ OST François, *A quoi sert le Droit? (Op. Cit)*, p. 308

¹⁴³⁶ VION-DURY Philippe, *La nouvelle servitude volontaire Op. Cit.*, pp. 124 - 136

¹⁴³⁷ OST François, *Op. Cit.* p. 310. L'auteur écrit: « *de tels programmes d'analyse et d'action (telles les machines à traduire, les automates joueurs d'échecs, ou les drones policiers) sont nécessairement basés sur la reproduction des comportements les plus fréquents, or, et voilà l'objection, on sait bien que l'innovation scientifique autant que le progrès moral ne se fraient un chemin que par les marges, en opposition au quod plerumque fit. « Toute science commence par un refus », a-t-on dit (refus du témoignage des sens, refus de l'argument d'autorité...); il en va de même de la moralité collective dont l'histoire est celle d'un lent arrachement aux conventions traditionnelles - quoi, par exemple, de moins naturel que l'exigence d'égalité sous-jacente aux droits de l'homme ?* ».

*institutionnelle*¹⁴³⁸ ». Le nudge s'inscrit pleinement dans le contrôle social attentionnel que cherche à obtenir la surveillance diffuse. Cette technique s'inscrit également dans la définition que David Lyon proposait en 2015 quant à la notion de surveillance. L'intention pratique de cette dernière « *peut aller de la protection, à la compréhension, en passant par le fait de prendre soin, d'assurer le droit, de contrôler, de gérer ou d'influencer des individus ou des groupes*¹⁴³⁹ ».

657. Aidée par les algorithmes et par une connectivité constante des individus, cette technique vise à produire le comportement responsable et vertueux par l'influence, la gestion, la direction, la protection, des individus et des groupes. Elle analyse leur environnement et y applique une règle de comportement visant à éluder toute créativité de l'individu, et tout comportement à risque. « *Le pas suivant de cette logique machinique, dans la ligne directe de cette évacuation de l'humain, est la mise au point de « machines morales » (...) auxquelles les décideurs envisagent de confier demain diverses conduites à risque*¹⁴⁴⁰ », écrit François Ost. Par l'évacuation de la pensée de l'homme en tant qu'être libre, doué de raison, la surveillance diffuse, par la technique des nudges, réduit toute règle et tout comportement à ce calcul d'utilité propre au libéralisme économique. Cette logique normative vise à la production d'un savoir instantané sur le réel d'une société, « *comme si l'intelligibilité du monde surgissait des faits eux-mêmes*¹⁴⁴¹ ». Ces techniques sont également à rapprocher des intentionnalités technophobiques précédemment dégagées. En ce qu'ils permettent un conditionnement de l'individu, plutôt que son émancipation, en ce qu'elles influencent, incitent persuadent et manipulent l'environnement de l'individu, et l'individu, les nudges algorithmiques et le comportementalisme numérique s'inscrivent dans ce que Heidegger évoquait sous l'expression de l'arrondissement de l'homme par la technique.

658. Ainsi que Philippe Vion-Dury le note, la normalisation par les nudges ambitionne un « *conditionnement opérant*¹⁴⁴² » de l'individu et de son environnement. Selon l'auteur, ce conditionnement se fonde sur deux éléments: « *le renforcement (l'encouragement) et la punition. Chacun des deux peut prendre une charge positive (ajout) ou négative (retrait), leur combinaison produisant quatre moyens de dressage. Le renforcement positif tend à faire en sorte que le*

¹⁴³⁸ Ibid. p. 310 - 311.

¹⁴³⁹ LYON David, Op. Cit, 2015

¹⁴⁴⁰ Op. Cit. p. 310

¹⁴⁴¹ Ibid. p. 309.

¹⁴⁴² VION-DURY Philippe, Op. Cit., p. 125

comportement souhaité se produise, en se servant d'un stimulus appétitif (d'une incitation), comme des félicitations ou une récompense. (...). Le renforcement - l'encouragement de certains comportements par le retrait d'un privilège, d'un plaisir, d'un droit (...) émerge mécaniquement (...) dans un monde où la connexion et la société numérique sont devenues aussi prégnantes¹⁴⁴³ ». Créant, selon l'auteur, un « *nouveau monopole radical¹⁴⁴⁴* », le renforcement négatif exclut et marginalise l'individu qui ne se soumet pas à la règle de comportement. Le refus d'avoir un téléphone portable, ou encore le refus de partager la logique d'exhibition que prône les réseaux sociaux, conduit comme nous l'avons démontré à une forme d'exclusion et de marginalisation des individus. Enfin, les nudges portent en eux une logique de quantification de soi dans un rapport performatif aux autres. Vion-Dury écrit à ce propos que ces « *systèmes d'évaluation des individus¹⁴⁴⁵* » sont issus d'un entremêlement des renforcements positifs et négatifs et font émerger des systèmes de notation des individus, d'un service. Pour l'auteur, « *on obtient alors ce mélange étrange de la quête de félicitation exprimée par un cinq étoiles et de la peur d'être mal noté, voire de ne plus utiliser ce service¹⁴⁴⁶* ».

659. Cette technique de normalisation réduit l'existence de l'individu à une influence constante, douce et bienveillante. Elle remplace la raison de l'individu, et du Droit par la vertu, le bien-être, la sécurité, la protection et la liberté de consommation technologique. Or, quand la vertu fait place à l'efficacité, c'est en réalité toute la société qui est sommée de se placer dans une logique performative et conservatrice, excluant de fait toute liberté de créativité.

2. De deux exemples pratiques de mise en place du nudge: les compteurs Linky et les péages inversés

660. La surveillance diffuse basée sur des technologies algorithmique produit à la fois une norme de comportement (influence, gestion, direction, protection des individus), mais également une normalisation de l'environnement de l'individu. Deux exemples pratiques permettent de mettre en lumière ce propos de la double normalisation: les compteurs Linky et les péages inversés. Ces deux exemples permettront également de mettre en exergue la dimension manipulatrice et influente des

¹⁴⁴³ Ibid. p. 126 - 127

¹⁴⁴⁴ Ibid. p. 127

¹⁴⁴⁵ Ibid. p. 128

¹⁴⁴⁶ Ibid.

nudges.

661. Le compteur Linky est une technologie communicante visant à analyser et suivre en temps réel des consommations électriques des clients d'Enedis¹⁴⁴⁷. La solution proposée par ce fournisseur, « e-equilibre¹⁴⁴⁸ », est quant à elle un outil de supervision et de gestion en temps réel des données de consommations électriques des individus. S'inscrivant dans une politique générale de modernisation des compteurs électriques, mais également de développement durable, ces compteurs communicants visent, pour les gestionnaires du réseau électrique, à « *réduire les pertes non techniques, constituées en particulier de l'électricité consommée après le départ de l'occupant d'un logement et avant l'arrivée de l'occupant suivant et de maîtriser les coûts notamment par l'automatisation de certaines fonctions (relève des index, modification de la puissance souscrite, opérations suite aux changements d'occupant, etc.)*¹⁴⁴⁹ ». Pour les individus, la modernisation des dispositifs permettrait de « *réduire le nombre d'erreurs de facturation et de bénéficier d'un meilleur service, sans nécessité d'être présent notamment pour les opérations de relevé de consommation, et d'accéder à des données de consommation plus détaillées et plus fréquentes, leur connaissance constituant en règle générale un prérequis pour toute action de maîtrise de la demande d'énergie (MDE). Il s'agit aussi de bénéficier des offres adaptées à leur situation personnelle, telles celles étendant à d'autres plages horaires l'actuel système d'heures pleines/heures creuses adapté aux chauffe-eau électriques*¹⁴⁵⁰ ». A la lecture de ces mots, on voit bien que les compteurs communicants s'inscrivent pleinement dans la rhétorique de l'utilitarisme et du calcul d'utilité, de performance et de rentabilisation.

662. La solution e-equilibre d'Enedis et les compteurs communicants visent à mettre le consommateur au centre du dispositif de modernisation de la gestion des consommations

¹⁴⁴⁷ La Cour des comptes vient définir le système Linky comme suit: « *Le système de compteurs communicants Linky est constitué des compteurs électriques eux-mêmes, des concentrateurs, situés au niveau de chaque transformateur haute tension / basse tension (230 ou 380 V), et du système d'information central. Les concentrateurs communiquent en aval avec les compteurs reliés au transformateur par les câbles électriques en utilisant la technologie du « courant porteur en ligne » (CPL) et en amont avec le système central par les réseaux de téléphonie mobile* ».in. Cour des Comptes, *Le rapport public annuel 2018 - Tome 1: Les observations*, p. 249, En ligne: https://www.ccomptes.fr/sites/default/files/2018-02/RPA2018-Tome-1-integral_0.pdf (dernière consultation: 5 mars 2018)

¹⁴⁴⁸ Voir le site dédié à la solution EDF: https://particulier.edf.fr/fr/accueil/autres-pages/Connexion-equilibre.html?ns_mchannel=sea&ns_source=adwords&ns_campaign=frp_mobilite_part&edf_support=marque&edf_strat=Perf&edf_s_eac=SUIVI_CONSO_MARQUE&edf_seaga=Equilibre_Exact&edf_seakw=%5Be%20equilibre%5D&gclid=EA1aIQobChMIjvmD64eS2gIVTLftCh1sRw7bEAAYASAAEgltzfD_BwE (dernière consultation: 5 mars 2018)

¹⁴⁴⁹ Ibid. p. 245.

¹⁴⁵⁰ Ibid.

électriques. Promouvant la mise en place par les individus d'éco-gestes et d'attitudes responsables au regard du développement durable, la solution e-équilibre permet à l'individu d'effectuer une synthèse en temps réel de ces consommations au jour le jour. Le fil d'actualité de cette solution propose de récompenser les comportements vertueux des consommateurs pour les jours où leur consommation électrique est jugée comme s'inscrivant dans une moyenne basse par rapport à d'autres consommateurs de même types (taille de la maison, nature des équipements). Cette récompense se traduit pas des pastilles de couleurs vertes, bleues et rouges permettant clairement de comprendre si l'individu s'est comporté en bon ou en mauvais consommateur, en homme responsable ou irresponsable. Cette mise en chiffre de la consommation électrique des individus en temps réel s'inscrit dans ce que Rouvroy et Berns évoquaient sous l'expression de comportementalisme numérique. Bien que le rapport public de la Cour des Comptes de 2018 dénonce à la fois le coût pour les consommateurs, la complexité pour la maîtrise réelle de demande d'énergie et le peu d'utilité de ces compteurs¹⁴⁵¹, ces compteurs communicants restent la seule réponse proposée par les distributeurs et la puissance publique dans la gestion et la maîtrise de la consommation électrique. On retrouve ici l'argument de la surveillance diffuse, précédemment développé, selon lequel son défaut d'efficacité tend à justifier son recours.

663. Les péages urbains inversés s'inscrivent, quant à eux, dans une logique de renforcement positif prôné par la technique de normalisation des nudges. Plusieurs pays européens ont envisagé le péage urbain afin de décongestionner la circulation automobiles, spécialement en centre ville. On pense notamment à Londres, Milan, Rotterdam et Stockholm. Le gouvernement français souhaite faciliter leur mise en place, et la métropole de Lille se lance depuis juin 2017 dans une expérimentation visant à l'élaboration du projet ecobonus¹⁴⁵². S'inscrivant dans la poursuite des pistes dégagées par le Grenelle de l'environnement afin de promouvoir le développement durable en incitant à l'utilisation de modes de transports plus doux, les péages urbains inversés consistent à rémunérer (2 euros dans la limite de 80 euros par mois) les automobilistes qui adopteraient un comportement vertueux. Par exemple, les automobilistes sont conviés à opter pour le télétravail, les horaires décalés, les transport en communs. La récompense de deux euros s'inscrit bien dans « le stimuli appétitif » décrit par Philippe Vion-Dury.

¹⁴⁵¹ Rapport précité

¹⁴⁵² Ministère de la Transition écologique et solidaire - Ministère de l'intérieur, Rapport CGEDD n°011008-01 - IGA n° 17018 - R établi par Dominique Hucher, Jean François Landel et Maxime Tandonnet, *Conditions de faisabilité du projet Ecobonus de la Métropole européenne de Lille - un « péage positif » innovant à consolider*, Juin 2017, En ligne: http://cgedd.documentation.developpement-durable.gouv.fr/documents/cgedd/011008-01_rapport.pdf (dernière consultation: 5 mars 2018)

664. Au delà de leur caractère proprement technique et de leur lien avec l'incitation et la gestion du comportement des individus, il faut ici conclure le propos par un retour au Droit, et spécialement au droit à la vie privée et à la protection des données à caractère personnel. Qu'il s'agisse des compteurs communicants ou du péage urbain inversé, ces éléments se fondent sur des informations techniques, souvent interconnectées à des informations personnelles. La courbe de charge¹⁴⁵³ comme la plaque d'immatriculation d'une voiture sont analysées par la CNIL comme des données personnelles. Le rapport de la Cour des Comptes de 2018 relève à juste titre un « *déficit de communication, s'agissant des questions de protection des données, (qui) font que les (...) dispositions prises par la CNIL n'ont pas été suffisamment entendues par les public*¹⁴⁵⁴ ». Si le rapport conclut ce propos vis-à-vis de l'impact de ce déficit sur le déploiement de Linky, il semble utile d'opter pour une autre conclusion. Le manque de communication à ce sujet sert les objectifs de ces instruments communicants. La vie privée et la protection des données personnelles sont perçues comme un frein au progrès technologique. Ce « déficit d'image de marque », de symbolicité de ces deux droits est clairement entretenu par le développement technologique. A travers ces deux exemples pratiques, on voit bien que l'idéologie dominante est le bien-être, la protection, le développement durable, la vertu produite par ces technologies sur l'environnement de l'individu, qui permet, à son tour, de produire un comportement lui-même vertueux et responsable. De fait, par cette logique de comportements vertueux et en maintenant l'individu dans une absence d'information claire au sujet de certains déploiements technologiques, on somme l'individu de passer de la raison juridique à la vertu normative. En cela, cette nouvelle régulation par la normalisation est manipulatrice, et dangereuse en termes de libertés et protection des droits fondamentaux. La vie privée et la protection des données personnelles font place à la transparence, l'incitation, l'influence, la gestion, la direction, la protection et la rentabilisation.

¹⁴⁵³ Selon la CNIL, « la courbe de charge est une nouvelle fonctionnalité offerte par les compteurs communicants qui permet d'avoir une connaissance plus précise de la consommation des ménages afin de leur fournir de nouveaux services (bilan énergétique, par exemple). Cette courbe de charge est constituée d'un relevé, à intervalles réguliers (le pas de mesure), de la consommation électrique de l'abonné », En ce sens: CNIL, *Les compteurs communicants Linky: la position de la CNIL sur le stockage local de la courbe de charge*, 30 novembre 2015, En ligne: <https://www.cnil.fr/fr/compteurs-communicants-linky-la-position-de-la-cnil-sur-le-stockage-local-de-la-courbe-de-charge-0> (dernière consultation: 5 mars 2018), Voir également: CNIL, Délibération N°2012-404 du 15 novembre 2012 portant recommandation relative aux traitements des données de consommation détaillées collectées par les compteurs communicants, En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000026958542&fastReqId=287627783&fastPos=1> (dernière consultation: 5 mars 2018)

¹⁴⁵⁴ Cour des Comptes, *Rapport public 2018 Op. Cit.*, p. 263

B. De la perte de symbolicit  du Droit   sa d sinstitution progressive

665. Ainsi que le r sume Christian Laval, « *on voit par l  le lien  troit entre surveillance, transparence, identification, s curit . Agir en libert , c'est agir en s curit . Nous ne sommes en s curit  que si nous pensons que les autres sont limit s dans leur capacit  de nuisance par la crainte des punitions et donc par la probabilit  de payer cher les d lits et les crimes. On agit d'autant plus librement que l'on sait que les gens potentiellement dangereux sont sous surveillance et sous contr le. Plus on veut  tre libre, plus on veut  tre en s curit , plus on doit  tre surveill , plus on doit demander de la surveillance et du contr le. Il est donc vain de chercher dans le panoptique l'image anticip e de la seule soci t  totalitaire, il n'est que l'un des aspects, mais non des moindres, de la soci t  de march . Il est vrai que les lib raux, loin de la froide lucidit  de Bentham, n'aiment pas s'en vanter¹⁴⁵⁵ ».*

666. Dans une volont  d'actualisation de ces propos et au vu des d veloppements qui pr c dent, il faudrait ajouter que dans sa dimension de normalisation de l'environnement physique des individus et du comportement des individus, la surveillance diffuse juge aujourd'hui l'ensemble de la population comme potentiellement dangereuse. En fonction d'objectifs pr d termin s et des int r ts fluctuants de la Nation (de la s curit    la libert  de consommation des technologies, en passant par le d veloppement durable), la surveillance diffuse et le contr le social attentionnel neutralisent toute capacit  de nuisance individuelle par la production d'un conformisme social et environnemental. Homog n sation des lieux de vie, des espaces publics et priv s, des comportements individuels, gestion des masses sont autant d'effets produits par la normalisation et le contr le social attentionnel. Loin de produire un individu  mancip , libre et autonome, ces techniques subvertissent le Droit, et sp cialement les droits de l'Homme et du citoyen. En perte de symbolicit  face   la volont  d'un libre march  technologique et rentable, le Droit est m me d sinstitu  dans certains cas au profit de la norme. Le nudge s duit, en effet, de plus en plus la Commission europ enne dans les domaines de la consommation et de la sant . Une unit  de prospective et d'analyse comportementale a  t  fond e par la Commission europ enne en vue de « *soutenir l' laboration des politiques de l'Union Europ enne en identifiant les  l ments comportementaux dans ces derni res et en proposant des leviers comportementaux pour accro tre*

¹⁴⁵⁵ LAVAL Christian, Surveiller et pr venir La nouvelle soci t  panoptique », Op. Cit. p. 59 - 60

*leur efficacité*¹⁴⁵⁶ ».

667. Alors que le Droit impose une raison juridique fondée sur le schéma du permis et de l'interdit et/ou de l'obligatoire et de l'interdit, mais également sur la pensée d'un homme libre, autonome et doué de raison, la surveillance et le contrôle social attentionnel imposent quant à eux une logique de comportement responsable fondée sur un schéma « *du tolérable et de l'intolérable*¹⁴⁵⁷ » (éco-conduite, éco-gestes). Ce passage de la loi et du Droit à la normalisation ne doit pas être analysé comme un renforcement du Droit. Ce dernier est, selon Mazabraud réduit à une place « *d'opérateur de l'intelligibilité économique*¹⁴⁵⁸ », « *le droit lui-même n'est considéré que comme un opérateur économique*¹⁴⁵⁹ ». Cette responsabilisation des individus par leurs comportements n'est pas à confondre avec le droit de la responsabilité. Bien au contraire, elle est une force douce faisant passer les règles de droit en arrière plan et les remplacent par la promotion des actions vertueuses. Elles rationalisent les dispositifs de responsabilisation, et incitent la population à la responsabilisation générale et à la vertu. Ainsi que le note Yannick Rumpala, « *pris sous un angle pragmatique, l'objectif de prise en compte anticipée des conséquences pose la question des leviers à utiliser pour que les activités plus ou moins courantes puissent s'organiser sur des bases de prévoyance et de prudence. (...). Tel qu'elle est le plus souvent reprise, une telle aspiration incite en effet à attacher une forme de conscience à chaque entreprise humaine. Elle tend ainsi à induire un mouvement d'élargissement des responsabilités. Et même de « permanentisation » de celles-ci, dans le sens où les raisonnements qui sous-tendent ce mouvement entraînent presque la production de responsabilités permanentes. L'obligation de responsabilité qui se dégage fonctionne comme une forme de rappel de l'attention à prêter aux conséquences de chaque activité. Le message prescriptif véhiculé sous-entend que chaque acteur doit accepter de se remettre en cause et, au besoin, de s'adapter*¹⁴⁶⁰ ».

668. Cette « permanentisation » se produit à plusieurs échelles: dans la vie quotidienne comme

¹⁴⁵⁶ Voir: <https://ec.europa.eu/jrc/en/research/crosscutting-activities/behavioural-insights> (dernière consultation: 5 mars 2018)

¹⁴⁵⁷ En ce sens: MAZABRAUD Bertrand, *Foucault, le droit et les dispositifs*, Op. Cit., p. 172

¹⁴⁵⁸ Ibid. p. 168

¹⁴⁵⁹ Ibid. p. 184

¹⁴⁶⁰ RUMPALA Yannick, « Gouverner en pensant systématiquement aux conséquences ? Les implications institutionnelles de l'objectif de « développement durable » », *VertigO - la revue électronique en sciences de l'environnement*, Volume 10, numéro 1, avril 2010, En ligne: <http://journals.openedition.org/vertigo/9468#toc> (dernière consultation: 5 mars 2018)

on a pu le démontrer au travers des nudges, mais également dans le temps. Les débats publics liés particulièrement à l'environnement et au développement durable sont touchés par la pensée du « droit » des générations futures¹⁴⁶¹. Si le propos peut séduire par son ambition à rompre avec la vision individualiste de l'être humain, encore faut-il ainsi que le rappelle Mireille Delmas-Marty « concilier des intérêts parfois antagonistes, distinguer les droits des générations présentes de la forme unilatérale des « devoirs » envers les générations futures » fondée sur le passage d'une « action en réparation à l'action en préservation¹⁴⁶² ». Véritable institutionnalisation d'un devoir de précaution et de solidarité, l'expression d'un droit des générations futures témoigne de l'ambition du Droit à être lui aussi envahi par l'anticipation et la précaution¹⁴⁶³.

669. Aussi, et par anticipation de la pensée des générations futures, peut-être serait-il utile de comprendre la situation de l'Homme aujourd'hui, et ce que signifie « l'agir humain¹⁴⁶⁴ ». Plus qu'une responsabilisation permanente dénoncée par Yannick Rumpala, on assiste aujourd'hui à la consécration du conformisme social que la surveillance diffuse et le contrôle social attentionnel ont engendré. Ainsi que François Ost le rappelle, « ici, le projet libéral d'estompement du politique au profit des bienfaits d'une « main invisible » atteint des sommets, de sorte que Thomas Berns peut bien parler de « gouverner sans gouverner, ou de « gouverner à partir du réel ». Comme si les choses, non content de « parler d'elles-mêmes » (au plan de la connaissance), « commandaient d'elles-mêmes ». Le « répondant » d'une telle politique (ou plutôt la « cible », car précisément on ne fait plus appel à la responsabilité de la cible, à sa capacité de « répondre de » et de « répondre à ») - la cible donc, d'un telle non-politique c'est l'agent susceptible de modifier son environnement. Non pas l'acteur, porteur de projets, mais l'agent, source d'une énergie de nature à affecter son milieu, comme on le dirait d'une bactérie, bonne ou mauvaise¹⁴⁶⁵ ». Et d'ajouter: « ces mouvements (je ne dis plus: ces actes) ne sont alors pris en compte que dans leur contingence nue, comme risque ou opportunité, indépendamment de la signification subjective que leur auteur pourrait leur attribuer¹⁴⁶⁶ ».

¹⁴⁶¹ Le propos séduit les hommes politiques et les intellectuels: Luc Ferry, Jacques Attali s'insèrent pleinement dans ces débats

¹⁴⁶² DELMAS-MARTY Mireille, *Résister, responsabiliser, anticiper ou comment humaniser la mondialisation*, Editions du Seuil, janvier 2013, et du même auteur: *Aux quatre vents du monde Op. Cit.*.

¹⁴⁶³ En ce sens: DELMAS-MARTY Mireille, *Aux quatre vents du monde Op. cit.*, p. 103 et s.

¹⁴⁶⁴ En ce sens: voir: ROUVROY Antoinette, « Pour une défense de ... » *Op. Cit.*,

¹⁴⁶⁵ OST François, *A quoi sert le Droit ? Op. Cit.*, p. 312

¹⁴⁶⁶ *Ibid.*

670. Bien que frappant de réalité, ces propos choquent le juriste car ils confirment que loin d'émanciper l'individu, les technologies sont en train de l'asservir. Ils interrogent la signification même du principe, ou plutôt, du droit fondamental à l'égale dignité. Rappelons que le préambule de la Déclaration Universelle des Droits de l'Homme déclare que la « *dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables constitue le fondement de la liberté, de la paix et de la justice dans le monde* ». Quelle est donc aujourd'hui la dignité de cet homme pleinement objectivé et sommé d'agir conformément à un déterminisme social ? Plus encore, quelle est encore la possibilité d'action réservée aux individus ? La désinstitution du droit par la norme engendre la neutralisation de toute forme de désobéissance, elle permet de diluer la pensée de l'être humain dans une puissance rationalisatrice de l'action. Ainsi que le note Antoinette Rouvroy « *cette potentialité, ou puissance des sujets, ce que j'ai appelé précédemment du nom de « virtualité », est indépendante de ce qu'ils font effectivement, c'est-à-dire qu'elle est indépendante de toute forme d'actualisation. Cet élément de virtualité est, me semble-t-il, essentiel pour « définir » ce dont il s'agit lorsque l'on parle de subjectivité dans une perspective non humaniste. Partir de là, de la virtualité, défendre non le sujet, mais une sorte de puissance subjectivante nous renforce dans la perspective, évoquée plus haut, d'une inversion du point de vue qui nous permet d'appréhender les choses non plus sous l'angle du contrôle, ni de l'intentionnalité, mais sous celui de la récalcitance, de l'excès du monde sur le réel, de la récalcitance de la vie à toute tentative d'organisation excessive, et de la production de sens, toujours a posteriori, en retard sur les faits, à travers notamment le mécanisme juridique d'interpellation des sujets appelés à « rendre compte ». La possibilité de désobéir, souvent dénoncée comme le résultat de la faiblesse de la loi, participe au contraire de sa dignité, pourrait-on dire¹⁴⁶⁷ ».*

¹⁴⁶⁷ ROUVROY Antoinette, « Pour une défense de ... » Op. Cit, p. 146 - 147

Conclusion de Titre

671. La surveillance diffuse en tant que principal dispositif de contrôle attentionnel a permis un nivellement par le bas du Droit et de la Liberté. Par la transformation des espaces sociaux et l'objectivation des individus, la surveillance diffuse a engendré la réduction de toutes règles et de tout comportement à un calcul d'utilité fortement influencé par la rhétorique de l'utilitarisme. Plus qu'un nivellement par le bas, la surveillance diffuse est en train progressivement de désinstituer le Droit et les libertés fondamentales.

672. A travers l'instauration de sa propre régulation, principalement définie comme un comportementalisme numérique, la surveillance diffuse gère, incite, protège, dirige l'espace social et le comportement des populations. Elle endigue toute possibilité d'action, de réaction de la part des individus. Tout se passe alors comme si la croyance en la toute puissance technologique et en son efficacité, en sa rationalisation, permettait à l'Etat et aux entreprises de nier à la fois toute décision individuelle mais également toute décision politico-juridique au « *bénéfice du régulateur cybernétique*¹⁴⁶⁸ », qu'est devenue la surveillance diffuse. Cette dernière a bouleversé l'ensemble des notions traditionnelles du Droit en s'inscrivant comme l'aboutissement de l'utilitarisme libéral, qu'il soit économique ou culturel.

Ajoutons que la surveillance diffuse s'inscrit pleinement dans ce que Hannah Arendt écrivait concernant les sociétés totalitaires et le meurtre de la personnalité juridique. Le soft-totalitarisme, ou la totalisation numérique prôné par la surveillance et le contrôle social attentionnel qu'elle porte en elle, permettent de réduire l'homme en un objet. Poursuivant les conclusions de Arendt, il faut s'inquiéter de la domination totale qu'elle met en oeuvre sur l'individu mais également sur le Droit.

¹⁴⁶⁸ MOROZOV Evgeny, « The rise of data and the death of politics », *The Guardian*, 20 juillet 2014, Op. Cit.

Conclusion Partielle

673. Ainsi que le notait Christian Laval: « *la sécurité est la condition du bonheur général. Le bonheur est le grand but, la surveillance qui conditionne la sécurité est le principal levier pour y parvenir*¹⁴⁶⁹ ». Ces objectifs de bien-être, de liberté principalement réduite à un versant économique (la consommation), et de sécurité modifient les Etats de Droit, en des Etats de Droit libéraux. Réglementation algorithmique, solutionnisme technologique, calcul d'utilité, injonction à la visibilité, économie de la visibilité sont autant d'effets que la surveillance diffuse produit aujourd'hui. Du point de vue des individus, ainsi que le soulignait Ellul, ce dernier « *est dépossédé de son choix et il en est satisfait. Il l'accepte en donnant raison à la technique*¹⁴⁷⁰ »

674. L'élaboration du panoptique chez Bentham était inséparable de la logique du libéralisme en matière économique. La surveillance diffuse en représente la pleine consécration. Elle engendre un principe de transparence générale par le comportementalisme numérique et le solutionnisme technologique qu'elle sous-tend. Cette transparence générale est obtenue par l'hybridation du droit des données personnelles et à la protection de la vie privée, par le marché économique. Les nouveaux instruments européens en la matière contribuent à intégrer pleinement la surveillance diffuse dans nos sociétés contemporaines. Reconnaissance de l'économie fondée sur la donnée, protection assurée par les acteurs du marché, désinstitution progressive du droit à la vie privée par les objectifs fluctuants de la Nation sont autant d'éléments permettant à la surveillance diffuse d'obtenir sa plénitude d'action. Les notions traditionnelles du droit des données personnelles n'ont dans cette nouvelle configuration plus aucun sens. Et malgré les différentes invectives du juge européen, la vie privée semble également en perte de symbolique et de sens normatif.

675. La surveillance diffuse, dans cette nouvelle configuration du droit des données personnelles et de la protection de la vie privée, devient une norme sociale qui influence le comportement et l'environnement des individus. Véritable consécration du monstre doux de Tocqueville, la surveillance diffuse désinstitutionne le Droit par son influence sur les espaces sociaux engendrant l'éclatement de la dichotomie public-privé, mais également sur les individus devenus des insujets non plus de droit, mais de norme. Le Droit fonctionne sans espace d'application et sans sujet de Droit. La normalisation des comportements, et son aboutissement technique, le nudge, viennent

¹⁴⁶⁹ LAVAL Christian, « Surveiller et prévenir - la nouvelle société panoptique », *Op. Cit.*, p. 52

¹⁴⁷⁰ ELLUL Jacques, *Op. Cit.*, p. 77

alors progressivement remplacer le Droit et la raison du Droit par la vertu et la responsabilisation des individus, sommés d'agir dans un conformisme social prônant bien-être, consommation, et sécurité.

676. Ainsi que le rappelait Neil Postman, la surveillance diffuse est également, comme toute technique, porteuse d'une idéologie et de profondes mutations pour la société. Postman déclarait alors, que les modifications de la société américaine de l'époque ne correspondaient à « *aucune idéologie formulée. (...). Ce n'est que la conséquence d'un changement radical dans nos modes de conversation publique. Mais cela relève néanmoins d'une idéologie qui impose un mode de vie, un type de relations entre les gens et les idées, et à propos desquels il n'y a pas eu de consensus, pas de discussion, pas d'opposition. Seulement de la complaisance* ¹⁴⁷¹ ». Et de conclure avec un ton désabusé que, « *la conscience publique n'a pas encore assimilé le fait que toute technique est porteuse d'une idéologie, alors que devant nos yeux, les nouvelles techniques ont transformé tous les aspects de la vie au cours des quatre-vingt dernières années. (...). Ne pas avoir conscience qu'une technique arrive équipée d'un programme de changement social, maintenir que la technique est neutre, penser que la technique est toujours l'amie de la culture est, à cette heure tardive, une stupidité pure et simple* ¹⁴⁷² ».

¹⁴⁷¹ POSTMAN Neil, *Se distraire à en mourir*, Traduit de l'américain par Thérèse de Chérissey, Préface de Michel Rocard, Editions Fayard, Collection Pluriel, 2010, p. 233 - 234

¹⁴⁷² Ibid. p. 234.

Conclusion Générale

Phénomène à diffusion mondiale, la surveillance s'est institutionnalisée dans les sociétés contemporaines. Elle est même devenue la principale caractéristique de la culture contemporaine en crise. Jacques Ellul évoquait à plusieurs reprises dans ses ouvrages consacrés à la technique, la notion de plasticité sociale. On retiendra sa première analyse¹⁴⁷³ de 1954, où Ellul écrivait que « *en réalité, nous avons une société atomisée et qui s'atomisera de plus en plus: l'individu reste la seule grandeur sociologique, mais on s'aperçoit que bien loin de lui assurer sa liberté, cela provoque le pire des esclavages. Cette atomisation confère à la société la plus grande plasticité possible. Et ceci est aussi, du point de vue positif, une condition décisive de la technique: c'est en effet la rupture des groupes sociaux qui permettra les énormes déplacements d'hommes au début du XIXème siècle qui assurent la concentration humaine qu'exige la technique moderne. (...). Voilà l'influence de la plasticité sociale. Sans elle pas d'évolution technique possible. Dans cette société atomisée, en face de l'individu, il n'y a plus que l'Etat, qui est fatalement l'autorité suprême, et qui se change aussi bien en autorité toute puissante. Ceci nous donne une société parfaitement malléable et d'une ductilité remarquable au point de vue intellectuel comme au point de vue matériel. Le phénomène technique y a son milieu le plus favorable depuis le début de l'histoire humaine*¹⁴⁷⁴ ». La surveillance diffuse s'inscrit pleinement dans ce que Ellul décrit quant à la plasticité sociale. La malléabilité de la société toute entière a été consacrée en poursuivant les objectifs de la société de l'information, en désinstitutionnant le droit des données personnelles et de la protection de la vie privée. En jouant sur les peurs, la sécurité, le bien-être et en produisant une nouvelle forme de gouvernamentalité, la surveillance diffuse a rendu les sociétés contemporaines malléables et entièrement tournées vers la consommation technologique.

A l'image des premières lignes de cette citation, bien loin d'assurer à l'individu une liberté, une émancipation, la surveillance diffuse élabore le pire des asservissements. De son intégration sociale et de son acculturation, il faut d'abord retenir que les premières législations informatiques et libertés ont en quelque sorte permis, du fait d'un double déficit d'effectivité et de conscience des enjeux propres à la surveillance diffuse, de donner une assise juridique à la surveillance. En parallèle, l'élaboration de politique managériale de sécurité, la gouvernamentalité par la peur, et l'explosion des usages technologiques ont engendré un besoin et une demande de protection, de

¹⁴⁷³ ELLUL Jacques, *La technique ou l'Enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990

¹⁴⁷⁴ Ibid. p. 47 - 48.

sécurité, de technologies. Demande, offre et consommation participent d'un langage économique qu'il faut d'abord appliquer à la surveillance diffuse. Les nouveaux instruments européens en matière de protection des données personnelles et de libre circulation des données non personnelles ont permis d'appliquer ces mêmes concepts à l'économie fondée sur la donnée. Le principal problème reste alors la compréhension des enjeux de la surveillance diffuse: normalisation des comportements des individus par la gouvernementalité algorithmique, libéralisme et utilitarisme économique, prédiction en temps réel comportent en eux un programme déshumanisant l'individu. Le « nouveau » droit des données personnelles représente alors un acte manqué dans l'élaboration d'une véritable protection de la vie privée des individus. Et, s'il n'est pas un acte manqué, il doit être analysé comme une véritable prise en compte par les institutions européennes d'un Droit devenu lui même libéral. Le Droit semble en effet réduit à un rôle d'opérateur économique. Tout se passe aujourd'hui comme si le Droit, la loi ne devaient servir qu'à assurer une logique marchande. La marchandisation de la vie privée en est la parfaite illustration.

L'introduction de ce travail a commencé par un rapprochement de la surveillance diffuse avec des concepts tels que la fiction, la fiction instituante et l'utopie. En référence à ces lignes, et en guise de conclusion notons avec Leszek Kolakowski que les trois traits typiques de la pensée utopique sont: *« la croyance que l'avenir, de quelque manière mystérieuse, serait déjà là et que nous serions en mesure de le saisir (et pas seulement de le prévoir de manière incertaine), l'idée que nous disposerions d'une méthode de pensée et d'action sûre, susceptible de nous conduire vers une société libre de défauts, de conflits et d'insatisfactions, la croyance selon laquelle nous saurions ce que l'homme est « réellement », en vérité, par opposition à ce qu'il est empiriquement et à ce qu'il croit être - et que nous saurions en quoi consiste sa véritable nature, par opposition à sa nature empirique contingente. Chacune de ces trois composantes de la foi utopique est utilisée pour nous fournir la justification et l'excuse de n'importe quelle barbarie¹⁴⁷⁵ »*. L'ensemble des traits dégagés par Kolakowski concernant l'utopie et la pensée utopique font étrangement écho à la surveillance diffuse et à la culture de la surveillance. Alors que la surveillance est perpétuellement critiquée quant à sa dynamique sécuritaire et commerciale, et son échec à prévenir le terrorisme ou les actes de délinquance, on peut s'étonner que ce dispositif de pouvoir soit maintenu. Dans la réalité, à l'image de ce qu'écrit Kolakowski, la surveillance tire, de son échec, sa force, car elle renforce les logiques qui la sous-tendent: sécurité, liberté, bien-être, méthode d'action et de pensée

¹⁴⁷⁵ KOLAKOWSKI Leszek, *L'esprit révolutionnaire suivi de marxisme : utopie et anti-utopie*, traduction de l'anglais, de l'allemand et postface Jacques Dewitte, Editions Complexe, Presses Universitaires de France, 1978, p. 131

sûre, normalisation des comportements et conformisme social, société aseptisée de tout risque, connaissance de la véritable nature de l'homme par son objectivation. Ces composantes de la surveillance diffuse éludent totalement la compréhension de la nouvelle forme de servitude volontaire de l'individu qu'elle contribue à créer.

Bibliographie

I. Les ouvrages

- **AGAMBEN Giorgio**, *Homo Sacer I, le pouvoir souverain et la vie nue*, Editions du Seuil, Paris, 1997
- **AGAMBEN Giorgio**, *La communauté qui vient -Théorie de la singularité quelconque*, paris, Seuil, 1990
- **AGAMBEN Giorgio**, *Qu'est ce qu'un dispositif ?*, Editions Rivages, Collection Rivage poche, 2014
- **AMSELEK Paul**, *Méthode phénoménologique et théorie du droit*, Paris, LGDJ, 1964
- **ANDERS Günther**, *L'obsolescence de l'homme- Sur l'âme à l'époque de la deuxième révolution industrielle*, tome 1, traduction française 2001, Paris, Éditions de l'Encyclopédie des Nuisances : Éditions Ivrea, 2001
- **ANDERS Günther**, *L'obsolescence de l'homme- Sur la destruction de la vie à l'époque de la troisième révolution industrielle*, tome 2, traduction française 2011, Paris, Éditions Fario, 2011
- **ARENDT Hannah**, *Condition de l'homme moderne* ; traduit de l'anglais par Georges Fradier ; préface de Paul Ricoeur, Paris, Pocket, 2009
- **ARENDT Hannah**, *La crise de la culture - Huit exercices de pensée politique*, Traduit de l'anglais sous la direction de Patrick Lévy, Collection Folio Essais, n°113, Editions Gallimard, 2016
- **ARENDT Hannah**, *Les origines du totalitarisme volume 1 ; suivi de Eichmann à Jérusalem*, édition établie sous la direction de Pierre Bouretz, traduction de Micheline Pouteau, Martine Leiris, Jean-Louis Bourget (et al.), Paris, Gallimard, 2002
- **ARENDT Hannah**, *Les origines du totalitarisme, volume 2, L'impérialisme*, Paris, Éditions du Seuil, 1997
- **ARENDT Hannah**, *Les origines du totalitarisme, volume 3 : sur l'antisémitisme*, Paris, Éditions du Seuil, 1984
- **AUBERT Nicole, HAROCHE Claudine (sous la direction de)**, *Les tyrannies de la visibilité - Etre visible pour exister?*, Editions Eres, Collection Sociologie clinique, 2011
- **BALLE Francis, COHEN-TANUGI Laurent**, *Dictionnaire du web*, 1ère édition, Dictionnaires Dalloz, Editions Dalloz-Sirey, 2001
- **BARD Alexander, SODERQVIST Jan**, *Les Netocrates 2, The Body machine*, traduit de

- l'anglais par Abeline Majorel, Editions Léo Scheer, 2011
- **BARJAVEL René**, *Ravage*, Folio, Gallimard, 1972
 - **BATIFFOL Henri**, *Traité élémentaire de droit international privé*, 2ème édition, 1955
 - **BAUMAN Zygmunt**, *L'amour liquide - De la fragilité des liens entre les hommes*, Fayard / Pluriel, 2010
 - **BAUMAN Zygmunt**, *Le coût humain de la mondialisation*, Fayard / pluriel, 2011
 - **BAUMAN Zygmunt**, *Le présent liquide - peurs sociales et obsession sécuritaire*, Editions du Seuil, 2007
 - **BAUMAN Zygmunt**, *La société assiégée*, Fayard / Pluriel, 2014
 - **BAUMAN Zygmunt**, *La vie liquide*, Fayard / Pluriel, 2013
 - **BECK Ulrich**, *La société du risque – Sur la voie d'une autre modernité*, Flammarion – Champs, 2001
 - **BECKER Howard**, *Outsiders: Etudes de sociologie de la déviance*, Editions Métailié, 2012
 - **BELL Daniel**, *Vers la société post-industrielle*, Robert Laffont, Paris, 1976
 - **BENNETT Colin, HAGGERTY Kevin, LYON David, STEEVES Valérie (sous la direction de)**, *Vivre à nu: la surveillance au Canada -Projet sur la nouvelle transparence* , Athabasca University Press, 2014
 - **BENTHAM Jérémy**, *Panoptique*, Mille et une nuits, département de la librairie Arthème Fayard, Septembre 2002
 - **BERGSON Henri**, *Les deux sources de la morale et de la religion*, Presses Universitaires de France, Paris, 1932
 - **BERNARD François (de)**, *L'homme post-numérique - Face à la société de surveillance générale*, Editions Yves Michel, 2015
 - **BERTRAND André**, *Droit d'auteur*, Editions Dalloz, Collection Dalloz Action, 2010
 - **BIGO Didier, BONELLI Laurent et DELTOMBE Thomas (sous la direction de)**, *Au nom du 11 septembre ... Les démocraties à l'épreuve de l'antiterrorisme*, éditions La découverte, 2008
 - **BOURDIEU Pierre**, *Contre-feux - Pour un mouvement social européen*, Raisons d'Agir, 2001
 - **BOURDIEU Pierre**, *La Distinction - Critique sociale du jugement*, Les éditions de Minuit, Collection Le sens commun, Paris, 1979
 - **BOYLE James**, *The Public Domain - Enclosing the commons of the Mind*, Yale University Press, New Haven & London, 2008, En ligne: <http://thepublicdomain.org/thepublicdomain1.pdf> (dernière consultation: 5 mars 2018)
 - **BRETON Philippe**, *L'utopie de la communication - le mythe du village planétaire*, Collection

Essais, Editions La Découverte / Poche, 1997

- **BRETON Philippe, POULX Serge**, *L'explosion de la communication - Introduction aux théories et aux pratiques de la communication*, Collection Grands Repères / Manuels, 4ème édition, La Découverte, 2012
- **BRZEZINSKI Zbigniew**, *La révolution technétronique*, traduit de l'américain par Jean Viennet, Collection Liberté de l'esprit, Calmann-Lévy, Paris, 1971
- **BRZEZINSKI Zbigniew**, *Le grand échiquier: l'Amérique et le reste du monde*, Editions Fayard, Paris, 1997
- **BURGORGUE-LARSEN Laurence (sous la direction de)**, *La France face à la Charte des Droits Fondamentaux de l'Union Européenne*, collection du CREDHO, édition Bruylant, 2005
- **CAMPBELL Duncan**, *Surveillance électronique planétaire*, Allia, 2001
- **CARBONNIER Jean**, *Droit et passion du droit sous la Vème République*, Champs Flammarion, 1996
- **CASSIN Barbara**, *Google-moi, La deuxième mission de l'Amérique*, Collection Banc Public, Editions Albin Michel, 2007
- **CASTELLS Manuel**, *La société en réseaux - l'ère de l'information*, traduit de l'anglais par Philippe Delamare, Fayard, 1998
- **CASTETS-RENARD Céline**, *Droit de l'Internet*, Montchrestien, Lextenso éditions, Collection Cours, 2010
- **CATALA Pierre**, *Le droit à l'épreuve du numérique - Jus ex Machina*, Presses Universitaires de France, Collection Droit, Ethique, Société, Première édition, mai 1998
- **CAZALA Julien**, *Le principe de précaution en Droit International*, Bibliothèque de l'institut des hautes études internationales de Paris, collection dirigée par Jean Combacau et Joe Verhoeven, Anthémis, 2006
- **CHANTEUR Janine**, *Du droit des bêtes à disposer d'elles-mêmes*, Editions du Seuil, Collection Couleur des idées, 1993
- **CHAPUS René**, *Droit Administratif Général – Tome 1*, 15ème édition, Montchrestien, 2001
- **CHARBONNEAU Bernard**, *L'État*, Éditions Economica, Collection Classique des sciences sociales, Pais, 1987
- **CHARBONNEAU Bernard**, *Le jardin de Babylone*, Éditions de l'Encyclopédie des Nuisances, 2002
- **CHARBONNEAU Bernard**, *Prométhée réenchaîné*, Éditions La table ronde, Collection la petite vermillon, 2001

- **CHARBONNEAU Bernard**, *Le système et le chaos – où va notre société ?*, préface de Daniel Cérézuelle, Éditions Sang de la terre – Medial, Collection La pensée écologique, 2012
- **CHARBONNEAU Bernard et ELLUL Jacques**, *Nous sommes des révolutionnaires malgré nous : textes pionniers de l'écologie politique*, Textes présentés par Quentin Hardy, Éditions du Seuil, collection Anthropocène, 2014
- **CHOMSKY Noam, HERMAN Edward**, *La fabrication du consentement - De la propagande médiatique en démocratie*, Editions Agone, Collection Contre-feux, 2008
- **CITTON Yves (sous la direction de)**, *L'économie de l'attention - Nouvel horizon du capitalisme ?*, Editions La Découverte, Paris, 2014
- **CITTON Yves**, *Mythocratie - Storytelling et imaginaire de gauche*, Editions Amsterdam, Paris, 2010
- **COMBY Jean-Baptiste**, *La question climatique: genèse et dépolitisation d'un problème public*, Collection Raison d'agir - Cours et travaux, Liber, 2015
- **CONSTANT Benjamin**, *Principes de politique applicables à tous les gouvernements représentatifs et particulièrement à la constitution actuelle de la France*, Chez Alexis Eymery, Libraire, rue Mazarine, N° 30, Mai 1815, En ligne: http://davidmhart.com/liberty/FrenchClassicalLiberals/Constant/Books/Constant_1815Principes_de_Politique.pdf (dernière consultation: 5 mars 2018)
- **CORNU Marie, ORSI Fabienne, ROCHFELD Judith (sous la direction de)**, *Dictionnaire des biens communs*, PUF / Humensis, Collection Quadrige, 2017
- **CREPON Marc**, *La culture de la peur - I. Démocratie, identité, sécurité*, Collection La philosophie en effet, Galilée, 2008
- **DAKHLI Leyla, MARIS Bernard, SUE Roger, VIGARELLO Georges**, *Gouverner par la peur*, Collection Transversales, Fayard, 2007
- **DAMASIO Alain**, *La Zone du Dehors*, Folio - Science-Fiction n°350, Gallimard, 2014
- **DARWIN Charles**, *L'origine des espèces: au moyen de la sélection naturelle ou la préservation des races favorisées dans la lutte pour la vie*, Flammarion, 2008
- **DEBORD Guy**, *La société du spectacle*, Editions Gallimard, Paris, 1992
- **DEBRAY Régis**, *Le nouveau pouvoir*, Les éditions du Cerf, Collection Médium - Transmettre pour innover, 2017
- **DEFERT Daniel et EWALD François (sous la direction de)**, *Michel Foucault, Dits et écrits 1954 - 1988, I. 1954 - 1975*, Editions Quarto Gallimard, 2001
- **DEFERT Daniel et EWALD François (sous la direction de)**, *Michel Foucault, Dits et écrits*

- 1954 - 1988, II. 1976 - 1988, Editions Quarto Gallimard, 2001
- **DELEUZE Gilles**, *Foucault*, Les Editions de Minuit, Paris, 2004
 - **DELEUZE Gilles, GUATTARI Félix**, *Mille plateaux, Capitalisme et schizophrénie II*, Paris, Minuit, 1980
 - **DELMAS- MARTY Mireille**, *Aux quatre vents du monde - Petit guide de navigation sur l'océan de la mondialisation*, Editions du Seuil, Version numérique réalisée par Nord Compo, Septembre 2016
 - **DELMAS-MARTY Mireille**, *Libertés et sûreté dans un monde dangereux*, Editions du Seuil, Collection La couleur des idées, 2010
 - **DEMOGUE René**, *Les notions fondamentales du droit privé : Essai critique, pour servir d'introduction à l'étude des obligations*, Librairie nouvelle de droit et de jurisprudence Arthur Rousseau, Paris, 1911
 - **DE TOCQUEVILLE Alexis**, *De la démocratie en Amérique II*, (3ème et 4ème parties), Collection Garnier-Flammarion, Editions Flammarion, 1999
 - **DOCTOROW Cory**, *Little Brother*, Pocket Jeunesse, Janvier 2012
 - **DUCLOS Denis**, *La peur et le savoir : la société face à la science, la technique et leurs dangers*, La Découverte, 1990
 - **DUPUY Pierre- Marie**, *Droit International Public*, 9ème édition, Dalloz, 2008
 - **ELIAS Norbert**, *La civilisation des moeurs*, Editions Calmann-Lévy, Collection Pocket, 1973
 - **ELIAS Norbert**, *La dynamique de l'occident*, Editions Calmann-Lévy, 1975
 - **ELIAS Norbert**, *La société des individus*, Editons Fayard, Collection Agora, 1991
 - **ELLUL Jacques**, *Le bluff technologique*, préface de Jean-Luc Porquet, *Ellul l'éclaireur*, Hachette, 1988 ; réédition Hachette Littératures, collection « Pluriel », 2004
 - **ELLUL Jacques**, *Le Système Technicien*, préface de Jean-Luc Porquet, *Ellul l'avait bien dit*, Calmann-Lévy, 1977 ; réédition Le Cherche-Midi, 2004
 - **ELLUL Jacques**, *La technique ou l'Enjeu du siècle*, Armand Colin, 1954 ; réédition Economica, 1990
 - **ENTHOVEN Raphaël**, *Little Brother*, Editions Gallimard, Collection Blanche - Essais, 2017
 - **ERSKINE Ralph et SMITH Michael**, *The Bletchley Park Codebreakers : Dialogue Espionage Classics*, Biteback, 20 janvier 2011
 - **FEDERBUSCH Serge**, *La marche des lemmings. La deuxième mort de Charlie Hebdo*, Ixelles Editions, 2015
 - **FERAL-SCHUHL Christiane**, *Cyberdroit, le Droit à l'épreuve de l'Internet*, Praxis Dalloz

2009/2010

- **FLORIN Agnès, PREAU Marie**, *Le bien-être*, L'Harmattan, 2013
- **FOREST David**, *Abécédaire de la société de surveillance*, Éditions Syllepse, 2009
- **FOUCAULT Michel**, *Il faut défendre la société - Cours au collège de France. 1976*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 1997
- **FOUCAULT Michel**, *Les anormaux - Cours au collège de France. 1974 -1975*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 1999
- **FOUCAULT Michel**, *L'herméneutique du sujet - Cours au collège de France, 1981 -1982*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 2001
- **FOUCAULT Michel**, *Sécurité, territoire, population Cours au collège de France. 1977 - 1978*, Collection Hautes Etudes, Ecole des Hautes études en sciences sociales, Editions Gallimard et Editions du Seuil, 2004
- **FOUCAULT Michel**, *Surveiller et punir - Naissance de la prison*, Editions Gallimard (numérique), 2013
- **FRIEDMANN Georges**, *Sept études sur l'homme et la technique*, Collection Bibliothèque Médiations, Gallimard 1971, Première parution en 1966
- **FRIER Pierre-Laurent**, *Précis de Droit Administratif*, 3^{ème} édition, Montchrestien, 2004
- **GANASCIA Jean-Gabriel**, *Voir et pouvoir : qui nous surveille ?*, Editions Le Pommier, Collection Les Essais 2009
- **GAUTRAIS Vincent**, *Neutralité technologique - Rédaction et interprétation des lois face aux changements technologiques*, Les Editions Themis, Montréal, Mai 2012, En ligne: <https://www.gautrais.com/publications/neutralite-technologique/> (dernière consultation: 5 mars 2018)
- **GIBSON William**, *Neuromancien*, Collection Science Fiction, Editions J'ai Lu, 2001
- **GICQUEL Jean**, *Droit Constitutionnel et institutions politiques*, 22^{ème} édition, Montchrestien, 2008
- **GLENNON Michael**, *National security and double government*, Oxford University Press, 2015
- **GODIN Seth**, *Tous les marketeurs sont des menteurs*, traduction de All Marketers are Liars, Les éditions Transcontinental, 2006
- **GOLDSTEIN Brett, DYSON Lauren (éds.)**, *Beyond Transparency - Open Data and the Future Civic Innovation*, Code for America Press, San Francisco, 2013, En ligne: <http://>

beyondtransparency.org/pdf/BeyondTransparency.pdf (dernière consultation: 5 mars 2018)

- **GUILLIEN Raymond et VINCENT Jean (sous la direction de)**, *Lexique des termes juridiques*, 14e édition, 2003
- **HABERMAS Jürgen**, *L'espace public: archéologie de la publicité comme dimension constitutive de la société bourgeoise*, traduit de l'allemand par M.B. de Launay, Editions Payot, Paris, 1978
- **HARDT Michel, NEGRI Antonio**, *Empire*, Harvard University Press, Cambridge, Massachusetts - London, England, 2000
- **HAVEL Vaclav**, *Essais politiques*, textes réunis par Roger Errera et Jan Vladislav, Collection Liberté de l'esprit, Calmann- Lévy, 1989
- **HAZAN Eric**, *Lingua Quintae Respublicae - La propagande au quotidien*, Editions Raisons d'agir, 2006
- **HEGEL Friedrich**, *Principes de la philosophie du droit*, traduit par R. Derathé, Paris, Vrin, 1986
- **HEIDEGGER Martin**, *Essais et conférences -La question de la technique ;* traduction par André Préau, Éditions Gallimard, Collection Tel, 1988
- **HOBBS Thomas**, *Du Citoyen*, présentation et traduction par Philippe Crignon, Editions Flammarion, Collection G.F. 1442, 2010
- **HUXLEY Aldous**, *Le meilleur des mondes*, Cooltour, 25 avril 2015
- **ILLICH Ivan**, *La convivialité*, Collection Points. Série Essais, Éditions du Seuil, Paris, 1973
- **JULIA Didier**, *Dictionnaire de la philosophie*, Larousse, 1995
- **KAFKA Franz**, *Le Procès*, Editions Gallimard, Collection Folio Classique, 1987
- **KESSOUS Emmanuel**, *L'attention au monde, sociologie des données personnelles à l'ère du numérique*, Editions Armand Colin, Collection Recherches, 2012
- **KOLAKOWSKI Leszek**, *L'esprit révolutionnaire, suivi de marxisme : utopie et anti-utopie*, traduction de l'anglais, de l'allemand et postface Jacques Dewitte, Editions Complexe, Presses Universitaires de France, 1978
- **KUHN Thomas**, *La structure des révolutions scientifiques*, Flammarion, Paris, 1970
- **LAFFAIRE Marie-Laure**, *Protection des données à caractère personnel*, éditions d'organisation, 2005
- **LAFONTAINE Céline**, *L'empire cybernétique – Des machines à penser à la pensée machine*, Essai, Editions du Seuil, Février 2004
- **LASCH Christopher**, *La culture du Narcissisme – La vie américaine à un âge de déclin des espérances*, Collection Sisyphe, Éditions Climats, 2000
- **LASCH Christopher et CASTORIADIS Cornelius**, *La culture de l'égoïsme*, Postface de Jean-

- Claude Michéa, Editions Climats, 2012
- **LASSWELL Harold**, *Propagande technique in the World War*, Alfred Knopf Inc., New York, 1927
 - **LAVENUE Jean-Jacques, VILLALBA Bruno (éds)**, *Vidéosurveillance et détection automatique des comportements anormaux - Enjeux techniques et politiques*, Presses Universitaires du Septentrion, 2011
 - **LEVY Pierre**, *L'intelligence collective – Pour une anthropologie du cyberspace*, Collection Sciences et Société, Editions La Découverte, 1994
 - **LIANOS Michalis**, *Le nouveau contrôle social - Toile institutionnelle, normativité et lien social*, Editions L'Harmattan, Collection Logiques Sociales, 2001
 - **Ligue des droits de l'Homme**, *Une société de surveillance ? L'état des droits de l'Homme en France*, La découverte, édition 2009
 - **LIPPMANN Walter**, *Public opinion*, New York, Harcourt, Brace and Company, 1922
 - **LIPPMANN Walter**, *The Phantom Public*, New York, Harcourt, Brace and Company, 1925
 - **LUCRECE**, *De la nature des choses*, traduit du latin par H. Clouard, G.F.- Flammarion, Paris, 1964
 - **LYON David**, *Surveillance after Snowden*, Polity Press, 2015
 - **LYON David**, *Surveillance society: monitoring everyday life*, Open University Press, Buckingham - Philadelphia, 2001
 - **LYON David**, *Surveillance Studies : An overview*, Polity Press, 2007
 - **MACHIAVEL Nicolas**, *Le Prince et autres textes*, Union Générale d'Éditions, Collection 10-18, Paris, 1962
 - **MACHLUP Fritz**, *Knowledge: Its Creation, Distribution and Economic Significance*, Volume III, Princeton University Press 1984
 - **MACHLUP Fritz**, *The Production and distribution of knowledge in the United States*, Princeton University Press, 1962
 - **MALAURIE Jean**, *Terre Mère*, Paris, CNRS éditions, 2008
 - **MALRAUX André**, *La tentation de l'occident*, in. *Oeuvres complètes*, tome 1, 1989
 - **MANACH Jean-Marc**, *La vie privée, un problème de vieux cons?*, Limoges, Editions Fyp, collection Présence, 2010
 - **MARX Karl**, *Le Capital, critique de l'économie politique*, Presses Universitaires de France, Collection Quadrige Grands Textes, 2009
 - **MATTELART Armand**, *Histoire de la société de l'information*, 4ème édition, Collection

- Repères, Editions La découverte, 2009
- **MATTELART Armand**, *Histoire de l'utopie planétaire - De la cité prophétique à la société globale*, La Découverte / Poche, 2009
 - **MATTELART Armand et Michèle**, *Histoire des théories de la communication*, 3ème édition, Collection Repères, Editions La découverte, Paris, 2004
 - **MATTELART Armand, NEVEU Erik**, *Introduction aux cultural studies*, Collection Repères, Editions La Découverte, Paris, 2008
 - **MATTELART Armand**, *La communication-monde - Histoire des idées et des stratégies*, La Découverte / Poche, 1999
 - **MATTELART Armand**, *La globalisation de la surveillance - Aux origines de l'ordre sécuritaire*, Editions la découverte, 2007
 - **MATTELART Armand**, *L'invention de la communication*, La Découverte / Poche, 2011
 - **MAUSS Marcel**, *Essai sur le don - Formes et raisons de l'échange dans les sociétés primitives*, édition électronique réalisée par Jean-Marie Tremblay, professeur de sociologie au Cégep de Chicoutimi, 2002, En ligne: <http://anthropomada.com/bibliotheque/Marcel-MAUSS-Essai-sur-le-don.pdf> (dernière consultation: 5 mars 2018)
 - **MC MILLAN Stuart**, *Se distraire à en mourir - BD: Aldous Huxley & George Orwell par Neil Postman*, traduction Jessica Aubin, Mai 2009, En ligne: <http://partage-le.com/2016/08/se-distraire-a-en-mourir-bd-huxley-orwell-par-neil-postman/> (dernière consultation: 5 mars 2018)
 - **MICHEA Jean-Claude**, *L'empire du moindre mal - Essai sur la civilisation libérale*, Editions Flammarion, Collection Champs Essai, 2010
 - **MOISI Dominique**, *La géopolitique de l'émotion*, Nouvelle édition, Collection Champs actuel, Flammarion, 2008
 - **MOROZOV Evgeny**, *L'aberration du solutionnisme technologique - Pour tout comprendre cliquez ici*, Editions FYP, Collection Innovation, 2014
 - **MUCCHIELLI Laurent**, *Criminologie et lobby sécuritaire - Une controverse française*, Collection Mouvements de société, Editions La dispute, 23 janvier 2014
 - **MUMFORD Lewis**, *technique et civilisation* ; traduit de l'américain par Denise Moutonnier, Éditions du Seuil, Les collections Esprit – La cité prochaine, Paris, 1950
 - **NEGROPONTE Nicholas**, *L'homme numérique*, Robert Laffont, 1995
 - **NYE Joseph**, *Bound to lead: the changing nature of American power*, Basic Books, 1990
 - **NYE Joseph**, *Soft power - the means to success in world politics*, Public Affairs, New York, 2004
 - **NYE Joseph**, *The future of power*, Public Affairs, New York, 2011

- **OPPENHEIMER Robert**, *La science et le bon sens*, Traduit de l'anglais par Albert Colnat, Collection Idées, Gallimard, 1955
- **ORWELL George**, *1984*, Traduit de l'anglais par Amélie Audiberti, Folio, Gallimard, 2003
- **OST François**, *A quoi sert le Droit ? - Usages, Fonctions, Finalités*, Editions Bruylant, Collection Penser le Droit, 2016
- **OST François**, *Le temps du Droit*, Odile Jacob, Novembre 1999, Paris
- **OST François**, *Raconter la loi - Aux sources de l'imaginaire juridique*, Odile Jacob, 2004
- **PEDROT Philippe (sous la direction de)**, *Traçabilité et responsabilité*, Economica, 2003
- **PELEGRIN - GENEL Elisabeth**, *Des souris dans un labyrinthe - Décrypter les ruses et manipulations de nos espaces quotidiens*, Editions La Découverte / Poche, n° 377, 2012
- **POLONY Natacha & Le Comité Orwell**, *Bienvenue dans le PIRE DES MONDES - Le triomphe du soft totalitarisme*, Editions Plon, Paris, 2016
- **PORQUET Jean-Luc**, *Jacques Ellul, l'homme qui avait (presque) tout prévu*, Le Cherche-Midi, 2003, réédition 2012
- **POSTEL Jacques**, *Dictionnaire de la psychiatrie*, Collection In Extenso, Larousse, 2011
- **POSTMAN Neil**, *Se distraire à en mourir*, Traduit de l'américain par Thérèse de Chérisey, Préface de Michel Rocard, Editions Fayard, Collection Pluriel, 2010
- **PRESTON William, HERMAN Edward, SCHILLER Herbert**, *Hope and Folly, The United States and Unesco - 1945 - 1985*, Media and Society, University of Minnesota Press, Minnesota Archive Edition, 1989
- **RIESEL René, SEMPRUN Jaime**, *Catastrophisme, administration du désastre et soumission durable*, Editions de l'encyclopédie des Nuisances, Paris, 2008
- **RIGOUSTE Mathieu**, *La généalogie coloniale et militaire de l'ordre sécuritaire dans la France contemporaine*, Collection La Découverte Poche/Essais n°348, Éditions Broché, juin 2011
- **ROUSSEAU Jean-Jacques**, *Oeuvres complètes - Tome deuxième - La nouvelles héloïse, Emile, Lettre à M. de Beaumont*, Chez Furne, Librairie - Editeur, Paris
- **RIVERO Jean**, *Libertés Publiques*, Montchrestien, 1989
- **SADIN Eric**, *La vie algorithmique - Critique de la raison numérique*, Editions L'échappée, Collection Pour en finir avec, 2015,
- **SADIN Eric**, *surveillance Globale - enquête sur les nouvelles formes de contrôle*, Flammarion, Climats, 2009
- **SALE Kirkpatrick**, *La révolte luddite – Briseurs de machines à l'ère de l'industrialisation*, Traduit de l'anglais par Célia Izoard, Editions L'échappée, Collection Dans le feu de l'action,

2006

- **SALMON Christian**, *Storytelling, La machine à fabriquer des histoires et à formater les esprits*, Éditions La découverte, 2007,
- **SCHILLER Herbert**, *Communication and cultural domination*, White Plains, New York, International Arts and Sciences Press, 1976
- **SCHILLER Herbert**, *Mass Communications and American Empire*, Beacon Press, 1969
- **SCHNEIDER Michel**, *Big Mother; Psychopathologie de la vie politique*, Odile Jacob, 2002
- **SCHUMPETER Joseph**, *Capitalisme, socialisme et démocratie*, Traduction française de Gaël Fain, 1942, Paris, éd. Payot
- **SENNETT Richard**, *Les tyrannies de l'intimité*, Editions du Seuil, 1979
- **SERIS Jean-Pierre**, *La technique*, Presses Universitaires de France, 2000
- **SERRES Michel**, *Petite Poucette*, Le pommier, 2012
- **SFEZ Lucien**, *Critique de la Communication*, Paris, 1988, Seuil, « Empreintes », réédition Seuil – Essais, 1992
- **SFEZ Lucien**, *Technique et Idéologie. Un enjeu de pouvoir*, Editions du Seuil, La couleur des idées, Paris, 2002
- **SIMONE Raffaele**, *Le Monstre doux - L'Occident vire-t- il à droite ?*, traduit par Katia Bienvenu, Collection Le Débat, Gallimard, 2010
- **SKINNER Burrhus**, *Par delà la liberté et la dignité*, traduit de l'américain par Anne-Marie et Marc Richelle, Collection Libertés 2000, Editions Robert Laffont, 1971
- **SLOTERDIJK Peter**, *Règles pour le parc humain, suivi de La domestication de l'Être*, Editions Fayard, Milles et une nuits, 2010
- **SOFSKY Wolfgang**, *Le citoyen de verre - entre surveillance et exhibition*, Traduit de l'allemand et préfacé par Olivier Mannoni, Editions de l'Herne, Paris, 2011
- **SOLJENITSYNE Alexandre**, *Le pavillon des cancéreux*, Pocket, 2005
- **STIEGLER Bernard**, *La société automatique - 1. L'avenir du travail*, Editions Fayard, 2015
- **SUE Roger**, *La société contre elle-même*, Collection Transversales, Fayard, 2005
- **SUPIOT Alain**, *Homo juridicus - Essai sur la fonction anthropologique du Droit*, Editions du Seuil, Collection La couleur des idées, 2005
- **SUPIOT Alain**, *La gouvernance par les nombres - Cours au Collège de France (2012 - 2014)*, Fayard, Collection Poids et mesures du monde, 2015
- **TABUTEAU Didier**, *Les contes de Ségur : les coulisses de la politique de santé (1988 – 2006)*, Ophrys, 2006

- **TARDE Gabriel**, *Les lois de l'imitation – Étude sociologique*, 7ème édition, Paris, Librairie Félix Alcan, 1921
- **TEUSCHER Christof (sous la direction de)**, *Alan Turing : Life and Legacy of a great thinker*, Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2004
- **THALER Richard, SUNSTEIN Cass**, *Nudge - Improving Decisions about Health, Wealth and Happiness*, Penguin Books, 2012
- **THOREAU Henri-David**, *La Désobéissance Civile*, Culture Commune, 2014
- **THOREAU Henry-David**, *Walden ou la vie dans les bois*, Traduction de Louis Fabulet, Éditions Gallimard, Collection L'imaginaire, 1990
- **THOREL Jérôme**, *Attentifs ensemble – L'injonction au bonheur sécuritaire*, Éditions La découverte, Paris, 2013
- **TURK Alex**, *La vie privée en péril. Des citoyens sous contrôle*, Paris, Odile Jacob, 2011
- **TURNER Fred**, *Aux sources de l'utopie numérique - de la contre-culture à la cyberculture*, *Stewart Brand*, un homme d'influence, C&F éditions, décembre 2012
- **VADROT Claude-Marie**, *La grande surveillance - Caméras, ADN, portables, Internet...*, Collection L'Histoire immédiate, Editions du Seuil, 2007
- **VAINER Arkadi, VAINER Gueorgui**, Traduction Pierre Léon, *La corde et la pierre*, Collection Série Noire, Editions Gallimard, 2006
- **VAISSE Justin**, *Zbigniew Brzezinski - Stratège de l'empire*, Odile Jacob, 2016
- **VIAL Stéphane**, *L'être et l'écran – Comment le numérique change la perception*, préface de Pierre Lévy, PUF, Paris, 2013
- **VION - DURY Philippe**, *La nouvelle servitude volontaire - Enquête sur le projet politique de la Silicon Valley*, FYP Editions, 2016
- **VIVERET Patrick**, *Pourquoi ça ne va pas plus mal ?*, Collection Transversales, Fayard, 2005
- **VOLTAIRE**, *Candide ou l'optimisme*, Edition Libre, Bibebook, 2013
- **WEBER Max**, *Économie et société – 1. Les catégories de la sociologie*, Traduit de l'allemand par J. Freund (et al.), Éditeur Pocket, Collection Pocket Agora, 1995
- **WEBER Max**, *L'éthique protestante et l'esprit du capitalisme*, Traduction inédite et présentation par Isabelle Kalinowski, Éditions Flammarion, Collection Champs, 2000
- **WEBER Max**, *Le savant et le politique*, traduit par J. Freund, Collection Le Monde en 10-18, Paris : Union Générale d'Éditions, 1963
- **WEBER Max**, *Le savant et le politique*, traduit par Catherine Colliot- Thélène, La Découverte / Poche, 2003

- **WEIL Simone**, *L'enracinement : prélude à une déclaration des devoirs envers l'être humain*, Éditions Gallimard, Collection Folio Essais, 1990
- **WEIL Simone**, *Note sur la suppression générale des partis politiques*, Éditions Climats, 2006
- **WEIL Simone**, *La pesanteur et la grâce*, Éditions Pocket, Collection Classique, 1993
- **WEIL Simone**, *Réflexions sur les causes de la liberté et de l'oppression sociale*, Les Éditions Gallimard, Collection Idées, 1955
- **WERBER Bernard**, *Le papillon des étoiles*, Albin Michel, 2006
- **WIENER Norbert**, *Cybernétique et société : L'usage humain des êtres humains*, Collection Points Sciences, Points, 2014
- **WOLTON Dominique**, *Sauver la communication*, Collection Champs Essais, Editions Flammarion, 2005
- **ZAMIATINE Evgueni**, *Nous autres*, traduit du russe par B. Cauvet-Duhamel, Gallimard, Collection L'imaginaire, Paris, 1979

II. Les études doctrinales

A. Les thèses et mémoires

- **OCHOA Nicolas**, *Le droit des données personnelles, une police administrative spéciale*, Droit. Université Paris 1 Panthéon-Sorbonne, 2014. Français. HAL Id: tel-01340600, En ligne: <https://tel.archives-ouvertes.fr/tel-01340600/document> (dernière consultation: 5 mars 2018)
- **ROQUES-BONNET Marie-Charlotte**, *Le droit peut-il ignorer la révolution numérique ?*, Préface de Lucien Rapp, Ouvrage publié avec le concours de la CNIL, Michalon Editions, 2010

B. Les articles de doctrine

- **ATTOUR Amel, RALLET Alain**, « Le rôle des territoires dans le développement des systèmes trans-sectoriels d'innovation locaux : le cas des smart cities », *Innovations*, 2014, Vol. 1, n°43, p. 253-279
- **AUBY Jean-Bernard**, « Espace public, espaces publics », *Droit administratif*, n°7, Juillet 2009
- **BADINTER Robert**, *Vers un monde plus sûr*, *Politique étrangère* 3/2005 (Automne) , p. 481-493, En ligne: www.cairn.info/revue-politique-etrangere-2005-3-page-481.htm (dernière consultation: 5 mars 2018)
- **BATTELIER Pierre**, *Acceptabilité sociale, cartographie d'une notion et de ses usages*, Cahier de recherches, 2015, UQAM: les publications du Centr'ERE, En ligne: <http://www.espace->

- ressources.uqam.ca/images/Documents/Recherche/Rapports_recherche/Batellier-2015-Acceptabilite-sociale.pdf (dernière consultation: 5 mars 2018)
- **BAUSARDO Thomas**, « Quel passé pour Prism et Snowden ? », *Vacarme* 2014/1 (n°66), p. 142 - 157, En ligne: <https://www.cairn.info/revue-vacarme-2014-1-page-142.htm> (dernière consultation: 5 mars 2018)
 - **BELLEAU André**, *Wiener, Mc. Luhan et la montée des automates*, Liberté, vol. 9, n° 5, (53), p. 38-50, En ligne: <https://www.erudit.org/culture/liberte1026896/liberte1027672/29597ac.pdf> (dernière consultation: 5 mars 2018)
 - **BLANC Maurice, CAUSER Jean-Yves**, « Privé - Public: quelles frontières ? », *Revue des sciences sociales*, En ligne: <http://www.revue-des-sciences-sociales.com/pdf/rss33-presentation.pdf> (dernière consultation: 5 mars 2018)
 - **BOUILLOUD Jean-Philippe**, « Du monde de la parole au règne du visible » p. 72 - 73, in. AUBERT Nicole, HAROCHE Claudine (sous la direction de), *Les tyrannies de la visibilité - Etre visible pour exister?*, Editions Eres, Collection Sociologie clinique, 2011, pp. 55 - 76.
 - **BOURDEAU Vincent, JARRIGE François, VINCENT Julien**, *Le passé d'une désillusion : les luddites et la critique de la machine*, Actuel Marx 1/2006 (n° 39) , p. 145-165, En ligne: <http://www.cairn.info/revue-actuel-marx-2006-1-page-145.htm> (dernière consultation: 5 mars 2018)
 - **BROUSSEAU Eric, CURIEN Nicolas**, *Introduction: Economie d'Internet, Economie du numérique*, Revue économique, Numéros Hors-série 2001, Economie de l'Internet, pp. 7 - 36, En ligne: http://www.persee.fr/docAsPDF/reco_0035-2764_2001_hos_52_1_410273.pdf (dernière consultation: 5 mars 2018)
 - **BRUNET Pierre**, *Le réalisme n'est-il qu'une théorie de l'interprétation?*, *Réalisme, interprétation, transgression*, 2012, France. Larcier, pp.397-414, 2013, En ligne: <https://halshs.archives-ouvertes.fr/halshs-00840601/document> (dernière consultation: 5 mars 2018)
 - **CAILLAUD Pascal**, « L'action juridique des institutions internationales sur le « travail décent » et la « qualité de l'emploi »: une définition par indicateurs du bien-être du travailleur ? », in. FLORIN Agnès, PREAU Marie, *Le bien-être*, L'Harmattan, 2013, pp. 35 - 59
 - **CANTEGREIL Julien**, « La doctrine américaine de « l'ennemi combattant illégal » », in DELMAS – MARTY Mireille, HALPERIN Jean - Louis et GIUDICELLI – DELAGE Geneviève (dir.), *Les politiques sécuritaires à la lumière de la doctrine pénale du 19ème au 21ème siècle*, RSC 2010. 81, 15 mars 2010
 - **CASILLI Antonio**, « Contre l'hypothèse de la « fin de la vie privée » - la négociation de la privacy dans les médias sociaux » *Revue française des sciences de l'information et de la*

- communication*, En ligne: <http://journals.openedition.org/rfsic/630> (dernière consultation: 5 mars 2018)
- **CATALA Pierre**, *Ebauche d'une théorie juridique de l'information*, Revue de droit prospectif 1983, no 1, p. 185, D. 1984, chr., p. 97
 - **CHARBONNEAU Alexandre**, « La référence au bien-être des gens de mer: entre institutionnalisation d'un service social et approche qualitative des conditions de vie et de travail à bord des navires », in. FLORIN Agnès, PREAU Marie, *Le bien-être*, L'Harmattan, 2013, pp. 117 - 132
 - **CHAUMETTE Patrick**, « La notion de bien-être en droit social. Une notion pleine d'avenir », in. FLORIN Agnès, PREAU Marie, *Le bien-être*, L'Harmattan, 2013, pp. 193 - 209
 - **CHOFFEL Denis, ALDRIN Jérémy**, « Réflexions autour de la notion « d'accountability » à travers l'application d'une grille d'analyse sur deux études de terrain en management public », *Gestion et management public*, 2015/3 (Volume 4 / N°1), p. 45 - 58, En ligne: <https://www.cairn.info/revue-gestion-et-management-public-2015-3-page-45.htm> (dernière consultation: 5 mars 2018)
 - **CHOQUET Olivier**, *L'automobile, un bien banalisé*. In. Economie et statistique n° 154, Avril 1983. *Les 39 heures / les salaires en 1982 / L'automobile, un bien banalisé*. P. 47 - 55; En ligne: http://www.persee.fr/doc/estat_0336-1454_1983_num_154_1_4741 (dernière consultation: 5 mars 2018)
 - **CRARY Jonathan**, « Le capitalisme comme crise permanente de l'attention, in. CITTON Yves (sous la direction de), *L'économie de l'attention - Nouvel horizon du capitalisme ?*, Editions La Découverte, Paris, 2014, pp. 35 - 54
 - **DANET Jean**, *La dangerosité, une notion criminologique, séculaire et mutante*, Champ pénal/ Penal field [En ligne], Vol. V | 2008, mis en ligne le 07 octobre 2008, URL : <http://champpenal.revues.org/6013> (dernière consultation: 5 mars 2018)
 - **DEDESSUS - LE - MOUSTIER Nathalie**, « Bien-être et droit du travail », in. FLORIN Agnès, PREAU Marie, *Le bien-être*, L'Harmattan, 2013, pp. 211 - 225
 - **DELAGE Pierre-Jérôme**, *Vérité et ambiguïté autour de l'imputabilité morale*, RSC, 2009, p. 69 – 74
 - **DELEUZE Gilles**, « Post-scriptum sur les sociétés de contrôle », in. *L'autre journal* n° 1, mai 1990
 - **DINUR Irit, NISSIM Koby**, *Revealing Information hile preserving Privacy*, 21 Décembre 2004, Université de Harvard, En ligne: <http://citeseerx.ist.psu.edu/viewdoc/download?>

[doi=10.1.1.101.1298&rep=rep1&type=pdf](#) (dernière consultation: 5 mars 2018)

- **DWORK** Cynthia, **ROTH** Aaron, « The Algorithmic Foundations of Differential Privacy ». Foundations and Trends, *Theoretical Computer Science*, Vol. 9; N° 3-4, pp. 211 -407, 2014, En ligne: <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf> (dernière consultation: 5 mars 2018)
- **FRANCK** Georg, « Economie de l'attention », in. CITTON Yves (sous la direction de), *L'économie de l'attention - Nouvel horizon du capitalisme ?*, Editions La Découverte, Paris, 2014, pp. 55 - 72
- **FRAYSSINET** Jean, « L'utilité et les fonctions d'une formulation d'objectifs : l'exemple de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés », *Revue de la Recherche Juridique*, n°4, 1989, pp. 903-918
- **FRAYSSINET** Jean, « Trente ans après la loi Informatique et libertés se cherche encore », *Lamy Droit de l'immatériel*, dossier spécial « les trente ans de la loi Informatique et libertés », n°34, janvier 2008, pp. 69-73
- **FROMONT** Michel, Analyse de l'arrêt de la Cour constitutionnelle fédérale allemande du 16 février 1983, *BVerfGE*, tome 62, p. 1, *Revue de Droit public* 1983, p. 954
- **GAILLARD** Isabelle, *De l'étrange lucarne à la télévision - Histoire d'une banalisation (1949 - 1984)*, Vingtième siècle. Revue d'histoire 2006/3 n°91, p. 9-23, En ligne: <http://www.cairn.info/revue-vingtieme-siecle-revue-d-histoire-2006-3-page-9.htm>
- **GALIC** Masa, **TIMAN** Tjerk, **KOOPS** Bert-Jaap, *Bentham, Deleuze and beyond: an overview of surveillance Theories from the Panopticon to Participation*, Mai 2016, Tilburg Institute for Law, Technology and Society
- **GALLOUX** Jean-Christophe, *Ebauche d'une définition juridique de l'information*, Recueil Dalloz, 1994, p. 229
- **GASNIER** Arnaud, *De nouveaux espaces publics urbains ? Entre privatisation des lieux publics et publicisation des lieux privés*, *Revue Urbanisme*, Publications d'architecture et d'urbanisme, 2006, pp. 70 - 73
- **GAUTIER** Pierre-Yves, **LINANT DE BELLEFONDS** Xavier, *De l'écrit électronique et des signatures qui s'y attachent*, JCP éd. G 2000, I, n°236, v. n°31 ; *Loché*, t. XII, p.505
- **GAY** Laurence, *La notion de « droits-créances » à l'épreuve du contrôle de constitutionnalité*, *Cahiers du Conseil Constitutionnel* n° 16, juin 2004, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/nouveaux-cahiers-du-conseil/cahier-n-16/la-notion-de-droits-creances-a-l-epreuve-du-contrôle-de-constitutionnalite.51982.html> (dernière

consultation: 5 mars 2018)

- **GENTOT Michel**, *La protection des données personnelles à la croisée des chemins*, in, Académie des Sciences Morales et Politiques (ASMP), Groupe de travail société d'information et vie privée coordonné par M. Pierre Tabatoni, *La protection de la vie privée dans la société d'information*, Tome 3, 1^{er} janvier 2002, En ligne: <http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr1.pdf> (dernière consultation: 5 mars 2018)
- **GOMART Thomas**, « De la diplomatie numérique », *La vie numérique*, Revue des deux mondes, janvier 2013, pp. 131 - 141, En ligne: https://www.ifri.org/sites/default/files/atoms/files/ifri_gomart_10-01-2013_revuedesdeuxmondes_diplomatie_numerique.pdf (dernière consultation: 5 mars 2018)
- **HUNYADI Mark**, « La logique du raisonnement de précaution », *Revue européenne des sciences sociales*, XLII-130|2004, En ligne: <http://ress.revues.org/341> (dernière consultation: 5 mars 2018)
- **JAKOBS Günther**, *Aux limites de l'orientation par le droit : le droit pénal de l'ennemi*, in RSC, 2009/, n°1
- **JAMIN Christophe**, *Le rendez-vous manqué des civilistes français avec le réalisme juridique : un exercice de lecture comparée*, Disponible en ligne à l'adresse suivante: <https://spire.sciencespo.fr/hdl:/2441/6ggbvnr6munghes9oc0gmell16/resources/jamin-realisme-juridique.pdf> (dernière consultation: 5 mars 2018)
- **JUIGNET Patrick**, « Les paradigmes scientifiques selon Thomas Kuhn », *Philosophie, science et société [en ligne]*, 2015, <https://philosciences.com/Pss/philosophie-et-science/methode-scientifique-paradigme-scientifique/113-paradigme-scientifique-thomas-kuhn> (dernière consultation: 5 mars 2018)
- **KAHANE Guy, EVERETT Jim, EARP Brian, FARIAS Miguel, SAVULESCU Julian**, *Utilitarian judgments in sacrificial moral dilemmas reflect impartial concern for the greater good*, Cognition, 13 novembre 2014, Disponible en ligne à l'adresse suivante: http://ac.els-cdn.com/S0010027714002054/1-s2.0-S0010027714002054-main.pdf?_tid=5e56ce28-5ccd-11e7-9566-00000aacb35e&acdnat=1498742458_c7b59ce690a17e62a9117c5e4c3f8caf (dernière consultation: 5 mars 2018)
- **KITCHIN Rob**, *The real-time city? Big data and smart urbanism*, *GeoJournal*, 2014, 79:1 - 14, p. 1, Disponible en ligne à l'adresse suivante: <https://pdfs.semanticscholar.org/6e73/7a0e5ef29303760a565ba5e9d98510ab0976.pdf> (dernière consultation: 5 mars 2018)
- **KYROU Ariel**, « L'hypnose de l'à-venir. ou des fables de science-fiction comme moyen de déjouer les pièges de la sousveillance », *Multitudes* 2010/1 (n°40), p. 114 à 125

- **LAGET Marc**, *Le numérique, simple mue du libéralisme ou avènement d'une économie soutenable*, Netcom, 22 - 3/4, 2008, En ligne: <https://netcom.revues.org/1618> (dernière consultation: 5 mars 2018)
- **LALANDE Sophie**, *L'adresse IP de votre ordinateur: une donnée personnelle relevant du régime de protection communautaire?*, Droit-NTIC, 2003, En ligne: http://www.droit-tic.com/pdf/adr_ip.pdf (dernière consultation: 5 mars 2018)
- **LARRIERE Stéphane**, « Uberisation du droit... et ainsi naquit le juriste digital », *Les Affiches Parisiennes*, 15 avril 2016, Disponible en ligne à l'adresse suivante: <http://www.affiches-parisiennes.com/uberisation-du-droit-et-ainsi-naquit-le-juriste-digital-6177.html> (dernière consultation: 5 mars 2018)
- **LAVAL Christian**, « Surveiller et prévenir. la nouvelle société panoptique », *Revue du Mauss* 2012/2 (n°40), p. 47-72, En ligne: <https://www.cairn.info/revue-du-mauss-2012-2-page-47.htm#re5no29> (dernière consultation: 5 mars 2018)
- **LAVENUE Jean-Jacques**, **BAUDEN-HAMEREL Gaylord**, **DESRUMEAUX Nicolas**, **CODRON Clémence**, « Privacy by design ou privacy by law? », *Revue Droit International, Commerce, Innovation et Développement (DICID)*, n° 2/2012, novembre 2012, Presses de l'Université de Bourgogne, pp. 77 - 104, En ligne: <http://credimi.u-bourgogne.fr/images/stories/pdf/dicid%202-4.pdf> (dernière consultation: 5 mars 2018)
- **LAVENUE Jean-Jacques**, « La privacy by design, panacée ou cheval de Troie ? », *Revue de la Recherche Juridique - Droit Prospectif*, 2013 - 1, pp. 59 - 73
- **LAVENUE Jean-Jacques**, « Gouvernance des données et naissance du « monstre doux » », in. BOUHADANA Irène, Gilles William (sous la direction de), *Droit et gouvernance des données publiques et privées à l'heure du numérique*, Les Editions Imodev, Février 2015, pp. 33 - 55
- **LECLERCQ Pierre**, « Un an d'application de la législation Informatique et Libertés », *Communication, Commerce électronique*, Octobre 2007
- **LE FICHANT Françoise**, « Le bien-être du voisin », in. FLORIN Agnès, PREAU Marie, *Le bien-être*, L'Harmattan, 2013, pp. 229 - 241
- **LE GOFF Tanguy** et **HEILMANN Eric**, *Vidéosurveillance: un rapport qui ne prouve rien*, En ligne: <https://www.laurent-mucchielli.org/public/Videosurveillance.pdf> (dernière consultation: 5 mars 2018)
- **LE TEXIER Thibault**, « Éric Sadin et le coup d'État technologique permanent », *Quaderni*, 86, Hiver 2014-2015, En ligne: <http://quaderni.revues.org/868> (dernière consultation: 5 mars 2018)
- **MACHLUP Fritz**, « Economie des connaissances et de l'information », in. Réseaux, volume 11,

- n°58, 1993, *L'information scientifique et technique*, pp.109 - 129, En ligne: http://www.persee.fr/docAsPDF/reso_0751-7971_1993_num_11_58_2308.pdf (dernière consultation: 5 mars 2018)
- **MARTINEAU-BOURGNINAUD Véronique**, « Le bien-être dans l'entreprise », in. FLORIN Agnès, PREAU Marie, *Le bien-être*, L'Harmattan, 2013, pp. 179 - 192
 - **MARX Gary**, « The Surveillance Society: The Threat of 1984-Style Techniques », *Futurist*, Juin 1985, n° 19, pp. 21 - 26
 - **MAZABRAUD Bertrand**, « Foucault, le droit et les dispositifs de pouvoir », *Cités* 2010/2 (n° 42), pp. 127-189, En ligne: <https://www.cairn.info/revue-cites-2010-2-page-127.htm> (dernière consultation: 5 mars 2018)
 - **MERCIER Silvère**, « Biens communs et données personnelles: il nous faut inventer », 12 mars 2014, En ligne: <http://www.bibliobsession.net/2014/03/12/biens-communs-et-donnees-personnelles-il-nous-faut-inventer/> (dernière consultation: 5 mars 2018)
 - **MULONE Massimiliano**, « La marchandisation de la sécurité : facteur de responsabilisation des individus ou des entreprises? », *Déviance et Société*, 2012/3, Vol. 36, p325 - 338, p. 325, En ligne: <http://www.cairn.info/revue-deviance-et-societe-2012-3-page-325.htm> (dernière consultation: 5 mars 2018)
 - **NEYRAT Frédéric**, « Avant propos sur les sociétés de clairvoyance. « Le progrès consiste à être poussé en avant par la police » (Chesterton), *Multitudes* 2010/1 (n°40), p. 104-111
 - **NYE Joseph, OWENS William**, « America's Information edge », in *Foreign Affairs*, Mars 1996, pp20-36, p20 et p. 35, En ligne: <http://www.unz.org/Pub/ForeignAffairs-1996mar> (dernière consultation: 5 mars 2018)
 - **NYE Joseph, KEOHANE Robert**, « Power and Interdependence in the Information Age », *Foreign Affairs*, vol. 77, n°5, pp. 81-94, En ligne: <https://fr.scribd.com/document/305854708/56826563-Power-and-Interdependence-in-the-Information-Age-pdf> (dernière consultation: 5 mars 2018)
 - **OCQUETEAU Frédéric**, « Les nouveaux besoins de protection », *Texte de la 157ème conférence de l'Université de tous les savoirs donnée le 5 juin 2000*, in. UNIVERSITE DE TOUS LES SAVOIRS, *Le Pouvoir, l'Etat, la Politique*, Volume 9, Odile Jacob, Mars 2002
 - **O'REILLY Tim**, « Open Data and Algorithmic Regulation », in. GOLDSTEIN Brett, DYSON Lauren (éds.), *Beyond Transparency - Open Data and the Future Civic Innovation*, Code for America Press, San Francisco, 2013, pp. 289 - 300, En ligne: <http://beyondtransparency.org/pdf/BeyondTransparency.pdf> (dernière consultation: 5 mars 2018)
 - **ORSI Fabienne**, « Elinor Ostrom et les faisceaux de droits : l'ouverture d'un nouvel espace pour

- penser la propriété commune », *Revue de la régulation*, 14 | 2e semestre / Autumn 2013, En ligne: <http://journals.openedition.org/regulation/10471> (dernière consultation: 5 mars 2018)
- **PELISSE Jérôme**, « Juridicisation ou judiciarisation : usages et réappropriations du droit dans les conflits du travail », *Politix* 2/2009 (n° 86) , p. 73-96, En ligne: www.cairn.info/revue-politix-2009-2-page-73.htm (dernière consultation: 5 mars 2018)
 - **PEUGEOT Valérie**, « Données personnelles: sortir des injonctions contradictoires », *VECAM*, 13 avril 2014, En ligne: <https://vecam.org/Donnees-personnelles-sortir-des-injonctions-contradictoires> (dernière consultation: 5 mars 2018)
 - **PHARABOD Anne-Sylvie, NIKOLSKI Véra, GRANJON Fabien**, « La mise en chiffres de soi. Une approche compréhensive des mesures personnelles », *Réseaux*, 2013/1 (n° 177), p. 97-129, En ligne: <https://www.cairn.info/revue-reseaux-2013-1-page-97.htm> (dernière consultation: 5 mars 2018)
 - **POKEMPNER Dinah**, « Le droit dont l'heure est (re) venue - Le respect de la vie privée à l'ère de la surveillance », in. *Human Rights Watch Rapport annuel 2014*, En ligne: https://www.hrw.org/sites/default/files/related_material/privacy_fr.pdf (dernière consultation: 5 mars 2018)
 - **POTTE-BONNEVILLE Mathieu**, « Surveillance, contrôle, gouvernement : l'ADN du contemporain. De l'actualité de la pensée de Michel Foucault au travers de l'exemple polémique des « tests génétiques » », *Multitudes* 2010/1 (n° 40), p. 68-76
 - **PRADEL Jean**, *Nature et application dans le temps des mesures créées par la loi du 25 février 2008 à l'égard des criminels atteints d'un trouble mental*, Recueil Dalloz, 2010, p. 471
 - **PRADEL Jean**, « Une double révolution en droit pénal français avec la loi du 25 février 2008 sur les criminels dangereux », *Dalloz* 2008, p. 1000
 - **QUESSADA Dominique, SADIN Eric**, « Big Brother n'existe pas, il est partout. Discussion à partir du livre d'Éric Sadin, autour de la surveillance comme prisme d'observation des mutations de l'environnement contemporain », *Multitudes* 2010/1 (n° 40), p. 78-87
 - **RANGEON François**, « Droits - libertés et droits créances : les contradictions du préambule de 1946 », *CURAPP*, En ligne: https://www.u-picardie.fr/curapp-revues/root/37/francois_rangeon.pdf_4a083159afa30/francois_rangeon.pdf (dernière consultation: 5 mars 2018)
 - **RAPOPORT Cécile**, « L'opposabilité des « droits-créances » constitutionnels en droit public français », *Communication présentée aux journées de l'association française de droit constitutionnel*, En ligne: <http://www.droitconstitutionnel.org/congresParis/comC8/RapportTXT.pdf> (dernière consultation: 5 mars 2018)

- **RAY Jean-Emmanuel**, « Le nouveau correspondant aux données personnelles », *Semaine sociale Lamy*, 27 septembre 2004, n° 1183
- **RIGAUX François**, « De la noosphère à la noopolitique. La mise en réseaux du savoir et du pouvoir », in *Liber amicorum Paul Maertens*, Bruxelles, Larcier, 2007, pp. 967-982, En ligne: <http://www.sfdi.org/wp-content/uploads/2014/08/RIGAUXnoos.pdf> (dernière consultation: 5 mars 2018)
- **RIGAUX François**, « L'individu, sujet ou objet de la société de l'information », *Groupe d'études Société de l'information et vie privée*, En ligne: <https://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr6.pdf> (dernière consultation: 5 mars 2018)
- **RIGOUSTE Mathieu**, « L'ennemi intérieur, de la guerre coloniale au contrôle sécuritaire », *Cultures & Conflits*, 67 | automne 2007, mis en ligne le 04 janvier 2010, En ligne: <http://conflits.revues.org/3128> (dernière consultation: 5 mars 2018)
- **RIVELINE Claude**, « Manifeste pour la désinformatisation de la société », *Pandore* n°17, Février 1982
- **ROUVROY Antoinette, BERNS Thomas**, « Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps « numériques »... », *Multitudes*, 2010 / 1, (n° 40), pp. 88 - 103, En ligne: <https://www.cairn.info/revue-multitudes-2010-1-page-88.htm> (dernière consultation: 5 mars 2018)
- **ROUVROY Antoinette, BERNS Thomas**, « Gouvernementalité algorithmique et perspectives d'émancipation », *Réseaux*, 2013/1, n° 177, pp. 163 - 196, p. 173, En ligne: <https://www.cairn.info/revue-reseaux-2013-1-page-163.htm> (dernière consultation: 5 mars 2018)
- **ROUVROY Antoinette**, « Pour une défense de l'éprouvante inopérationnalité du droit face à l'opérationnalité sans épreuve du comportementalisme numérique », *Dissensus*, Avril 2011, n° 4, pp. 127 - 149, En ligne: <https://popups.uliege.be/2031-4981/index.php?id=1269&file=1&pid=963> (dernière consultation: 5 mars 2018)
- **RUMPALA Yannick**, « Gouverner en pensant systématiquement aux conséquences ? Les implications institutionnelles de l'objectif de « développement durable » », *VertigO - la revue électronique en sciences de l'environnement*, Volume 10, numéro 1, avril 2010, En ligne: <http://journals.openedition.org/vertigo/9468#toc> (dernière consultation: 5 mars 2018)
- **SADIN Eric**, « Le nouveau paradigme de la surveillance. Cerner l'humain par l'entrelacs du marketing et de la sécurité », *Multitudes*, 2010/1 (n°40), p. 60 - 66, En ligne: <https://www.cairn.info/revue-multitudes-2010-1-page-60.htm> (dernière consultation: 5 mars 2018)
- **SHANNON Claude Elwood**, « A mathematical theory of communication », *The Bell System*

- Technical Journal*, Vol. 27, pp. 379-423, 623-656, July, October, 1948, Université de Harvard, En ligne: <http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf> (dernière consultation: 5 mars 2018)
- **SIMON Bart**, « The return of Panopticism: Supervision, Subjection and the New surveillance », *Surveillance & Society*, 3 (1): 1-20, En ligne: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3317/3279> (dernière consultation: 5 mars 2018)
 - **SIMON Herbert**, « Designing organizations for an information-rich world », in. GREENBERGER Martin, *Computers, communications, and the public interest*, Baltimore, MD, The John Hopkins Press, 1971, En ligne: <http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=33748> (dernière consultation: 5 mars 2018)
 - **TARDIEU Claire**, « Corriger ou évaluer ? », *Cahiers de l'APLIUT*, Vol. XXVIII N° 3 | 2009, En ligne: <http://journals.openedition.org/apliut/65> (dernière consultation: 5 mars 2018)
 - **TEILHARD DE CHARDIN Pierre**, « Une interprétation biologique plausible de l'histoire humaine: la formation de la Noosphère », *Revue des questions scientifiques*, Louvain, janvier 1947
 - **TOSEL André**, « Libres réflexions à partir de Hannah Arendt - Superfluité humaine et conformisme de l'insujet », in. CALLOZ-TSCHOPP Marie-Claire (dir.), *Lire Hannah Arendt aujourd'hui - Pouvoir, guerre, pensée, jugement, politique*, Actes du colloque international de Lausanne 11 - 12 mai 2007, Université de Lausanne, Institut d'Etudes Politiques Internationales, L'Harmattan, 2008, Paris, pp. 81 - 96
 - **TREMBLAY Gaëtan**, « De Marshall Mc Luhan à Harold Innis ou du village global à l'empire mondial », *TIC & société*, vol. 1, n°1, 2007, En ligne: <http://ticetsociete.revues.org/222> (dernière consultation: 5 mars 2018)
 - **VAN ZONEN Liesbet**, « Privacy concerns in smart cities », *Government Information Quarterly*, 2016, En ligne: <http://www.sciencedirect.com/science/article/pii/S0740624X16300818> (dernière consultation: 5 mars 2018)
 - **WARREN Samuel, BRANDEIS Louis**, « The Right to Privacy », *Harvard Law Review*, vol. 4, no. 5, 15 décembre 1890, pp. 193 - 220, En ligne: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> (dernière consultation: 5 mars 2018)
 - **WYVEKENS Anne**, « La sécurité urbaine, affaire d'Etat ou problème local ? », *Métropolitiques*, 2012, p. 2, <https://halshs.archives-ouvertes.fr/halshs-00673473/document> (dernière consultation: 5 mars 2018)

C. Les numéros spéciaux

- **BOISSONADE Jérôme (sous la direction de)**, « Mettre à l'épreuve l'acceptabilité sociale », *Vertigo*, Volume 15 numéro 3, décembre 2015, disponible en ligne à l'adresse suivante: <https://vertigo.revues.org/16679> (dernière consultation: 5 mars 2018)
- **TURK Alex, FRAYSSINET Jean, NAFTALSKI Fabrice, FOREST David, PERRAY Romain, JOB Jean- Marie**, Dossier Spécial Loi « informatique et libertés », *Lamy Droit de l'Immatériel*, n° 34, Janvier 2008, pp. 67 - 94
- *Multitudes* 2010 / 1, n° 40, « Du contrôle à la sousveillance », pp. 51 à 138, disponible en ligne à l'adresse suivante: <https://www.cairn.info/revue-multitudes-2010-1.htm> (dernière consultation: 5 mars 2018)
- *Revue de Science Criminelle et de droit comparé, Droit pénal de l'ennemi et droit pénal de l'inhumain*, RSC n°1/2009, p. 3 à p. 68

III. Les actes de colloques

- **BOURDIEU Pierre, BOLTANSKI Luc**, « La production de l'idéologie dominante », in. *Actes de la recherche en sciences sociales*, 1976, Volume 2, numéro pp 3 - 73, En ligne: http://www.persee.fr/docAsPDF/arss_0335-5322_1976_num_2_2_3443.pdf (dernière consultation: 5 mars 2018)
- **DELEUZE Gilles**, *Qu'est ce que l'acte de création ?*, Conférence donnée dans le cadre des mardis de la fondation Femis, 17 mai 1987, En ligne: <https://www.webdeleuze.com/textes/134> (dernière consultation: 5 mars 2018)
- **GARDNER Howard, DAVIS Katie**, *The App Generation - How today's Youth navigate identity, intimacy, and imagination in a digital world*, intervention du 21 octobre 2013 à la Harvard Graduate School of Education, Askwith Forum, En ligne: <http://theappgenerationbook.com> (dernière consultation: 5 mars 2018)
- **JERPHAGNON Lucien**, *Plotin, ou l'anti-Narcisse*, In: *Platonisme et néoplatonisme. Antiquité et temps modernes*. Actes du 1er colloque de la Villa Kérylos à Beaulieu-sur-Mer du 27 au 30 septembre 1990. Paris : Académie des Inscriptions et Belles- Lettres, 1991. pp. 46-50. (Cahiers de la Villa Kérylos, 1); Disponible en ligne à l'adresse suivante: http://www.persee.fr/docAsPDF/keryl_1275-6229_1991_act_1_1_864.pdf (dernière consultation: 5 mars 2018)
- **LAVAL Christian**, *Foucault, la surveillance et nous*, Séminaire du Sophiapol: « Politiques de Foucault », 15 mars 2014, En ligne: <http://questionmarx.typepad.fr/files/foucault-la-surveillance->

[et-nous.pdf](#) (dernière consultation: 5 mars 2018)

- **SUDRE Frédéric**, « Rapport introductif : la « construction » par le juge européen du droit au respect de la vie familiale », SUDRE Frédéric (dir.), *Le droit au respect de la vie familiale au sens de la Convention européenne des droits de l'Homme : actes du colloque des 22 et 23 mars 2002 organisé par l'Institut de droit européen des droits de l'Homme (UMR-CNRS 5415), Faculté de droit de l'Université Montpellier I*, Bruylant : Nemesis, Bruxelles, 2005
- **TETU Jean-Francois**, *Identité, culture et communication*, Congrès franco-mexicain SFSIC et AMIC, 2002, Mexico, Mexique, Disponible en ligne à l'adresse suivante: <https://hal.archives-ouvertes.fr/halshs-00396403/document> (dernière consultation: 5 mars 2018)
- **WEYEMBERGH Maurice**, *J. Ellul et M. Heidegger. Le prophète et le penseur*, in. TROUDE-CHASTENET Patrick (sous la direction de.), *Sur Jacques Ellul – un penseur de notre temps*, Éditions L'esprit du temps, Collection Philosophie, 1994

IV. Les textes juridiques

A. Les textes juridiques internationaux et communautaires

1. Les textes internationaux

- **Charte des Nations Unies (et Statut de la Cour Internationale de Justice)**, signée à San Francisco le 26 juin 1945 suite à la Conférence des Nations Unies pour l'Organisation Internationale, entrée en vigueur le 24 octobre 1945, En ligne: <http://www.un.org/fr/sections/un-charter/introductory-note/index.html> (dernière consultation: 5 mars 2018)
- **Convention créant une Organisation des Nations Unies pour l'éducation, la science et la culture (acte constitutif de l'UNESCO)**, Adoptée à Londres le 16 novembre 1945 et modifiée par la Conférence générale lors de ses 2e, 3e, 4e, 5e, 6e, 7e, 8e, 9e, 10e, 12e, 15e, 17e, 19e, 20e, 21e, 24e, 25e, 26e, 27e, 28e, 29e et 31e sessions, in. UNESCO, Textes fondamentaux, Editions 2004 comprenant les textes et amendements adoptés par la Conférence générale lors de sa 32 ème session (Paris, 2003), UNESCO, Paris, 2004, En ligne: <http://unesdoc.unesco.org/images/0013/001337/133729f.pdf#page=7> (dernière consultation: 5 mars 2018)
- **Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales**, Conseil de l'Europe, 4 novembre 1950, En ligne: http://www.echr.coe.int/documents/convention_fra.pdf (dernière consultation: 5 mars 2018)
- **Convention STE n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel**, Strasbourg, 28 janvier 1981, En ligne: <http://>

www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108 (dernière consultation: 5 mars 2018)

- **Programme des Nations Unies pour l'environnement**, Secrétariat de l'ozone, *Convention de Vienne pour la protection de la couche d'ozone*, 22 mars 1985, En ligne: https://www.diplomatie.gouv.fr/sites/odyssee-developpement-durable/files/4/Convention_Vienne_1985.pdf (dernière consultation: 5 mars 2018)
- **The Holden Agreement, encore nommé The Travis-Wenger Arrangement – Memorandum for Op-20**, Collaboration of US and British radio intelligence organizations on Japanese and German projects, 1^{er} octobre 1942, En ligne: https://www.marinersmuseum.org/sites/micro/battle_of_the_atlantic/travis_wenger.pdf (dernière consultation: 5 mars 2018)
- **The British-U.S. Communications Intelligence Agreement (B.R.U.S.A.)**, 17 Mai 1943, En ligne: <http://discovery.nationalarchives.gov.uk/details/r/C11536914> (dernière consultation: 5 mars 2018)
- **The United Kingdom – United States Communications Intelligence Agreement (U.K.U.S.A.)**, 5 Mars 1946, En ligne: <http://discovery.nationalarchives.gov.uk/details/r/C11536921> (dernière consultation: 5 mars 2018)
- **United Nations, A/CONF.32/41, Final Act of the International Conference on Human Rights – Teheran, 22 April to 13 May 1968**, United Nations Publication, New York 1968, En ligne: http://legal.un.org/avl/pdf/ha/fatchr/Final_Act_of_TehranConf.pdf (dernière consultation: 5 mars 2018)

2. Les textes communautaires

a. Le traité communautaire

- **Acte unique européen des 17 et 28 février 1986**, JOCE, 29 juin 1987, n°L169
- **Charte des Droits Fondamentaux de l'Union européenne**, 2000/C 364/01, JOCE du 18 décembre 2000, En ligne: http://www.europarl.europa.eu/charter/pdf/text_fr.pdf (dernière consultation: 5 mars 2018)
- **Traité instituant la Communauté européenne** (version consolidée) du 25 mars 1957, JOCE, n°C325, 24 décembre 2002
- **Traité d'Amsterdam modifiant le traité sur l'Union Européenne**, les traités instituant les Communautés Européennes et certains actes connexes, JOCE C 340 du 10 novembre 1997

b. Les règlements communautaires

- **Règlement (CE) n° 820/97 du Conseil du 21 avril 1997 établissant un système d'identification**

et d'enregistrement des bovins et relatif à l'étiquetage de la viande bovine et des produits à base de viande bovine, JOCE 7 mai 1997, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31997R0820&from=FR> (dernière consultation: 5 mars 2018)

- **Règlement (CE) n°1760/2000 du Parlement européen et du Conseil du 17 juillet 2000 établissant un système d'identification et d'enregistrement des bovins et concernant l'étiquetage de la viande bovine et des produits à base de viande bovine et abrogeant le règlement (CE) n° 820/97 du Conseil**, JOCE 11 août 2000, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32000R1760&from=FR> (dernière consultation: 5 mars 2018)
- **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)**, JOUE L 119 du 4 Mai 2016, P;1 - 88, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR> (dernière consultation: 5 mars 2018)

c. Les directives communautaires

- **Directive 90/388/CEE de la Commission du 28 juin 1990, relative à la concurrence dans les marchés des services de télécommunication**, Journal officiel n° L 192 du 24/07/1990 p. 0010 - 0016, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31990L0388> (dernière consultation: 5 mars 2018)
- **Directive 90/387/CEE du Conseil du 28 juin 1990, relative à l'établissement du marché intérieur des services de télécommunication par la mise en oeuvre de la fourniture d'un réseau ouvert de télécommunications**, Journal officiel n° L 192 du 24/07/1990 p. 0001 - 0009, En ligne <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31990L0387&from=FR> (dernière consultation: 5 mars 2018)
- **Directive 93/13/CEE du Conseil du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs**, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31993L0013&from=FR> (dernière consultation: 5 mars 2018)
- **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**, Journal officiel n° L 281 du 23 novembre 1995, p. 0031 - 0050, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046> (dernière consultation: 5 mars 2018)

- **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 »)*, Journal officiel n° L 178 du 17 juillet 2000, p. 0001 – 0016, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2000:178:TOC> (dernière consultation: 5 mars 2018)
- **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*, Journal officiel n° L167 du 22 juin 2001, p. 0010 – 0019, En ligne: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2001.167.01.0010.01.FRA&toc=OJ:L:2001:167:TOC (dernière consultation: 5 mars 2018)
- **Directive 2002/58/CE du Parlement européen et du conseil du 12 juillet 2002**, *concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, JOCE L 201/37 du 31 juillet 2002, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0058&from=FR> (dernière consultation: 5 mars 2018)
- **Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006**, *sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication modifiant la directive 2002/58/CE*, JOUE L 105/54 du 13 avril 2006, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32006L0024&from=FR> (dernière consultation: 5 mars 2018)
- **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 de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision - cadre 2008/977/JAI du Conseil*, JOUE L 119 du 4 Mai 2016, p. 89 - 131, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0680&from=FR> (dernière consultation: 5 mars 2018)
- **Directive (UE) 2016/1148 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*, JOUE du 19 juillet 2016, L 194, p. 1 -30, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=FR> (dernière consultation: 5 mars 2018)

d. Les décisions d'exécution

- **Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis**, JOUE L207/1, du 1^{er} août 2016, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016D1250&from=EN> (dernière consultation: 5 mars 2018)

3. Les textes d'autres pays

a. L'Allemagne

- **Hessische Datenschutzgesetz** vom 7 Oktober 1970 GVB1. II 300-10, publié à Wiesbaden, 12 octobre 1970, (loi sur la protection des données du Land de Hesse du 7 Octobre 1970), Gesetz und Verordnungsblatt für das Land Hessen, Part I, n°41
- **Gesetz zum schutz vor Missbrauch personenbezogener daten bei der datenverarbeitung**, vom 21 Januar 1977, in der Fassung der Bekanntmachung vom 1. Februar 1977 (BGBl. I Nr. 7 S. 201). In Kraft ab 1. Januar 1978. (loi visant à protéger les données personnelles contre l'utilisation abusive de ces dernières dans les traitements de données du 27 janvier 1977, dans la version publiée du 1^{er} février 1977 (BGBl. I n°7, p. 201), en vigueur à partir du 1^{er} janvier 1978), et En ligne: https://www.datenschutz-wiki.de/BDSG_1977 (dernière consultation: 5 mars 2018)

b. Les États-Unis

- **Federal-Aid Highway Act**, Public Law 627, 29 Juin 1956, En ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-70/pdf/STATUTE-70-Pg374.pdf> (dernière consultation: 5 mars 2018)
- **Foreign Intelligence surveillance Act (FISA)**, 1978
- **FISA Reform Act of 2005**, S. 1469, 114th Congress, 1st Session, 23 mai 2015, En ligne: <https://www.gpo.gov/fdsys/pkg/BILLS-114s1469is/pdf/BILLS-114s1469is.pdf> (dernière consultation: 5 mars 2018)
- **High-Performance Computing Act of 1991**, 15 USC 5501, Public Law 102-194, 9 décembre 1991, En ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-105/pdf/STATUTE-105-Pg1594.pdf> (dernière consultation: 5 mars 2018)
- **Telecommunications Act of 1996**, Intergovernmental relations, 47 USC 609 note, Public Law 104-104 - 8 février 1996, En ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-110/pdf/STATUTE-110-Pg56.pdf> (dernière consultation: 5 mars 2018)

- **The Privacy Act of 1974**, S.3418, Public Law 93-579, *An act to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.* December 31, 1974 ; version initiale en ligne: <https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf> (dernière consultation: 5 mars 2018)
- **Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 – USA Freedom Act**, Public Law 114-23, 2 juin 2015, En ligne: <https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf> (dernière consultation: 5 mars 2018)
- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act – USA Patriot Act**, Public Law 107-56, 26 octobre 2001, H.R. 3162.ENR, En ligne: <https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf> (dernière consultation: 5 mars 2018)

c. La Suède

- **Datalag**, 11 mai 1973, Svensk författningssamling [SFS] 1973:289

d. Le Royaume-Uni

- **Investigatory Powers Act 2016 Chapter 25**, 29 novembre 2016, En ligne: <https://www.legislation.gov.uk/ukpga/2016/25/contents> (dernière consultation: 5 mars 2018)

B. Les textes juridiques nationaux

1. Les normes de valeur constitutionnelle

- **Déclaration des droits de l'Homme et du Citoyen** du 27 août 1789
- **Préambule de la Constitution** du 27 octobre 1946
- **Charte de l'environnement** de 2004
- **Constitution** du 4 octobre 1958

2. Les lois et les ordonnances

a. les lois

- * La loi constitutionnelle

- **Loi constitutionnelle n° 2005-205 du 1er mars 2005**, *relative à la Charte de l'environnement*, JORF n°51 du 2 mars 2005, page 3697, texte n°2, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000790249&categorieLien=id> (dernière consultation: 5 mars 2018)

* Les lois organiques

- **Loi organique n°2001-692 du 1er août 2001**, *relative aux lois de finances*, JORF n°177 du 2 août 2001, p. 12480, texte n°1, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000394028 (dernière consultation: 5 mars 2018)

* les lois ordinaires

- **Loi du 29 juillet 1881**, *sur la liberté de la presse*, En ligne <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722&dateTexte=20090302> (dernière consultation: 5 mars 2018)
- **Loi n°70-643 du 17 juillet 1970**, *tendant à renforcer la garantie des droits individuels des citoyens*, JORF du 16 juillet 1970, p. 06751 et s., En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000693897&pageCourante=06751 (dernière consultation: 5 mars 2018)
- **Loi n° 78-17 du 6 Janvier 1978**, *relative à l'informatique, aux fichiers et aux libertés*, Journal Officiel du 7 Janvier 1978, p. 227, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000886460 (dernière consultation: 5 mars 2018)
- **Loi du 6 janvier 1978**, *relative à l'informatique, aux fichiers et aux libertés modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004*, En ligne: https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive-annotee.pdf (dernière consultation: 5 mars 2018)
- **Loi n° 86-1077 du 30 septembre 1986**, *relative à la liberté de communication*, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000512205 (dernière consultation: 5 mars 2018)
- **Loi n°90-1170 du 29 décembre 1990**, *sur la réglementation des télécommunications*, JORF n° 303 du 30 décembre 1990, p. 16439, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000533747&categorieLien=id> (dernière consultation: 5 mars 2018)
- **Loi n° 91-646 du 10 juillet 1991**, *relative au secret des correspondances émises par la voie des télécommunications* JORF n°162 du 13 juillet 1991 p. 9167, En ligne: <http://>

- www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000000173519 (dernière consultation: 5 mars 2018)
- **Loi n°95-73 du 21 janvier 1995** *d'orientation et de programmation relative à la sécurité*, spécialement son article 10, JORF n°0020 du 24 janvier 1995, page 1249, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000369046&categorieLien=id> (dernière consultation: 5 mars 2018)
 - **Loi 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, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000556901&dateTexte=19980618> (dernière consultation: 5 mars 2018)
 - **Loi n°99-574 du 9 juillet 1999**, *d'orientation agricole*, JORF n°158 du 10 juillet 1999, p. 10231, texte n°1, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000395813> (dernière consultation: 5 mars 2018)
 - **Loi n°2000-494 du 6 juin 2000**, *portant création d'une Commission nationale de déontologie de la sécurité*, Disponible en ligne à l'adresse suivante: <http://www.legifrance.gouv.fr/affichTexte.docidTexte=LEGITEXT000005629481&dateTexte=20090205> (dernière consultation: 5 mars 2018)
 - **Loi n°2002-1094 du 29 août 2002**, *d'orientation et de programmation pour la sécurité intérieure*, JORF du 30 août 2002, page 14398, texte n° 1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000780288&categorieLien=id> (dernière consultation: 5 mars 2018)
 - **Loi n°2003-239 du 18 mars 2003**, *pour la sécurité intérieure*, Disponible en ligne: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005634107&dateTexte=20090305> (dernière consultation: 5 mars 2018)
 - **Loi n° 2004-575 du 21 juin 2004**, *pour la confiance dans l'économie numérique*, JORF N°0143 du 22 juin 2004, page 11168, texte n°2, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&categorieLien=id> (dernière consultation: 5 mars 2018)
 - **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*, JORF n° 0020 du 24 janvier 2006, texte n°1, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000454124&categorieLien=id> (dernière consultation: 5 mars 2018)
 - **Loi n° 2007-1631 du 20 novembre 2007**, *relative à la maîtrise de l'immigration, à l'intégration et à l'asile*, JORF n° 270 du 21 novembre 2007, page 18993, texte n°1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000163100&dateTexte=20071120> (dernière consultation: 5 mars 2018)

www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000524004&categorieLien=id
(dernière consultation: 5 mars 2018)

- **Loi du 25 février 2008**, *relative à la rétention de sûreté et à la déclaration d'irresponsabilité pour cause de trouble mental*, JORF n°0048 du 26 février 2008, p. 3266, texte n° 1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000018162705&categorieLien=id> (dernière consultation: 5 mars 2018)
- **Loi n° 2009-669 du 12 juin 2009**, *favorisant la diffusion et la protection de la création sur internet*, JORF n°0135 du 13 Juin 2009, p. 9666, texte n°2, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id> (dernière consultation: 5 mars 2018)
- **Loi n° 2010-788 du 12 juillet 2010**, *portant engagement national pour l'environnement*, JORF n°0160 du 13 juillet 2010 p. 12905, texte n° 1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022470434&categorieLien=id> (dernière consultation: 5 mars 2018)
- **Loi n°2010-1192 du 11 octobre 2010**, *interdisant la dissimulation du visage dans l'espace public*, JORF n°0237 du 12 octobre 2010, p. 18344, Texte n° 1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022911670&categorieLien=id> (dernière consultation: 5 mars 2018)
- **Loi n°2011-267 du 14 mars 2011**, *d'orientation et de programmation pour la performance de la sécurité intérieure*, JORF n° 0062 du 15 mars 2011, page 4582, texte n°2, En ligne: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000023707312 (dernière consultation: 5 mars 2018)
- **Loi n°2013-1168 du 18 Décembre 2013**, *relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, JORF n°0294 du 19 décembre 2013 page 20570, texte n° 1, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id> (dernière consultation: 5 mars 2018)
- **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, texte n°5, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id> (dernière consultation: 5 mars 2018)
- **Loi n° 2015 – 912 du 24 juillet 2015**, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 page 12735, texte n°2, En ligne: <http://www.legifrance.gouv.fr/eli/loi/2015/7/24/>

[PRMX1504410L/jo/texte](#) (dernière consultation: 5 mars 2018)

- **Loi n°2015-1556 du 30 novembre 2015**, *relative aux mesures de surveillance des communications électroniques internationales*, JORF n°0278 du 1 décembre 2015, page 22185, texte n°1, En ligne: <https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte> (dernière consultation: 5 mars 2018)
- **Loi n°2016-1321 du 7 octobre 2016**, *pour une République numérique*, JORF n°0235 du 8 octobre 2016, Disponible en ligne à l'adresse suivante: https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=40114AB2CC997861AA4011EAB0025ED6.tplgfr31s_3?cidTexte=JORFTEXT000033202746&categorieLien=id (dernière consultation: 5 mars 2018)

3. les textes réglementaires

a. Les décrets

- **Décret n°2012-1400 du 13 décembre 2012**, *relatif au Conseil national du numérique*, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026767396> (dernière consultation: 5 mars 2018)
- **Décret n° 2013-596 du 8 juillet 2013**, *supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle*, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027678782> (dernière consultation: 5 mars 2018)
- **Décret n°2015-125 du 5 février 2015**, *relatif au blocage de 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*, JORF n°0031 du 6 février 2015 page 1811, texte n° 71, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030195477&categorieLien=id> (dernière consultation: 5 mars 2018)
- **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*, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030313562> (dernière consultation: 5 mars 2018)
- **Décret n° 2016 - 1460 du 28 octobre 2016**, *autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*, JORF n° 0254 du 30 octobre 2016, texte n°18, En ligne: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345&dateTexte=&categorieLien=id> (dernière consultation: 5

mars 2018)

V. Les codes

- Code civil
- Code de commerce
- Code de justice administrative
- Code de l'éducation
- Code de l'environnement
- Code de l'organisation judiciaire
- Code de l'urbanisme
- Code de la consommation
- Code de la propriété intellectuelle
- Code de la santé publique
- Code de la sécurité intérieure
- Code des marchés publics
- Code des postes et des communications électroniques
- Code du travail
- Code pénal
- Code de procédure pénale

VI. Les textes infra-juridiques - Les documents référents

- **BATHO Delphine, GRANDGUILLAUME Laurent**, *Amendement à l'article 26 de la loi pour une république numérique n°3318*, Non soutenu, n°CL125, 6 janvier 2016, En ligne: http://www.assemblee-nationale.fr/14/amendements/3318/CIION_LOIS/CL125.pdf (dernière consultation: 5 mars 2018)
- **Exposé des motifs, Loi n° 2015-912 du 24 juillet 2015 relative au renseignement**, Disponible en ligne à l'adresse suivante: http://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=AC82D0703DA2374DEF16BEA404A88989.tpdila23v_3?idDocument=JORFDOLE000030375694&type=expose&typeLoi=&legislature=14 (dernière consultation: 5 mars 2018)
- **Compte rendu intégral, 1ère séance et 2ème séance du Lundi 13 avril 2015, Loi n° 2015-912**

du 24 juillet 2015 relative au renseignement, Journal Officiel de la République Française, Assemblée Nationale XIVe législature, session ordinaire de 2014-2015, En ligne: <http://www.assemblee-nationale.fr/14/pdf/cri/2014-2015/20150212.pdf> (dernière consultation: 5 mars 2018)

VII. Les décisions de justice et les avis juridictionnels

A. Les décisions de justice et les avis juridictionnels internationaux et communautaires

- CEDH, *Affaire Tyrer c. Royaume-Uni*, Requête n°5856/72, Strasbourg, 25 avril 1978
- CEDH, *Malone contre Royaume-Uni*, n° 8691/79, 2 août 1984
- CEDH, *Loizidou contre Turquie*, n° 15318/89, 23 mars 1995
- CEDH (Grande Chambre), *Affaire S. et Marper contre Royaume-Uni*, Requêtes n° 30562/04 et 30566/04, Strasbourg, 4 décembre 2008, En ligne: <https://rm.coe.int/16806ae19a> (dernière consultation: 5 mars 2018)
- CJCE, *Affaire C-1/00, Arrêt de la Cour du 13 décembre 2001, Commission des communautés européennes contre République française*, Recueil de la jurisprudence 2001 I-09989, En ligne: http://curia.europa.eu/juris/showPdf.jsf?jsessionid=9ea7d2dc30dd84f84dc8e3b64819a74cdbc69833368e.e34KaxiLc3qMb40R_c_h_0_S_a_x_y_N_a_N_n_0_?text=&docid=46950&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=66877 (dernière consultation: 5 mars 2018)
- CJCE, *Affaire C-101/01, Lindqvist, arrêt de la Cour du 6 novembre 2003*, Recueil de la jurisprudence 2003 I-12971, En ligne: <http://curia.europa.eu/juris/showPdf.jsf?docid=48382&pageIndex=0&doclang=FR&dir=&occ=first&part=1&cid=1403476> (dernière consultation: 5 mars 2018)
- CJCE, *Affaire C-275/06, arrêt de la Cour (grande chambre) du 29 janvier 2008, Promusicae contre Telefonica de Espana SAU*, Recueil de la jurisprudence 2008 I-00271, En ligne: <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=70107&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=1413942>, (dernière consultation: 5 mars 2018)
 - *Conclusions de Mme Kokott - Affaire C-275/06, Conclusions de l'avocat général Mme Juliane Kokott*, présentées le 18 juillet 2007, Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/showPdf.jsf?>

[text=&docid=62901&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=413083](http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:62901:20120419:1&as=judgments&cid=413083) (dernière consultation: 5 mars 2018)

- **CJUE**, *Affaire C-461/10, arrêt de la Cour (troisième chambre) du 19 avril 2012, Bonnier Audio AB, contre Perfact Communication Sweden AB*, publié au Recueil numérique (Recueil général), Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=1421614> (dernière consultation: 5 mars 2018)
- **CJUE**, *Affaires jointes C-293/12 et C-594/12, Arrêt de la Cour (grande chambre), du 8 Avril 2014, Digital Rights Ireland Ltd Contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, Demande de décision préjudicielle, introduite par la High Court (Irlande) et le Verfassungsrichtsof, publié au Recueil numérique (Recueil général), En ligne: <http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-293/12> (dernière consultation: 5 mars 2018)
- **CJUE**, *Affaire C-131/12, Arrêt de la Cour (grande chambre) du 13 mai 2014, Google Spain et Google Inc*, Publié au Recueil numérique, Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/document/document.jsf?sessionId=9ea7d2dc30dd03f02947f35f4beeb42abca6d82bd0d4.e34KaxiLc3qMb40Rch0SaxyNaNz0?text=&docid=152065&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=1212706> (dernière consultation: 5 mars 2018)
- **CJUE**, *Affaire C-362/14, Arrêt de la Cour (grande chambre) du 6 octobre 2015, Maximilian Schrems contre Data Protection Commissioner*, Demande de décision préjudicielle, introduite par la High Court (Irlande), publié au Recueil numérique (Recueil général), En ligne: <http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-362/14> (dernière consultation: 5 mars 2018)
- **CJUE**, *Affaire C-582/14, arrêt de la Cour (deuxième chambre) du 19 octobre 2016, Patrick Breyer contre Bundesrepublik Deutschland*, publié au Recueil numérique, (Recueil général), Disponible en ligne à l'adresse suivante: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=755321> (dernière consultation: 5 mars 2018)
- **CJUE**, *Affaires jointes C-203/15 et C-698/15, Arrêt de la Cour (grande chambre) du 21 décembre 2016, Tele2 Sverige AB contre Post-och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a.*, Demandes de décision préjudicielle, introduite par le Kammarrätten i Stochholm et la Court of Appeal (England and Wales) (Civil Division), publié au

Recueil numérique (Recueil général), En ligne: <http://curia.europa.eu/juris/liste.jsf?num=C-203/15> (dernière consultation: 5 mars 2018)

- **United States Court of Appeals for the second circuit**, *ACLU v/ Clapper*, 7 mai 2015, Case 14-42, Document 168-1, En ligne: <https://www.eff.org/document/aclu-v-clapper-second-circuit-opinion> (dernière consultation: 5 mars 2018)

B. Les décisions de justice et les avis juridictionnels nationaux

1. Le Conseil constitutionnel

- **Décision n°94-352 DC du 18 janvier 1995**, *concernant la loi d'orientation et de programmation relative à la sécurité*, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html> (dernière consultation: 5 mars 2018)
- **Décision n° 99-416 DC du 12 juillet 1999**, *relative à la loi portant création d'une couverture maladie universelle*, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-416-dc/decision-n-99-416-dc-du-23-juillet-1999.11847.html> (dernière consultation: 5 mars 2018)
- **Décision n°99-419 DC du 19 novembre 1999**, *concernant la loi relative au pacte civil de solidarité*, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-419-dc/decision-n-99-419-dc-du-9-novembre-1999.11849.html> (dernière consultation: 5 mars 2018)
- **Décision n°2003-467 DC du 13 mars 2003**, *relative à la loi pour la sécurité intérieure*, En ligne: <http://www.conseil-constitutionnel.fr/conseil-con..c/decision-n-2003-467-dc-du-13-mars-2003.855.html> (dernière consultation: 5 mars 2018)
- **Décision n°2005-532 DC du 19 janvier 2006**, *portant sur la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2006/2005-532-dc/decision-n-2005-532-dc-du-19-janvier-2006.979.html> (dernière consultation: 5 mars 2018)
- **Décision n°2007-557 DC du 15 novembre 2007**, *Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile*, En Ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2007/2007-557-dc/decision-n-2007-557-dc-du-15-novembre-2007.1183.html> (dernière consultation: 5 mars 2018)
- **Décision n°2011-625 DC du 11 mars 2011**, *relative à la loi d'orientation et de programmation*

pour la performance de la sécurité intérieure, En ligne: <http://www.conseil-constitutionnel.fr/decision/2011/2011-625-dc/decision-n-2011-625-dc-du-10-mars-2011.94924.html> (dernière consultation: 5 mars 2018)

- **Décision n°2015-713 DC du 23 juillet 2015**, *concernant la loi relative au renseignement*, En ligne: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html> (dernière consultation: 5 mars 2018)

2. Le Conseil d'Etat

- **Conseil d'Etat 29 décembre 1999**, n° 206945, Publié au Recueil Lebon, En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000007996586> (dernière consultation: 5 mars 2018)
- **Conseil d'État 26 juillet 2006**, n°285714, Publié au Recueil Lebon, En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000008218473&dateTexte=> (dernière consultation: 5 mars 2018)
- **Conseil d'Etat 23 mai 2007**, n° 288149, Inédit au recueil Lebon, En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000018259508> (dernière consultation: 5 mars 2018)
- **Conseil d'Etat 16 mars 2015**, n° 370072, *Société Gatpharm*, Inédit au recueil Lebon, En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000030642893> (dernière consultation: 5 mars 2018)
- **Conseil d'Etat 8 février 2017**, 10ème - 9ème Chambres réunies, n° 393714, *JCDecaux*, Mentionné dans les tables du recueil Lebon, En ligne: <https://www.legifrance.gouv.fr/affichJuriAdmin.do?&idTexte=CETATEXT000034017907> (dernière consultation: 5 mars 2018)

3. Les juridictions judiciaires

a. La Cours de cassation

- **Cass. Crim., 7 avril 1999**, n° de pourvoi: 98-83770, Publié au Bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007070450> (dernière consultation: 5 mars 2018)
- **Cass. Soc., Audience publique du mardi 2 octobre 2001**, N° de pourvoi n° 99-42942, NIKON, Publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007046161> (dernière consultation: 5 mars 2018)

- **Cass. Crim. 14 mars 2006**, n° de pourvoi: 05-83423, Publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007069872> (dernière consultation: 5 mars 2018)
- **Cass. Crim. 21 janvier 2009**, n°de pourvoi : 08-83492, Publié au bulletin, Bulletin criminel 2009, n°24
- **Cass. Crim. 17 mai 2011**, n° de pourvoi: 10-87646, Non publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000024252814> (dernière consultation: 5 mars 2018)
- **Cass. Civ., 1ère Chambre Civile, Audience publique du jeudi 3 novembre 2016**, n° de pourvoi 15-22595, publié au bulletin, En ligne: <https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000033346676&fastReqId=233794771&fastPos=1> (dernière consultation: 5 mars 2018)

b. Les cours d'appel

- **Cour d'Appel de Paris, 13 ème chambre, section B, arrêt du 27 avril 2007**, *Anthony G. c/ SCPP*, En ligne: <https://www.legalis.net/jurisprudences/cour-dappel-de-paris-13eme-chambre-section-b-arret-du-27-avril-2007/> (dernière consultation: 5 mars 2018)
- **Cour d'Appel de Paris 13 ème chambre, section A, arrêt du 15 mai 2007**, *Henri S. c/ SCPP*, En ligne: <https://www.legalis.net/jurisprudences/cour-dappel-de-paris-13eme-chambre-section-a-arret-du-15-mai-2007/> (dernière consultation: 5 mars 2018)

c. Les tribunaux judiciaires

- **TGI de Paris**, 1ère Chambre, Section sociale, du 19 avril 2005, En ligne: <https://www.cnil.fr/sites/default/files/typo/document/JgtTGIParis19-4-2005Biometrie.pdf> (dernière consultation: 5 mars 2018)
- **TGI Paris**, 1ere Ch. 4 avril 2006
- **TGI de Bobigny**, 14 décembre 2006, *Laurent F. c/ SACEM et autres*, En ligne: <https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-bobigny-15eme-chambre-jugement-du-14-decembre-2006/> (dernière consultation: 5 mars 2018)
- **TGI de Saint Briec**, 6 septembre 2007, *Ministère public, SCPP, SACEM c/ J. P.*, En ligne: <https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-saint-briec-jugement-du-06-septembre-2007/> (dernière consultation: 5 mars 2018)

VIII. Les documents officiels

A. Les documents officiels internationaux et communautaires

1. Les documents officiels internationaux

- **Centre pour la recherche et l'innovation dans l'enseignement**, *The Well-Being of Nations: The Role of Human and Social Capital*, Paris, OCDE, 2011
- **Commission internationale d'étude des problèmes de la communication**, *Voix multiples - Un seul monde*, La Documentation Française, Les Nouvelles Editions Africaines, Unesco, 1980, En ligne: <http://unesdoc.unesco.org/images/0004/000400/040066fb.pdf> (dernière consultation: 5 mars 2018)
- **Commission Internationale de l'intervention et de la souveraineté des États**, *La responsabilité de protéger*, Décembre 2001, publié par le centre de recherches pour le développement international, 2001, p. VII – VIII, En ligne: <http://www.idrc.ca/FR/Resources/Publications/Pages/IDRCBookDetails.aspx?PublicationID=237> (dernière consultation: 5 mars 2018)
- **Commission sur la sécurité humaine**, *Rapport La sécurité humaine maintenant*, Paris, Presses de Science-Po, 2003
- **Conférence Internationale des commissaires à la protection des données personnelles et à la vie privée**, Communiqué de fermeture de la 28ème Conférence des 2 et 3 novembre 2006, *Une société de surveillance?*, Londres, Grande Bretagne, En ligne: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/06-11-03_London_Communique_EN.pdf (dernière consultation: 5 mars 2018)
- **GOHAN-KLAS Tomasz**, *The concept of the « Free and balanced flow of information » in the interpretation of central and east European countries*, UNESCO, Paris, 25 Septembre 1978, En ligne: <http://unesdoc.unesco.org/images/0003/000333/033313eb.pdf> (dernière consultation: 5 mars 2018)
- **Information Infrastructure Task Force**, *The National Information Infrastructure: Agenda for Action*, Department of Commerce, Washington DC., 15 Septembre 1993, En ligne: <http://files.eric.ed.gov/fulltext/ED364215.pdf> (dernière consultation: 5 mars 2018)
- **KIRBY Michael, TURNER Mark, DE LA QUADRA SALCEDO Tomas, KARJALA Dennis, ANGELES Jaime, NAYER André**, *Les droits de l'homme dans le cyberspace*, Comnection Droit du cyberspace, Éditions UNESCO/ECONOMICA
- **MASMOUDI Mustapha**, *The new world information order*, Commission Internationale d'étude

- des problèmes de la communication, n° 31, Juillet 1978, En ligne: <http://unesdoc.unesco.org/images/0003/000340/034010EB.pdf> (dernière consultation: 5 mars 2018)
- **OCDE**, *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel*, 23 septembre 1980, En ligne: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm> (dernière consultation: 5 mars 2018)
 - **OCDE**, *L'information numérique et la protection des libertés individuelles*, Paris, 1971, 76 pages
 - **OCDE**, *The OECD Privacy Framework*, 2013, En ligne: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (dernière consultation: 5 mars 2018)
 - **ONU**, Groupe de personnalités de haut niveau sur les menaces, les défis et le changement, *Un monde plus sûr : notre affaire à tous*, rapport ONU , 1^{er} décembre 2004, En ligne: <http://www.un.org/french/secureworld/> (dernière consultation: 5 mars 2018)
 - **ONU**, Rapport du Millénaire du Secrétaire Général, *Nous les peuples, le rôle des Nations Unies au XXI^{ème} siècle*, Nations Unies, 2000, En ligne: <http://www.un.org/french/millenaire/sg/report/> (dernière consultation: 5 mars 2018)
 - **ONU**, *Résolution adoptée par l'Assemblée générale le 25 septembre 2015, 70/1. Transformer notre monde*, le Programme de développement durable à l'horizon 2030, A/ RES/ 70/ 1, Soixante-dixième session, Ponts 15 et 116 de l'ordre du jour, Distribution générale le 21 octobre 2015, En ligne: <http://www.ipu.org/splz-f/unga16/2030-f.pdf> (dernière consultation: 5 mars 2018)
 - **PRONK Jan**, *Observations sur la relation entre le nouvel ordre international de l'information et le nouvel ordre économique international*, UNESCO - Commission internationale d'étude des problèmes de la communication, n°35, 1978, En ligne: <http://unesdoc.unesco.org/images/0003/000346/034647fb.pdf> (dernière consultation: 5 mars 2018)
 - **RUNDLE MARY, CONLEY Chris**, *Etude sur les implications éthiques des nouvelles technologies*, Programme Information pour tous, Secteur de la communication et de l'information, Unesco, Paris, 2007, En ligne: <http://unesdoc.unesco.org/images/0014/001499/149992f.pdf> (dernière consultation: 5 mars 2018)
 - **SCHILLER Herbert**, *La communication suit le capital*, UNESCO - Commission internationale d'étude des problèmes de la communication, n°47, 1978, En ligne: <http://unesdoc.unesco.org/images/0003/000342/034210fb.pdf> (dernière consultation: 5 mars 2018)
 - **Sommet Mondial sur la Société de l'Information**, Document WSIS- 03 / Geneva / DOC / 4 - F, *Déclaration de Principes - Construire la société de l'information: un défi mondial pour le nouveau millénaire*, 12 Mai 2004, En ligne: <http://www.itu.int/net/wsis/docs/geneva/official/dop->

[fr.html](#) (dernière consultation: 5 mars 2018)

- **UNESCO**, *Allocution de M. Amadou - Mahtar M'bow, Directeur général de l'UNESCO à l'ouverture de la Commission Internationale d'étude sur les problèmes de communication*, Paris, 14, décembre 1977, DG/77/15, Disponible en ligne à l'adresse suivante: <http://unesdoc.unesco.org/images/0002/000290/029029fb.pdf> (dernière consultation: 5 mars 2018)
- **UNESCO**, *Résolution de la Conférence générale de l'UNESCO, 19 C/Résolutions, 4.126*, in Records of the General Conference, Nineteenth Session, Nairobi, du 26 octobre au 30 novembre 1976, Volume 1 Résolutions, Disponible en ligne à l'adresse suivante: <http://unesdoc.unesco.org/images/0011/001140/114038E.pdf> (dernière consultation: 5 mars 2018)
- **UNESCO**, *Résolution de la Conférence générale de l'UNESCO, 20 C/ Résolutions, 15.1, Déclaration sur les principes fondamentaux concernant la contribution des organes d'information au renforcement de la paix et de la compréhension internationale, à la promotion des droits de l'homme et à la lutte contre le racisme, l'apartheid et l'incitation à la guerre*, in Actes de la Conférence générale, Vingtième session, Paris, 24 octobre - 28 novembre 1978, Volume 1, Résolutions, En ligne: <http://unesdoc.unesco.org/images/0011/001140/114032F.pdf> (dernière consultation: 5 mars 2018)
- **Union Internationale des Télécommunications**, *Document d'information sur l'UIT - Connect 2020: définir un programme d'action mondial pour le secteur des TIC*, Conférence de plénipotentiaires de l'UIT, 2014, Busan, Corée, En ligne: <https://www.itu.int/en/ Plenipotentiary/2014/newsroom/Documents/backgrounders/pp14-backgrounder-connect-2020-fr.pdf> (dernière consultation: 5 mars 2018)
- **Union Internationale des Télécommunications**, *Rapport Mesurer la société de l'information 2015 - Résumé analytique*, 2015, UIT, Genève, Suisse, En ligne: <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-F.pdf> (dernière consultation: 5 mars 2018)

2 Les documents officiels communautaires

a. Les communications et avis

- **Comité économique et social européen**, *Avis sur la communication au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions – Vers une économie de la donnée prospère*, Com (2014), 4442 final, 2915/C 242/11, paru au JOCE le 23 juillet 2015, C 242/61, En ligne: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C_.2015.242.01.0061.01.FRA&toc=OJ:C:2015:242:TOC (dernière consultation: 5 mars 2018)

- **Commission Européenne**, *Communication de la Commission - Les services d'intérêt général en Europe*, Journal Officiel C281 du 26 septembre 1996 modifiée par la Communication de la Commission, *les services d'intérêt général en Europe*, Journal Officiel C17 du 19 janvier 2001
- **Commission Européenne**, Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions accompagnant la communication intitulée « un marché unique pour l'Europe du 21ème siècle », *Les services d'intérêt général, y compris les services sociaux d'intérêt général: un nouvel engagement européen*, Com. (2007) 725 final, 20 novembre 2007, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52007DC0725&from=FR> (dernière consultation: 5 mars 2018)
- **Commission Européenne**, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions, *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Com (2010), 609 final, Bruxelles, 4 novembre 2010, En ligne: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_fr.pdf (dernière consultation: 5 mars 2018)
- **Commission Européenne**, Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions, COM (2012) 9 final, *Protection de la vie privée dans un monde en réseau - Un cadre européen relatif à la protection des données, adapté aux défis du 21 ème siècle*, Bruxelles, 25 janvier 2012, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012DC0009&from=EN> (dernière consultation: 5 mars 2018)
- **Commission Européenne**, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 2 juillet 2014, *Vers une économie de la donnée prospère*, Com (2014), 442 final, Non publiée au JOCE, En ligne: <http://ec.europa.eu/transparency/regdoc/rep/1/2014/FR/1-2014-442-FR-F1-1.Pdf> (dernière consultation: 5 mars 2018)
- **Commission Européenne**, Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et au comité des régions, Com (2017) 9 final, *Créer une économie européenne fondée sur les données*, Bruxelles, 10 janvier 2017, En ligne: <http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-9-F1-FR-MAIN-PART-1.PDF> (dernière consultation: 5 mars 2018)
- **Commission Européenne**, Décision de la Commission n° 2000/520/CE du 26 Juillet 2000, *conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la*

pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32000D0520&from=FR> (dernière consultation: 5 mars 2018)

- **Contrôleur européen de la protection des données**, *Avis sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la Sécurité intérieure*, 2012/C 35/O3, JOUE du 9 février 2012, En ligne: [http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012XX0209\(03\)&from=FR](http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012XX0209(03)&from=FR) (dernière consultation: 5 mars 2018)
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 1/99 du 26 janvier 1999 concernant le niveau de protection des données à caractère personnel aux États-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain*, WP 15, 26 janvier 1999
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 2/99 du 19 avril 1999 concernant la pertinence des « principes internationaux de la sphère de sécurité » publiés par le ministère du commerce des États-Unis le 19 avril 1999*, 3 mai 1999, WP 19
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 2/2007 concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record - PNR) aux autorités américaines du 15 février 2007 et révisé et mis à jour le 24 juin 2008*, 000345/07/FR, WP 132, 000345-01/07/FR, WP 151
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 4/2007 sur le concept de données à caractère personnel*, Adopté le 20 juin 2007, 01248/07/FR, WP 136
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, Adopté le 16 février 2010, 00264/10/FR, WP 169, En ligne: https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp169_fr.pdf (dernière consultation: 5 mars 2018)
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 3/2010 sur le principe d'accountability*, Adopté le 13 juillet 2010, 00062/10/EN, WP 173
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 15/2011 sur la définition du consentement*, 13 juillet 2011, 01197/11/FR, WP 187, En ligne: https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp187_fr.pdf (dernière consultation: 5 mars 2018)
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 04/2014 sur la*

surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, adopté le 10 avril 2014, 819/14/FR, WP 215, En ligne: <http://www.dataprotection.ro/servlet/ViewDocument?id=1287> (dernière consultation: 5 mars 2018)

- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 05/2014 sur les techniques d'anonymisation*, adopté le 10 avril 2014, 0829/14/FR, WP 216, En ligne: <http://www.dataprotection.ro/servlet/ViewDocument?id=1288> (dernière consultation: 5 mars 2018)
- **Groupe de travail « Article 29 » sur la protection des données**, *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable de traitement des données au sens de l'article 7 de la directive 95/46/CE*, Adopté le 9 avril 2014, 844/14/FR, WP 217
- **Groupe de travail « Article 29 » sur la protection des données**, *EU - US Privacy Shield - First annual Joint Review*, Adopté le 28 novembre 2017, 17/EN, WP 255
- **Groupe de travail « Article 29 » sur la protection des données**, *Lignes directrices concernant les délégués à la protection des données*, Adoptées le 13 décembre 2016, Version révisée et adoptée le 5 avril 2017, 16/FR, WP 243 rev.01, En ligne: https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf (dernière consultation: 5 mars 2018)
- **Secrétariat Général du Conseil européen**, EUCO 169/13, CO EUR 13, CONCL 7, *Conclusions du Conseil Européen des 24 et 25 octobre 2013, Bruxelles, 25 octobre 2013*, En ligne: <http://data.consilium.europa.eu/doc/document/ST-169-2013-INIT/en/pdf> (dernière consultation: 5 mars 2018)

b. Les rapports et les documents de travail

- **BECKER Peggy, (sous la direction de Dick Holdsworth)**, *Development of surveillance technology and risk of abuse of economic information, Vol 1/5, Presentation and Analysis*, Document de travail pour le Panel STOA, Luxembourg, Décembre 1999, Disponible en ligne: [http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET\(1999\)168184_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf) (dernière consultation: 5 mars 2018)
- **CAMPBELL Duncan**, *Development of surveillance technology and risk of abuse of economic information – Part. 2/5 : The state of the art in communications Intelligence (COMINT) of automated processing for Intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition*, Working Document for the STOA Panel, Luxembourg, Octobre 1999
- **Commission des Communautés Européennes**, *Livre Blanc Croissance, compétitivité, emploi - Les défis et les pistes pour entrer dans le XXI ème siècle*, Bulletin des Communautés européennes,

- Supplément 6/93, Luxembourg: Office des publications officielles des Communautés européennes, 1993, En ligne: <http://bookshop.europa.eu/fr/croissance-comp-titivit-emploi-les-d-fis-et-les-pistes-pour-entrer-dans-le-xxie-si-cle.-livre-blanc-bulletin-des-communaut-s-europ-ennes-suppl-ment-6-93-pbCMNF93061/> (dernière consultation: 5 mars 2018)
- **Commission des Communautés Européennes**, COM (1999) 719 final, *Livre blanc sur la sécurité alimentaire*, Bruxelles, 12 janvier 2000, Disponible en ligne à l'adresse suivante: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:51999DC0719&from=FR> (dernière consultation: 5 mars 2018)
 - **Commission des Communautés européennes**, COM (2003) 270 final, *Livre vert sur les services d'intérêt général*, Bruxelles, 21 mai 2003, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52003DC0270&from=FR> (dernière consultation: 5 mars 2018)
 - **Commission des Communautés européennes**, Com (2005), *Livre vert sur un programme européen de protection des infrastructures critiques*, présenté par la Commission, Bruxelles, le 17 novembre 2005, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52005DC0576&from=FR> (dernière consultation: 5 mars 2018)
 - **Commission Européenne**, Com (2017) 611 final, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield*, Bruxelles, 18 octobre 2017
 - **Groupe de travail « Article 29 » sur la protection des données**, *Document de travail: Le respect de la vie privée sur Internet - Une approche européenne intégrée sur la protection des données en ligne*, Adopté le 21 novembre 2000, 5063/00/FR/Final, WP 37
 - **Groupe de travail « Article 29 » sur la protection des données**, *Working document 01/2016 on the justification of interference with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data*, 13 avril 2016
 - **GOMES Ana - Commission des libertés civiles, de la justice et des affaires intérieures**, Rapport du Parlement européen (2016/2025 (INI)) *sur les incidences des mégatonnes pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi*, 20 février 2017, En ligne: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0044+0+DOC+PDF+V0//FR> (dernière consultation: 5 mars 2018)
 - **PIODI Franco et MOMBELLI Iolanda**, *L'affaire Échelon - Les travaux du Parlement européen sur le système global d'interception, 1998 – 2002 – Étude*, Parlement Européen, Direction Générale des services de recherche Parlementaire – Unité Archives Historiques, Octobre 2014, En

ligne: <http://www.europarl.europa.eu/EPRS/EPRS-Study-538877-Echelon.pdf> (dernière consultation: 5 mars 2018)

- **Proposition de Règlement du Parlement européen et du Conseil du 25 janvier 2012, 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**, COM (2012) 11 final, Non publiée au JOCE. En ligne: <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012PC0011&from=FR> (dernière consultation: 5 mars 2018)
- **Proposition de Règlement du Parlement européen et du Conseil**, COM (2017) 10 final, *concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive de 2002/58/CE (règlement « vie privée et communications électroniques »)*, Bruxelles, 10 janvier 2017, En ligne: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017PC0010&from=EN> (dernière consultation: 5 mars 2018)
- **Proposition de Règlement du Parlement européen et du Conseil**, COM (2017) 495 final, *concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne*, Bruxelles, 13 Septembre 2017, En ligne: <http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-495-F1-FR-MAIN-PART-1.PDF> (dernière consultation: 5 mars 2018)
- **WRIGHT Steve**, *An appraisal of technologies of political control*, S.T.O.A., Working document, PE 166.499, 6 Janvier 1998, En ligne: <http://aei.pitt.edu/5538/1/5538.pdf> (dernière consultation: 5 mars 2018)

B. Les documents officiels nationaux

1. La France

a. Les projets et propositions de lois

- **Projet de loi n° 2516, relatif à l'informatique et aux libertés**, renvoyé à la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République à défaut de constitution d'une Commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement, Présenté au nom de M. Jacques CHIRAC, Premier Ministre, par M. Jean LECANUET, garde des sceaux, Enregistré à la Présidence de l'Assemblée Nationale le 9 août 1976, annexe au procès-verbal de la séance du 2 octobre 1976, Assemblée Nationale, Première session ordinaire de 1976-1977, En ligne: <https://www.senat.fr/leg/pjl76-2516.pdf> (dernière consultation: 5 mars 2018)

- **Projet de loi n°490**, *relatif à la protection des données personnelles*, (Procédure accélérée), Présenté au nom de M. Edouard Philippe, Premier Ministre, Par Mme Nicole Belloubet, garde des sceaux, ministre de la Justice, Enregistré à la Présidence de l'Assemblée nationale le 13 décembre 2017, Assemblée nationale, Quinzième législature, En ligne: <http://www.assemblee-nationale.fr/15/pdf/projets/pl0490.pdf> (dernière consultation: 5 mars 2018)
- **Proposition de loi n°1454**, *tendant à la création d'un comité de surveillance et d'un tribunal de l'informatique*, déposée par Michel PONIATOWSKI, distribuée et renvoyée à la commission des lois constitutionnelles, de la législation et de l'Administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et & du Règlement, mentionnée par le compte rendu intégral de la 69ème séance en Assemblée Nationale, du 25 novembre 1970 (séance 2), En ligne: <http://archives.assemblee-nationale.fr/4/cri/1970-1971-ordinaire1/069.pdf> (dernière consultation: 5 mars 2018)
- **Proposition de loi n°144**, *tendant à créer un directoire et un tribunal de l'informatique*, déposée par M. Henri Caillavet, mentionnée dans le compte rendu intégral des séances du sénat, seconde session ordinaire de 1973 – 1974, séance du mardi 2 avril 1974, Débats Parlementaires, Journal officiel de la République Française du mercredi 3 avril 1974, En ligne: http://www.senat.fr/comptes-rendus-seances/5eme/pdf/1974/04/s19740402_0201_0246.pdf (dernière consultation: 5 mars 2018)
- **Proposition de loi n°1004**, *tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens*, (renvoyée à la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République à défaut de constitution d'une Commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement), présentée par M. Pierre-Bernard COUSTE, enregistré à la Présidence de l'Assemblée Nationale le 4 avril 1974, annexe au procès-verbal de la séance du 6 juin 1974, Assemblée Nationale, seconde session ordinaire de 1973-1974, En ligne: <https://www.senat.fr/leg/pp173-1004.pdf> (dernière consultation: 5 mars 2018)
- **Proposition de loi constitutionnelle**, *visant à retirer le principe de précaution du bloc de constitutionnalité*, (Renvoyée à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement), présentée par M. Eric WOERTH, Enregistrée à la Présidence de l'Assemblée nationale le 13 juin 2014, En ligne: <http://www.assemblee-nationale.fr/14/propositions/pion2033.asp> (dernière consultation: 5 mars 2018)

b. Les délibérations de la CNIL

- **CNIL**, *Délibération n° 00-056 du 16 novembre 2000, portant avis sur un projet d'arrêté présenté par le ministre de l'éducation nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès par la reconnaissance des empreintes digitales de certains personnels de l'éducation nationale, pour certains locaux de la cité académique de Lille*, En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653132> (dernière consultation: 5 mars 2018)
- **CNIL**, *Délibération n° 02-075 du 24 octobre 2002 portant dénonciation au Parquet d'infractions à la loi du 6 janvier 1978*, En ligne: https://www.cnil.fr/sites/default/files/typo/document/delib_spam.pdf (dernière consultation: 5 mars 2018)
- **CNIL**, *Délibération n°2008 - 422 du 6 novembre 2008 portant décision de la formation restreinte à l'égard de la société X*, En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000020444356> (dernière consultation: 5 mars 2018)
- **CNIL**, *Délibération n°2011-035 du 17 mars 2011 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société X*, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023733987&fastReqId=1901417590&fastPos=1> (dernière consultation: 5 mars 2018)
- **CNIL**, *Délibération N°2012-404 du 15 novembre 2012 portant recommandation relative aux traitements des données de consommation détaillées collectées par les compteurs communicants*, Disponible en ligne à l'adresse suivante: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000026958542&fastReqId=287627783&fastPos=1> (dernière consultation: 5 mars 2018)
- **CNIL**, *Délibération n°2015-255 du 16 juillet 2015 refusant la mise en oeuvre par la société JCDecaux d'un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense (demande d'autorisation n° 1833589)*, En ligne: <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000031159401> (dernière consultation: 5 mars 2018)

c. Les avis, communiqués et délibérations émanant d'autres institutions

- **Conseil National du Numérique**, *Avis du Conseil National du numérique sur le fichier TES*, décembre 2016, En ligne: https://cnnumerique.fr/files/2017-10/Avis-TES_CNNum_Web_0.pdf (dernière consultation: 5 mars 2018)

- **Conseil National du Numérique**, Communiqué de Presse - *Fichier TES: le CNNum réaffirme ses préoccupations et invite le Gouvernement à expliciter le plan d'action correspondants aux recommandations de l'ANSSI et de la DINSIC*, Paris, 8 février 2017
- **Conseil National du Numérique**, Communiqué de Presse - *Renseignement: le Conseil national du numérique s'inquiète d'une extension du champ de la surveillance et invite à renforcer les garanties et les moyens du contrôle démocratique*, Paris, 19 mars 2015

d. Réponse ministérielle

- **Réponse du Ministère de l'intérieur** publiée dans le JO, Sénat, 16 avril 2015, p. 887, à la question écrite n°13406 de M. Hervé Maurey publiée dans le JO, *Dispositif Voisins Vigilants*, Sénat, 23 octobre 2014, p. 2375, En ligne: <https://www.senat.fr/questions/base/2014/qSEQ141013406.html> (dernière consultation: 5 mars 2018)

e. Les rapports et les documents de travail officiels

- **ATTALI Jacques**, *Rapport de la Commission pour la libération de la croissance française*, XO Éditions, La Documentation française, 2008, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000041.pdf> (dernière consultation: 5 mars 2018)
- **BLOCHE Patrick, VERCHERE Patrice**, *Rapport d'information n° 3560 déposé en application de l'article 145 du Règlement par la mission d'information commune sur les droits de l'individu dans la révolution numérique*, Assemblée nationale, 13^{ème} législature, enregistré à la Présidence de l'Assemblée nationale le 22 juin 2011, En ligne: <http://www.assemblee-nationale.fr/13/pdf/rap-info/i3560.pdf> (dernière consultation: 5 mars 2018)
- **BRAIBANT Guy**, *Données personnelles et société de l'information - Rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46*, 3 mars 1998, La Documentation française, décembre 1998
- **BOCKEL Jean-Marie**, *Rapport d'information n°681 fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense*, Sénat, Session extraordinaire de 2011 -2012, Enregistré à la Présidence du Sénat le 18 juillet 2012, En ligne: <https://www.senat.fr/rap/r11-681/r11-6811.pdf> (dernière consultation: 5 mars 2018)
- **CARCENAC Thierry**, *Pour une administration électronique citoyenne : contributions au débat*, Paris, La Documentation française, 2001, 124 pages. En ligne à l'adresse suivante: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/014000291.pdf> (dernière consultation: 5 mars 2018)

- **CNIL**, *27 ème Rapport d'activité* , 2006, Paris, La documentation française, Juillet 2007, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000422.pdf> (dernière consultation: 5 mars 2018)
- **CNIL**, Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, En ligne: <https://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf> (dernière consultation: 5 mars 2018)
- **CNIL**, *Les transferts de données à caractère personnel hors Union européenne*, Novembre 2012, En ligne: <https://www.cnil.fr/sites/default/files/typo/document/GUIDE-transferts-integral.pdf> (dernière consultation: 5 mars 2018)
- **CNIL**, *Le corps, nouvel objet connecté – Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde*, Cahiers Innovation et Perspectives n°02, Mai 2014, En ligne: https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf (dernière consultation: 5 mars 2018)
- **CNIL**, *Les compteurs communicants Linky: la position de la CNIL sur le stockage local de la courbe de charge*, 30 novembre 2015, En ligne: <https://www.cnil.fr/fr/compteurs-communicants-linky-la-position-de-la-cnil-sur-le-stockage-local-de-la-courbe-de-charge-0> (dernière consultation: 5 mars 2018)
- **CNIL**, *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing*, En ligne: http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf (dernière consultation: 5 mars 2018)
- **CNIL**, *Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique - Comment permettre à l'Homme de garder la main ? - Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017, Disponible en ligne à l'adresse suivante: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf (dernière consultation: 5 mars 2018)
- **CNIL**, *Synthèse des réponses à la consultation publique sur le Cloud computing lancée par la CNIL d'octobre à décembre 2011 et analyse de la CNIL*, Disponible en ligne à l'adresse suivante: http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Synthese_des_reponses_a_la_consultation_publique_sur_le_Cloud_et_analyse_de_la_CNIL.pdf (dernière consultation: 5 mars 2018)
- **Commission des maires sur la sécurité**, *Rapport au Premier Ministre: Face à la délinquance:*

- prévention, répression, solidarité*, Décembre 1982, Collection des rapports officiels, La documentation Française, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/834037801.pdf> (dernière consultation: 5 mars 2018)
- **Conseil d'Etat**, *Etude annuelle 2014 - Le numérique et les droits fondamentaux*, La Documentation française, Septembre 2014, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf> (dernière consultation: 5 mars 2018)
 - **Conseil Général de l'économie, de l'industrie, de l'énergie et des technologies**, *Rapport à Madame la Secrétaire d'Etat chargée du Numérique concernant les modalités de régulation des algorithmes de traitement des contenus*, 13 mai 2016, En ligne: [https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2016_05_13_Rapport_Algorithmes\(1\).pdf](https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2016_05_13_Rapport_Algorithmes(1).pdf) (dernière consultation: 5 mars 2018)
 - **Conseil National du Numérique**, *Rapport du Conseil national du numérique sur la neutralité des plateformes remis au ministre de l'Economie, du Redressement productif et du Numérique et à la secrétaire d'Etat chargée du Numérique, Neutralité des plateformes - Réunir les conditions d'un environnement numérique ouvert et soutenable*, Mai 2014, En ligne: https://cnnumerique.fr/wp-content/uploads/2014/06/CNNum_Rapport_Neutralite_des_plateformes.pdf (dernière consultation: 5 mars 2018)
 - **Cour des Comptes**, Rapport public thématique – *L'organisation et la gestion des forces de sécurité publique*, juillet 2011, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/114000374/0000.pdf> (dernière consultation: 5 mars 2018)
 - **Cour des Comptes**, *Le rapport public annuel 2018 - Tome 1: Les observations*, En ligne: https://www.ccomptes.fr/sites/default/files/2018-02/RPA2018-Tome-1-integral_0.pdf (dernière consultation: 5 mars 2018)
 - **CURIEN Nicolas, MUET Pierre-Alain**, *Rapport sur la société de l'information*, Conseil d'Analyse économique, La Documentation française, Paris, 2004, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/044000180.pdf> (dernière consultation: 5 mars 2018)
 - **DETRAIGNE Yves, ESCOFFIER Anne-Marie**, *Rapport d'information n° 441 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, Sénat, Session ordinaire de 2008 - 2009, Annexe au procès verbal de la séance du 27 mai 2009, En ligne: <http://www.senat.fr/rap/r08-441/r08-4411.pdf> (dernière consultation: 5 mars 2018)

- **Direction Générale de la Police Nationale, Comité interministériel de prévention de la délinquance**, *Guide méthodologique de vidéoprotection – L'outil vidéo dans une démarche de sûreté et de sécurité*, La Documentation Française, Paris, 2009
- **GAUDIN Michel, BAUER Alain**, *Livre blanc sur la sécurité publique*, Ministère de l'intérieur, de l'outre mer, des collectivités territoriales et de l'immigration, Collection des rapports officiels, La documentation française, novembre 2011, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/114000645.pdf> (dernière consultation: 5 mars 2018)
- **JOYANDET Alain, HERISSON Pierre, TÜRK Alex**, *Rapport d'information n° 436 Mission commune d'information sur l'entrée dans la société de l'information*, Sénat, annexe au procès-verbal de la séance du 25 septembre 1997, En ligne: https://www.senat.fr/rap/r96-436/r96-436_mono.html (dernière consultation: 5 mars 2018)
- **KOURILSKY Philippe, VINEY Geneviève**, *Rapport au premier ministre - Le principe de précaution*, Odile Jacob, La Documentation française, 1999, Disponible en ligne à l'adresse suivante : <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/004000402.pdf> (dernière consultation: 5 mars 2018)
- **LAFFITTE Pierre, Office Parlementaire d'évaluation des choix scientifiques et technologiques**, *Rapport n° 3335 sur les réseaux grands débits et l'entrée dans la société de l'information*, enregistré à la Présidence de l'Assemblée nationale le 7 février 1997, En ligne: <http://www.assemblee-nationale.fr/10/rap-off/i3335-t1.pdf> (dernière consultation: 5 mars 2018)
- **LASBORDES Pierre**, *Sécurité des systèmes d'information: un enjeu majeur pour la France*, La documentation française, 13 janvier 2006, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000048.pdf> (dernière consultation: 5 mars 2018)
- *Livre Blanc sur la défense et la sécurité nationale*, La documentation française, Odile Jacob, juin 2008, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf> (dernière consultation: 5 mars 2018)
- *Livre Blanc sur la défense et la sécurité nationale*, Direction de l'information légale et administrative, Paris, 2013, En ligne: <http://fr.calameo.com/read/000331627d6f04ea4fe0e> (dernière consultation: 5 mars 2018)
- **Ministère de l'enseignement supérieur et de la recherche**, *Rapport général sur la stratégie de recherche et d'innovation 2009 - 2012*, 2009, En ligne: http://media.enseignementsup-recherche.gouv.fr/file/SNRI/69/8/Rapport_general_de_la_SNRI_-_version_finale_65698.pdf (dernière consultation: 5 mars 2018)
- **Ministère de la Transition écologique et solidaire - Ministère de l'intérieur**, Rapport CGEDD

- n°011008-01 - IGA n° 17018 - R établi par Dominique Hucher, Jean François Landel et Maxime Tandonnet, *Conditions de faisabilité du projet Ecobonus de la Métropole européenne de Lille - un « péage positif » innovant à consolider*, Juin 2017, Disponible en ligne l'adresse suivante: http://cgedd.documentation.developpement-durable.gouv.fr/documents/cgedd/011008-01_rapport.pdf (dernière consultation: 5 mars 2018)
- **MORIN-DESAILLY Catherine**, *Rapport d'information n°443 fait au nom de la commission des affaires européennes sur l'Union européenne, colonie du monde numérique ?*, Sénat, Session ordinaire 2012-2013, enregistré à la Présidence du Sénat le 20 mars 2013, En ligne: <https://www.senat.fr/rap/r12-443/r12-4431.pdf> (dernière consultation: 5 mars 2018)
 - **MORIN-DESAILLY Catherine**, *Rapport d'information n°696 fait au nom de la mission commune d'information « nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet »*, Sénat, Session extraordinaire de 2013-2014, enregistré à la Présidence du Sénat le 8 juillet 2014, En ligne: <https://www.senat.fr/rap/r13-696-1/r13-696-11.pdf> (dernière consultation: 5 mars 2018)
 - **NORA Simon et MINC Alain**, *Rapport à Monsieur le Président de la République concernant l'informatisation de la société*, 1978, La documentation française, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000252.pdf> (dernière consultation: 5 mars 2018)
 - **PAUL Christian, FERAL-SCHUHL Christiane**, *Rapport d'information n° 3119 déposé par la Commission de Réflexion et de propositions sur les droits et libertés à l'âge du numérique - Numérique et Libertés: Un nouvel âge démocratique*, 2015, En ligne: <http://www.assemblee-nationale.fr/14/pdf/rapports/r3119.pdf> (dernière consultation: 5 mars 2018)
 - **PLACE Jean-Vincent**, *Rapport d'information fait au nom de la commission des finances sur les investissements dans la police et la gendarmerie*, Enregistré à la Présidence du Sénat le 22 octobre 2013, En ligne: <http://www2.senat.fr/rap/r13-091/r13-0911.pdf> (dernière consultation: 5 mars 2018)
 - **ROMANI Roger**, *Rapport n° 449 d'information fait au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense*, Sénat, Session extraordinaire de 2007 - 2008, Annexe au procès verbal de la séance du 8 juillet 2008, En ligne: <https://www.senat.fr/rap/r07-449/r07-4491.pdf> (dernière consultation: 5 mars 2018)
 - **SALLAZ Jean-Pierre, DEBROSSE Philippe, HAN Dominique**, *Rapport sur l'efficacité de la vidéoprotection*, Ministère de l'intérieur, de l'Outre-Mer et des collectivités territoriales, Octobre 2009, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/>

[094000540.pdf](#) (dernière consultation: 5 mars 2018)

- **STIGLITZ Joseph, SEN Amartya, FITOUSSI Jean-Paul**, *Rapport au Président de la République de la Commission sur la mesure des performances économique et du progrès social*, Ministère de l'économie, de l'industrie et de l'emploi, Septembre 2009, En ligne: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000427.pdf> (dernière consultation: 5 mars 2018)
- **THERY Gérard, BONAFE Alain**, *Rapport au premier ministre - Les autoroutes de l'information*, *Collection des rapports officiels*, La documentation française, Janvier 1994
- **TURK Alex**, *Rapport n°218 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, relatif 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*, Sénat, Session ordinaire de 2002-2003, annexe au procès-verbal de la séance du 19 mars 2003, En ligne: <https://www.senat.fr/rap/102-218/102-2181.pdf> (dernière consultation: 5 mars 2018)
- **URVOAS Jean-Jacques**, Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014*, En ligne: <http://www.assemblee-nationale.fr/14/pdf/rap-off/i2482.pdf> (dernière consultation: 5 mars 2018)
- **URVOAS Jean-Jacques et VERCHERE Patrice**, *Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, enregistrée à la présidence de l'Assemblée nationale le 14 mai 2013, En ligne: <http://www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf> (dernière consultation: 5 mars 2018)
- **VEIL Simone**, *Redécouvrir le Préambule de la Constitution*, *Rapport du Comité de Réflexion sur le Préambule de la Constitution au Président de la République*, La Documentation française, *Collection des rapports officiels*, Décembre 2008, Disponible en ligne à l'adresse suivante: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000758.pdf> (dernière consultation: 5 mars 2018)

2. Les Etats-Unis

- **ARMITAGE Richard, NYE Joseph**, *A smarter, more secure America*, Center for Strategic and International Studies, Commission on Smart Power, Library of Congress Cataloging in

- Publication Data, 2007, En ligne: <https://carnegieendowment.org/files/csissmartpowerreport.pdf> (dernière consultation: 5 mars 2018)
- **National Security Council Intelligence**, *Directive n°6 – Signals Intelligence*, et datant du 17 février 1972, En ligne: <https://fas.org/irp/offdocs/nsqid-6.pdf> (dernière consultation: 5 mars 2018)
 - **PORAT Marc Uri**, *The Information economy: definition and measurement*, Nine Volumes, Washington DC, Department of Commerce Government Printing Office, 1977
 - **The Privacy Protection Study Commission**, *The Report of the Privacy Protection Study Commission - Personal Privacy in an information Society*, July 1977, En ligne: <https://www.ncjrs.gov/pdffiles1/Digitization/49602NCJRS.pdf> (dernière consultation: 5 mars 2018)
 - **THE WHITE HOUSE**, *A framework for global electronic commerce*, 1 er Juillet 1997, En ligne: <https://clinton4.nara.gov/WH/New/Commerce/read.html> (dernière consultation: 5 mars 2018)
 - **U.S. Congress Senate Committee on Government Operations**, *Legislative history of the Privacy Act of 1974, S.3418, Public Law 93-579*, Source Book on Privacy, September 1976, En ligne: http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf (dernière consultation: 5 mars 2018)

3. L'Irlande

- **KITCHIN Rob**, *Getting smarter about smart cities: Improving data privacy and data security*, Data Protection Unit, Department of the Taoiseach, Dublin, Ireland, 28 Janvier 2016, En ligne: <http://eprints.maynoothuniversity.ie/7242/1/Smart> (dernière consultation: 5 mars 2018)

IX. Les discours politiques, les articles de presse et les enquêtes

A. Les discours politiques

- **CONSTANT Benjamin**, *De la liberté des anciens comparées à celle des modernes*, Discours prononcé à l'Athénée royal de Paris, 1819, En ligne: http://etienne.chouard.free.fr/Europe/Documents_conferences/Constant_Benjamin_Liberte_anciens_modernes_1819.pdf (dernière consultation: 5 mars 2018)

B. Les enquêtes

- **BAUER Alain**, *Où sont les policiers?*, La gazette des communes, 8 février 1999
- **BAUER Alain, SOULLEZ Christophe**, *Où sont les policiers et les gendarmes?*, La gazette des communes, 16 avril 2010, En ligne: <http://www.lagazettedescommunes.com/telechargements/>

[etude_policiers_gendarmes_bauer_04_2010.pdf](#) (dernière consultation: 5 mars 2018)

X. Les sites Internet

- **Blog et journal allemand:** <https://opendatacity.de>
 - Et spécialement: *Stasi Versus NSA, Quelle place prendraient les armoires d'archivage de la STASI et de la NSA - si la NSA décidait d'imprimer ses 5 zettaoctet de fichiers?* (0,0019 km² pour la Stasi, 17 millions de km² pour la NSA), En ligne: <https://apps.opendatacity.de/stasi-vs-nsa/francais.html> (dernière consultation: 5 mars 2018)
- **Blog d'Henri Verdier** (directeur d'Etalab) :
 - **VERDIER Henri**, *Non les données ne sont pas du pétrole*, blog en ligne, <http://www.henriverdier.com/2013/03/non-les-donnees-ne-sont-pas-du-petrole.html> (dernière consultation: 5 mars 2018)
 - **VERDIER Henri**, *Gouvernement des algorithmes: une contribution au débat*, 27 octobre 2014, En ligne: <http://www.henriverdier.com/2014/10/gouvernement-des-algorithmes-whats-next.html> (dernière consultation: 5 mars 2018)
- **Département du commerce des Etats-Unis:** <https://www.ntia.doc.gov/home>
 - Et spécialement: **National Telecommunication and Information Administration**, *Elements of Effective selfregulation for privacy Protection*, Janvier 1998, United States Department of Commerce, En ligne: <http://www.ntia.doc.gov/reports/privacydraft/198dftrprin.htm> (dernière consultation: 5 mars 2018)
- **Dictionnaire (9ème édition) de l'Académie française:** <http://atilf.atilf.fr/academie9.htm>
- **Dictionnaire et Encyclopédie Larousse:** <http://www.larousse.fr>
- **Dictionnaire Trésor de la langue française informatisée:** <http://www.atilf.fr/spip.php?rubrique77>
- **Site d'actualités Clubic:** <http://www.clubic.com/>
 - **GAROSCIO Paolo**, *Facebook: l'IA pour lutter contre le terrorisme*, 16 juin 2017, Clubic, En ligne: <http://www.clubic.com/internet/facebook/actualite-832002-facebook-ia-lutter-terrorisme.html> (dernière consultation: 5 mars 2018)
 - **GAROSCIO Paolo**, *Lisez les conditions d'utilisation ou vous finirez par laver des toilettes*, 22 juillet 2017, Clubic, <http://www.clubic.com/insolite/actualite-833734-lisez-conditions-utilisation-finirez-laver-toilettes.html> (dernière consultation: 5 mars 2018)
- **Site d'actualités Numerama:** <http://www.numerama.com>

- **CHAMPEAU Guillaume**, *Données de connexion: la France « ne pourra pas continuer à ignorer » la CJUE*, 12 mars 2015, En ligne: <http://www.numerama.com/magazine/32470-donnees-de-connexion-la-france-ne-pourra-pas-continuer-a-ignorer-la-cjue.html> (dernière consultation: 5 mars 2018)
- **CHAMPEAU Guillaume**, *Free peut attribuer la même adresse Ip à plusieurs abonnés*, 15 février 2016, En ligne: <http://www.numerama.com/tech/145703-free-peut-attribuer-la-meme-adresse-ip-a-plusieurs-abonnes.html> (dernière consultation: 5 mars 2018)
- **Site d'actualités ZDnet**: <http://www.zdnet.fr/>
 - **AUFFRAY Christophe**, *SONOS: les données ou la vie de vos (nos) appareils !*, 22 août 2017, Zdnet, Disponible en ligne à l'adresse suivante: <http://www.zdnet.fr/actualites/sonos-les-donnees-ou-la-vie-de-vos-nos-appareils-39856314.htm> (dernière consultation: 5 mars 2018)
 - **AUFFRAY Christophe**, *CNIL: « pas d'innovation sans protection des données personnelles »*, 28 mars 2017, En ligne: <http://www.zdnet.fr/actualites/cnil-pas-d-innovation-sans-protection-des-donnees-personnelles-39850464.htm> (dernière consultation: 5 mars 2018)
- **Site de l'AFNOR**: <https://www.afnor.org/>
 - Et spécialement: **AFNOR**, *Guide protection des données personnelles - l'apport des normes volontaires*, Janvier 2017, En ligne: https://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf (dernière consultation: 5 mars 2018)
- **Site des BigBrotherAwards / Privacy France**: <http://bigbrotherawards.eu.org>
 - **GIXEL**, *Livre Bleu - Grands programmes structurants - Propositions des industries électroniques et numériques*, Juillet 2004, En ligne: http://bigbrotherawards.eu.org/IMG/pdf/Livre_bleu.pdf (dernière consultation: 5 mars 2018)
- **Site du cabinet international de conseil en management et en stratégie Boston Consulting Group**: <https://www.bcg.com/fr-fr/default.aspx>
 - Et spécialement: **The Boston Consulting Group**, *The value of our digital identity*, Liberty Global Policy Series, Novembre 2012 <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf> (dernière consultation: 5 mars 2018)
- **Site de la chaîne américaine d'informations CNN**: <http://edition.cnn.com>
 - Et spécialement: **WESTHOVEN Jennifer**, *CNET: We've been blackballed by Google*, CNN, 5 août 2005, En ligne: http://money.cnn.com/2005/08/05/technology/google_cnet/

(dernière consultation: 5 mars 2018)

- **Site de la CNIL:** <http://www.cnil.fr/>

- *Infographie résumant les procédures de blocage de sites internet pour des contenus faisant l'apologie du terrorisme, provoquant à acte terroriste, ou à caractère pédopornographique*, En ligne: <https://www.cnil.fr/fr/infographie-la-procedure-de-blocage-des-sites-internet> (dernière consultation: 5 mars 2018)

- *Infographie concernant les grands fichiers en fiche - le Système d'immatriculation des véhicules*: <https://www.cnil.fr/fr/siv-systeme-dimmatriculation-des-vehicules-0> (dernière consultation: 5 mars 2018)

- *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes*, 2 août 2007, <https://www.cnil.fr/fr/ladresse-ip-est-une-donnee-caractere-personnel-pour-lensemble-des-cnil-europeennes> (dernière consultation: 5 mars 2018)

- *Les principes clés de la protection des données personnelles*, Infographie, <https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles> (dernière consultation: 5 mars 2018)

- *PIA, La méthode - Etude d'impact sur la vie privée (EIVP), Privacy Impact Assessment (PIA) - Comment mener une EIVP, un PIA - Contexte, mesures, risques décision*, Edition 2015, <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf> (dernière consultation: 5 mars 2018)

- *Statistiques ethniques, quel cadre légal ?*, 7 mai 2015, <https://www.cnil.fr/en/node/15780> (dernière consultation: 5 mars 2018)

- *Mesure de fréquentation et analyse du comportement des consommateurs dans les magasins*, 19 août 2014, <https://www.cnil.fr/fr/mesure-de-frequentation-et-analyse-du-comportement-des-consommateurs-dans-les-magasins> (dernière consultation: 5 mars 2018)

- **Site de la Commission européenne:** http://ec.europa.eu/index_fr.htm

- Et spécialement la page dédiée à l'unité de prospective et d'analyse comportementale: <https://ec.europa.eu/jrc/en/research/crosscutting-activities/behavioural-insights> (dernière consultation: 5 mars 2018)

- **Site de la documentation française:** <http://www.ladocumentationfrancaise.fr>

- **Site de l'Electronic Frontier Foundation:** <https://www EFF.org/fr>

- Et spécialement: **OPSAHL Kurt**, *Facebook's erodind privacy policy: a timeline*, EFF, 28 avril 2010, En ligne: <https://www EFF.org/deeplinks/2010/04/facebook-timeline/> (dernière consultation: 5 mars 2018)

- **Site de la Fondation pour l'innovation politique, Fondapol:** <http://www.fondapol.org>
 - Et spécialement: **ABERKANE Idriss**, *La noopolitique: le pouvoir de la connaissance*, Fondation pour l'innovation politique, novembre 2015, En ligne: <http://www.fondapol.org/etude/idriss-j-aberkane-la-noopolitique-le-pouvoir-de-la-connaissance/> (dernière consultation: 5 mars 2018)
- **Site de Forbes:** <http://www.forbes.com>
 - Spécialement: **ROTELLA Perry**, *Is Data the new oil ?*, 4 février 2012, <http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/> (dernière consultation: 5 mars 2018)
- **Site de France Culture:** <https://www.franceculture.fr>
 - et spécialement: **ROPERT Pierre**, *Interview d'Alain Damasio à l'occasion du 30^{ème} anniversaire de la mort de Michel Foucault dans le cadre d'un dossier relatif à la société de surveillance de Foucault*, France Culture, 13 juin 2016, En ligne: <https://www.franceculture.fr/philosophie/la-societe-de-surveillance-de-foucault> (dernière consultation: 5 mars 2018)
- **Site de France info:** <https://www.francetvinfo.fr/>
 - Et plus particulièrement: *Extrait de « Razzia sur le bois » une enquête de Cash Investigation*, diffusée le 24 janvier 2017 à 20h55 sur France 2, En ligne: https://www.francetvinfo.fr/france/video-cash-investigation-des-labels-en-bois_2012290.html (dernière consultation: 5 mars 2018)
- **Site du gouvernement français relatif au projet de loi sur le renseignement:** <http://www.gouvernement.fr/le-vraifaux-du-gouvernement-sur-le-pjlrenseignement> (dernière consultation: 5 mars 2018)
- **Site de l'accès au droit de l'Union européenne:** <http://eur-lex.europa.eu/homepage.html>
- **Site de l'INA:** <http://www.ina.fr/>
 - *Journal télévisé de 20h00 d'Antenne 2, du 15 juillet 1976* <http://www.ina.fr/video/CAB7600764601/informatique-et-liberte-rossi-video.html> (dernière consultation: 5 mars 2018)
 - *Journal télévisé de 20h00 de TF1, du 18 février 1976, à propos de l'affaire Patrick Henri, « La France a peur »*, <http://www.ina.fr/video/CAA87014358> (dernière consultation: 5 mars 2018)
 - *L'information et l'UNESCO, Journal télévisé de 20h, 22 novembre 1978, TF1*, <http://www.ina.fr/video/CAA7801810101/l-information-et-l-unesco-video.html> (dernière

consultation: 5 mars 2018)

- *Présentation du rapport Nora-Minc sur l'informatisation de la société par Roger Gicquel, suivi d'un reportage consacré à la télématique et ses différentes implications par François de Closets*, le 19 mai 1978, TF 1, archive de l'INA, En ligne: <http://www.ina.fr/video/CAA7800628501/informatique-rapport-nora-video.html> (dernière consultation: 5 mars 2018)

- **Site de l'INRIA**: <http://www.inria.fr/>

- **Site du journal Le Figaro**: <http://www.lefigaro.fr>

- **D'ALMEIDA Pierre**, *Google est-il capable de truquer une élection ?*, Le Figaro, 2 septembre 2015, Disponible en ligne à l'adresse suivante: <http://www.lefigaro.fr/secteur/high-tech/2015/09/02/32001-20150902ARTFIG00091-google-est-il-capable-de-truquer-une-election.php> (dernière consultation: 5 mars 2018)

- **KOENIG Gaspard**, *Quand Ebola relance le débat sur le principe de précaution*, Figaro Vox, Vox Monde, 11 août 2014, En ligne: <http://www.lefigaro.fr/vox/monde/2014/08/11/31002-20140811ARTFIG00111-quand-ebola-relance-le-debat-sur-le-principe-de-precaution.php> (dernière consultation: 5 mars 2018)

- **LECLERC Jean-Marc**, *Vidéosurveillance: le rapport qui prouve son efficacité*, Le Figaro, 21 août 2009, Disponible en ligne à l'adresse suivante: <http://www.lefigaro.fr/actualite-france/2009/08/21/01016-20090821ARTFIG00361-videosurveillance-le-rapport-qui-prouve-son-efficacite-.php> (dernière consultation: 5 mars 2018)

- **ROY Soline**, *Si Pokemon GO ne vous tue pas, il vous rendra (un peu) plus fort*, Le Figaro, 25 août 2016, En ligne: <http://sante.lefigaro.fr/actualite/2016/08/25/25326-si-pokemon-go-ne-vous-tue-pas-il-vous-rendra-peu-plus-fort> (dernière consultation: 5 mars 2018)

- **Site du journal Le Monde** :<http://www.lemonde.fr/>

- **ARSENE Séverine**, *La Chine nouveau laboratoire du contrôle social de la population*, Le Monde, 26 octobre 2017, p. 2

- **CASSIN Barbara**, *Sarkosy « m'à tuer »*, Le Monde, 28 février 2009, mis à jour le 2 Mars 2009, http://www.lemonde.fr/idees/article/2009/02/28/sarkosy-m-a-tuer-par-barbara-cassin_1161665_3232.html (dernière consultation: 5 mars 2018)

- **CLAIROUIN Olivier**, *Il y a un vrai Prism à la française*, Le Monde, 4 Juillet 2013, En ligne: http://www.lemonde.fr/societe/video/2013/07/04/il-y-a-un-vrai-prism-a-la-francaise_3441637_3224.html (dernière consultation: 5 mars 2018)

- **DELMAS-MARTY Mireille**, *Au néoprottestantisme, on préférerait l' « esprit*

- protestataire* », Le Monde, 29 août 2017, En ligne: http://www.lemonde.fr/idees/article/2017/08/29/mireille-delmas-marty-au-neoprotestantisme-de-regis-debray-on-prefererait-l-esprit-protestataire_5177870_3232.html (dernière consultation: 5 mars 2018)
- **FOLLOROU Jacques, JOHANNES Franck**, *Révélation sur le Big Brother français*, Le Monde, 4 Juillet 2013, En ligne: http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (dernière consultation: 5 mars 2018)
 - **JACQUIN Jean-Baptiste**, *Ce que des juristes reprochent au projet de loi de sortie de l'état d'urgence*, Le Monde, 18 juillet 2017, En ligne: http://www.lemonde.fr/police-justice/article/2017/07/18/des-juristes-vent-debout-contre-le-projet-de-loi-de-sortie-de-l-etat-d-urgence_5161786_1653578.html (dernière consultation: 5 mars 2018)
 - *SAFARI ou la chasse aux Français*, Le Monde, 21 mars 1974, http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg (dernière consultation: 5 mars 2018)
 - **SZADKOWSKI Michaël, LELOUP Damien**, *Prism, Snowden, surveillance: 7 questions pour tout comprendre*, Le Monde, 2 juillet 2013, En ligne: http://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html (dernière consultation: 5 mars 2018)
 - **VIDBERG Martin, CLAIROUIN Olivier**, *Comment les métadonnées permettent de vous surveiller (expliqué en patates)*, Lemonde.fr, 15 juin 2015, En ligne: http://www.lemonde.fr/pixels/video/2015/06/15/comment-les-metadonnees-permettent-de-vous-surveiller-explique-en-patates_4654461_4408996.html (dernière consultation: 5 mars 2018)
 - **Site du journal Le Monde Informatique**: <http://www.lemondeinformatique.fr>
 - **DUNN John (E.)**, adapté par **ELYAN Jean**, *La sécurité absolue n'existe pas, retour sur 7 backdoors*, Le monde informatique, 2 février 2006, En ligne: <http://www.lemondeinformatique.fr/actualites/lire-la-securite-absolue-n-existe-pas-retour-sur-7-backdoors-63787.html> (dernière consultation: 5 mars 2018)
 - **PISANI Francis**, *La nouvelle plateforme Facebook : séduisante et dangereuse*, 4 mai 2010, Le Monde, En ligne: <http://pisani.blog.lemonde.fr/2010/05/04/la-nouvelle-plateforme-facebook-seduisante-et-dangereuse/> (dernière consultation: 5 mars 2018)
 - **Site du journal LePoint**: www.lepoint.fr
 - **FOURMY Marc**, *Mark Zuckerberg s'offre un bout d'île à Hawaï*, Le Point, 3 octobre 2014, En ligne: http://www.lepoint.fr/people/mark-zuckerberg-s-offre-un-bout-d-ile-a-hawaii-03-10-2014-1869024_2116.php (dernière consultation: 5 mars 2018)

- **NEUER Laurence**, *Protection des données personnelles: ce règlement qui inquiète les entreprises - Le nouveau règlement européen expose les entreprises et acteurs du Net à de lourdes sanctions financières. Quels en sont les enjeux ? Comment s'y préparer ?*, LePoint.fr, 8 février 2018, En ligne: http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/protection-des-donnees-personnelles-ce-reglement-qui-inquiete-les-entreprises-08-02-2018-2193245_56.php (dernière consultation: 5 mars 2018)
- **Site du journal les Echos**: <http://www.lesechos.fr>
 - *Bercy : du « data mining » pour lutter contre la fraude fiscale des entreprises*, 2014, En ligne: http://m.lesechos.fr/redirect_article.php?id=021365257320&fw=1 (dernière consultation: 5 mars 2018)
 - **FAY Pierrick**, *Apple, Amazon, Google et Facebook plus forts que le CAC 40*, 20 février 2015, En ligne: http://www.lesechos.fr/20/02/2015/lesechos.fr/0204174102171_apple--amazon--google-et-facebook-plus-forts-que-le-cac-40.htm# (dernière consultation: 5 mars 2018)
 - Interview, *Isabelle Falque-Pierrotin: « ceux qui pensent être propriétaires de nos données se trompent »*, 25 novembre 2014, En ligne: https://www.lesechos.fr/25/11/2014/lesechos.fr/0203937716964_isabelle-falque-pierrotin-----ceux-qui-pensent-etre-proprietaires-de-nos-donnees-se-trompent--.htm (dernière consultation: 5 mars 2018)
 - **NIEDERCORN Frank**, *Les algorithmes, pour le meilleur ou le pire*, 10 Mai 2016, En ligne: https://www.lesechos.fr/10/05/2016/LesEchos/22188-045-ECH_les-algorithmes--pour-le-meilleur-ou-le-pire.htm (dernière consultation: 5 mars 2018)
- **Site du journal l'Express**: <http://www.lexpress.fr>
 - **ATTALI Jacques**, *Etre propriétaire de soi*, 18 Février 2013, L'express, En ligne: <http://blogs.lexpress.fr/attali/2013/02/18/etre-proprietaire-de-soi/> (dernière consultation: 5 mars 2018)
 - **DE LA BROSSE Julie**, *Paul Duan, ce petit génie qui a élaboré un algorithme anti-chômage*, 25 février 2016, L'Express, En ligne: https://www.lexpress.fr/emploi/paul-duan-ce-petit-genie-qui-a-elabore-un-algorithme-antichomage_1766940.html (dernière consultation: 5 mars 2018)
 - **LAZARD Jean-Marc**, *L'Europe régleme l'utilisation des données: une révolution à venir*, L'express, 20 Mars 2017, En ligne: https://lexpansion.lexpress.fr/actualite/reglement-general-sur-la-protection-des-donnees-une-revolution-imminente-a-l-echelle-europeenne_1890897.html (dernière consultation: 5 mars 2018)

- **SIGNORET Perrine**, *Comment le centre commercial des quatre temps a traqué ses visiteurs ?*, L'Express, 15 juillet 2017, En ligne: http://lexpansion.lexpress.fr/high-tech/comment-le-centre-commercial-des-quatre-temps-a-traque-ses-visiteurs_1927269.html (dernière consultation: 5 mars 2018)
- **Site du journal Libération**: <http://www.liberation.fr>
 - **DELMAS-MARTY Mireille**, *De l'état d'urgence au despotisme doux*, Libération, 16 juillet 2017, En ligne: http://www.liberation.fr/debats/2017/07/16/de-l-etat-d-urgence-au-despotisme-doux_1584185 (dernière consultation: 5 mars 2018)
 - **ROUVROY Antoinette**, « Quand les algorithmes décident à notre place », *Libération*, 10 avril 2014, En ligne: http://www.liberation.fr/evenements-libe/2014/04/10/quand-les-algorithmes-decident-a-notre-place_994175 (dernière consultation: 5 mars 2018)
- **Site du journal Médiapart**: <https://www.mediapart.fr/>
 - Et spécialement: **LELIEVRE Claude**, *Le numérique à l'école: une (vieille) affaire présidentielle ?*, 10 novembre 2014, Médiapart, En ligne: <https://blogs.mediapart.fr/claude-lelievre/blog/101114/le-numerique-lecole-une-vieille-affaire-presidentielle> (dernière consultation: 5 mars 2018)
- **Site du journal Nord Eclair**: <http://www.nordeclair.be>
- **Site du journal NouvelObs - Rue 89**: <http://tempsreel.nouvelobs.com/rue89/>
 - **FRADIN Andréa**, « *La sécurité est la première des libertés. » Ou l'inverse?*, NouvelObs, Rue 89, 19 novembre 2015, En ligne: <http://tempsreel.nouvelobs.com/rue89/rue89-politique/20151119.RUE8786/la-securite-est-la-premiere-des-libertes-ou-l-inverse.html> (dernière consultation: 5 mars 2018)
- **Site du journal anglais The independent**: <http://www.independent.co.uk>
 - et spécialement: **HAWKING Stephen, RUSSELL Stuart, TEGMARK Max, WILCZEK Frank**, *Stephen Hawking: Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough ?*, The Independent, 1er Mai 2014, Disponible en ligne à l'adresse suivante: <http://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence-but-are-we-taking-9313474.html> (dernière consultation: 5 mars 2018)
- **Site du journal The Guardian**: www.theguardian.com
 - **JOHNSON Bobbie**, *Privacy no longer a social norm, says Facebook founder*, The Guardian, 11 janvier 2010, En ligne: <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> (dernière consultation: 5 mars 2018)

- **MOROZOV Evgeny**, *The rise of data and the death of politics*, 20 juillet 2014, En ligne: <https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation> (dernière consultation: 5 mars 2018), ou pour une traduction: « La prise de pouvoir des données et la mort de la politique », article paru dans *The Guardian*, 20 juillet 2014, traduit par Guy Weet et republié par Paul Jorion, En ligne: <http://www.pauljorion.com/blog/2014/08/25/la-prise-de-pouvoir-par-les-donnees-et-la-mort-de-la-politique-par-evgeny-morozov/> (dernière consultation: 5 mars 2018)
- **Site du journal Washington Post**: www.washingtonpost.com
 - et spécialement sa page dédiée à l'affaire du Watergate : <http://www.washingtonpost.com/wp-srv/politics/special/watergate/>
- **Site du journaliste d'investigation, spécialiste du réseau Échelon Duncan Campbell** : <http://www.duncancampbell.org/content/echelon>
 - Spécialement: *Somebody's listening – They've got it taped*, The New Statesman, 12 août 1988, En ligne : <http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf> (dernière consultation: 5 mars 2018)
- **Site de legifrance** : www.legifrance.gouv.fr
- **Site de la ligue des droits de l'Homme**: <http://www.ldh-france.org>
 - **Ligue des Droits de l'Homme**, *Résolution adoptée lors du 85ème congrès de la LDH - Société de surveillance, vie privée et libertés*, En ligne: http://www.ldh-france.org/IMG/pdf/Resolution_Societe_de_surveillance_-_85eme_congres_def_.pdf (dernière consultation: 5 mars 2018)
- **Site de l'Université de Harvard**: <https://www.harvard.edu/>
 - Et spécialement: **Harvard University Privacy Tools Project**, *Differential Privacy, What is differential privacy ?*, En ligne : <https://privacytools.seas.harvard.edu/differential-privacy> (dernière consultation: 5 mars 2018)
- **Site du magazine et blog boingboing**: <http://boingboing.net>
 - Et spécialement: **DOCTOROW Cory**, *Google CEO Says privacy doesn't matter: google blacklists CNet for violating CEO's privacy*, 9 décembre 2009, En ligne: <http://boingboing.net/2009/12/09/google-ceo-says-priv.html> (dernière consultation: 5 mars 2018)
- **Site du magazine Comment ça marche**: <http://www.commentcamarche.net>
 - Et spécialement: *L'open-graph de Facebook (qui) distribue les données privées des utilisateurs*, du 17 janvier 2011, En ligne: <http://www.commentcamarche.net/news/>

[5853945-l-open-graph-de-facebook-distribue-les-donnees-privées-des-utilisateurs](#) (dernière consultation: 5 mars 2018)

- **Site du magazine Développez:** <http://magazine.developpez.com>

- **GUILLOUX Michael**, *Geofeedia a surveillé les utilisateurs de Twitter, Facebook et Instagram pour la police - la start-up avait un accès commercial à leurs données*, 12 octobre 2016, En ligne: <https://www.developpez.com/actu/105233/Geofeedia-a-surveille-les-utilisateurs-de-Twitter-Facebook-et-Instagram-pour-la-police-la-startup-avait-un-acces-commercial-a-leurs-donnees/> (dernière consultation: 5 mars 2018)

- **MICHEL Claude**, *Un hacker réussit à contourner la sécurité d'une arme à feu intelligente - Et déclencher un tir sans autorisation*, 31 Juillet 2017, En ligne: <https://www.developpez.com/actu/152306/Un-hacker-reussit-a-contourner-la-securite-d-une-arme-a-feu-intelligente-et-declencher-un-tir-sans-autorisation/> (dernière consultation: 5 mars 2018)

- **Site du magazine NewYork Mag:** www.nymag.com

- Et spécialement: **AMIRA Dan**, *Inside Google Chairman Eric Schmidt's Lavish Sex Palace*, Daily Intelligencer, 25 juillet 2013, En ligne: <http://nymag.com/daily/intelligencer/2013/07/eric-schmidt-penthouse-new-york-photos-apartment.html> (dernière consultation: 5 mars 2018)

- **Site du magazine Sciences et avenir:** <https://www.sciencesetavenir.fr>

- **CHAUVEAU Loïc**, *Les géologues du monde entier sont à la recherche du clou d'or*, Sciences et avenir, 1er Septembre 2016, En ligne: https://www.sciencesetavenir.fr/fondamental/geologie/les-geologues-du-monde-entier-sont-a-la-recherche-du-clou-d-or_104313 (dernière consultation: 5 mars 2018)

- **LOUME Lise**, *Transhumanisme: Nous risquons de provoquer une vague de déception*, Sciences et avenir, 15 avril 2016, En ligne: https://www.sciencesetavenir.fr/sante/cerveau-et-psy/transhumanisme-nous-risquons-de-provoquer-une-vague-de-deception_104399 (dernière consultation: 5 mars 2018)

- **SENDER Elena, François Berger**, *Le transhumanisme est un charlatanisme dangereux*, Sciences et avenir, 20 août 2016, En ligne: https://www.sciencesetavenir.fr/sante/cerveau-et-psy/francois-berger-le-transhumanisme-est-un-charlatanisme-dangereux_104462 (dernière consultation: 5 mars 2018)

- **SERMONDADAZ Sarah, Bernard Stiegler**, *Le transhumanisme, un néodarwinisme dangereux*, Sciences et avenir, 14 décembre 2016, En ligne: https://www.sciencesetavenir.fr/sante/cerveau-et-psy/sermondadaz-sarah-bernard-stiegler-le-transhumanisme-un-neodarwinisme-dangereux_104462

www.sciencesetavenir.fr/high-tech/le-transhumanisme-est-un-neodarwinisme-dangereux-avertit-bernard-stiegler_108864 (dernière consultation: 5 mars 2018)

- **Site du magazine en ligne Slate:** <http://www.slate.fr>

- **MASIMBERT Maïlys**, *Quand les ados menacent l'anonymat du e-commerce de la drogue*, Slate, 7 septembre 2013, En ligne: <http://www.slate.fr/monde/77682/ados-anonymat-web-droque-silk-road> (dernière consultation: 5 mars 2018)

- **Site du magazine Wired:** <https://www.wired.com/>

- Et spécialement: **GREENBERG Andy**, *Apple's « differential privacy » is about collecting your data - but not your data*, Wired, 13 juin 2016, En ligne: <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/> (dernière consultation: 5 mars 2018)

- **Site de Monsieur le Professeur Gilles Guglielmi:** <https://www.guglielmi.fr>

- Et spécialement: **GUGLIELMI Gilles**, « *Homo numericus* », *un citoyen digitalisé et numérisé conscientisé*, 10 Juin 2009, En ligne: <https://www.guglielmi.fr/spip.php?article199#nh2> (dernière consultation: 5 mars 2018)

- **Site du mensuel Le Monde diplomatique :** <https://www.monde-diplomatique.fr/>

- **Borradori Giovanna**, *Entretiens avec deux grands intellectuels sur le « concept » du 11 septembre 2001 - qu'est ce que le terrorisme ?*, Le Monde diplomatique, Février 2004, p. 16, En ligne : <https://www.monde-diplomatique.fr/2004/02/DERRIDA/11005> (dernière consultation: 5 mars 2018)

- **BOURDIEU Pierre**, *L'essence du néolibéralisme*, Le Monde diplomatique, Mars 1998, p. 3, En ligne: <http://www.monde-diplomatique.fr/1998/03/BOURDIEU/3609> (dernière consultation: 5 mars 2018)

- **COOLSAET Rick**, *Au temps du terrorisme anarchiste*, Le Monde diplomatique, septembre 2004, En ligne: <https://www.monde-diplomatique.fr/2004/09/COOLSAET/11443> (dernière consultation: 5 mars 2018)

- **MOROZOV Evgeny**, *Noces du Numérique et de l'austérité - Résister à l'uberisation du monde*, Le Monde Diplomatique, Septembre 2015, pp. 1 et 22, En ligne <https://www.monde-diplomatique.fr/2015/09/MOROZOV/53676> (dernière consultation: 5 mars 2018)

- **RAMONET Ignacio**, *Les nouvelles armes du contrôle social - Citoyens sous surveillance*, Le Monde Diplomatique, Mai 1994, pages 15 et 20, En ligne: <http://www.monde-diplomatique.fr/1994/05/RAMONET/46012> (dernière consultation: 5 mars 2018)

- **SCHILLER Herbert**, *La communication , une affaire d'Etat pour Washington. Cinquante*

- ans d'horreur médiatique*, in Le Monde Diplomatique, 521, août 1997, Paris pp. 20-21 - En ligne: <http://www.monde-diplomatique.fr/1997/08/SCHILLER/4900> (dernière consultation: 5 mars 2018); *Vers un nouveau siècle d'impérialisme américain - Dominer l'ère électronique*, in Le Monde Diplomatique, 533, août 1998, Paris, pp. 1, 18 et 19 - En ligne: <http://www.monde-diplomatique.fr/1998/08/SCHILLER/3927> (dernière consultation: 5 mars 2018); *Décervelage à l'américaine - La fabrique des maîtres*, Le Monde Diplomatique, 545, août 1999, Paris, p.15 - En ligne: <http://www.monde-diplomatique.fr/1999/08/SCHILLER/3231> (dernière consultation: 5 mars 2018)
- **SOUCHIER Emmanuel, JEANNERET Yves**, *Publicité et mensonges*, in. Le Monde Diplomatique, *Médias et contrôle des esprits*, Manière de voir, n° 27, Août - Septembre - Octobre 1995, En ligne: <http://www.monde-diplomatique.fr/mav/27/> (dernière consultation: 5 mars 2018)
 - **Site du ministère de la Défense** : www.defense.gouv.fr
 - **Site du ministère de l'Intérieur**: <http://www.interieur.gouv.fr>
 - et spécialement: **Communiqué du Ministère de l'Intérieur**, *Expérimentation des voitures-radar conduites sous le contrôle l'Etat, par des opérateurs privés*, 20 février 2017, En ligne: <http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Experimentation-des-voitures-radar-conduites-sous-le-controle-de-l-Etat-par-des-operateurs-privés> (dernière consultation: 5 mars 2018)
 - **Site de l'Organisation de Coopération et de Développement Economiques (OCDE)**: <http://www.oecd.org/fr/>
 - Et spécialement sa page consacrée aux recherches et études en cours concernant le fait de mesurer le bien être et le progrès: <http://www.oecd.org/fr/statistiques/mesurer-bien-etre-et-progres.htm> (dernière consultation: 5 mars 2018)
 - **Site de l'Organisation Internationale de Normalisation (ISO)**: <https://www.iso.org/fr/home.html>
 - Et spécialement: <https://www.iso.org/fr/standard/29280.html> (dernière consultation: 5 mars 2018), <https://www.iso.org/fr/standard/45481.html> (dernière consultation: 5 mars 2018)
 - **Site du portail e-santé**: <http://esante.gouv.fr>
 - **Site du portail de l'union européenne** :http://europa.eu/index_fr
 - Spécialement: **Commission européenne**, Communiqué de presse - *Etat de l'Union 2017 : un cadre pour la libre circulation des données à caractère non personnel dans l'Union européenne*, Bruxelles, 19 septembre 2017, En ligne: <http://europa.eu/rapid/press->

[release_IP-17-3190_fr.htm](#) (dernière consultation: 5 mars 2018)

- **Site du portail de statistique:** <https://fr.statista.com/>
 - Et spécialement: <https://fr.statista.com/statistiques/664257/francais-preoccupation-collecte-donnees-internet/> (dernière consultation: 5 mars 2018)
- **Site de la Préfecture de Police:** <http://www.prefecturedepolice.interieur.gouv.fr>
- **Site du Président de la République fédérale d'Allemagne :** http://www.bundespraesident.de/DE/Home/home_node.html
- **Site de Privacy international :**<http://www.privacyinternational.org/>
- **Site du Privacy Shield:** <https://www.privacyshield.gov/welcome>
- **Site Radio France Inter:** <https://www.franceinter.fr>
 - Et spécialement: **REBEIHI Ali**, *Quand la publicité alimentaire nous raconte des histoires*, France Inter, 3 Mai 2017, En ligne: <https://www.franceinter.fr/emissions/grand-bien-vous-fasse/grand-bien-vous-fasse-03-mai-2017> (dernière consultation: 5 mars 2018)
- **Site de recueil de poésie :** <http://poesie.webnet.fr/lesgrandsclassiques/index.html>
- **Site du Réseau Etudes Digitales** lancé par l'Institut de Recherche et d'Innovation: <https://digital-studies.org/wp/fr/>
 - Et spécialement: **ROUVROY Antoinette, STIEGLER Bernard**, *Séminaire Digital Studies, Deuxième Séance, Institut de recherche et d'innovation, Paris, 7 octobre 2014*, Compte rendu disponible en ligne à l'adresse suivante: <https://digital-studies.org/wp/seminaire-digital-studies-antoinette-rouvroy-et-bernard-stiegler-paris-07102014/?lang=fr> (dernière consultation: 5 mars 2018)
- **Site de Reuters:** www.reuters.com
 - Et spécialement: **CHAR Pravin**, *Europe seeks power to seize overseas data in challenge to tech giants*, 26 février 2018, Reuters, Disponible en ligne à l'adresse suivante: https://www.reuters.com/article/us-eu-data-order/europe-seeks-power-to-seize-overseas-data-in-challenge-to-tech-giants-idUSKCN1GA0LP?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29 (dernière consultation: 5 mars 2018)
- **Site du Safe Harbor :** <http://www.export.gov/safeharbor/>
- **Site du Sénat:** www.senat.fr
- **Site de la société APPLE:** <http://www.apple.com/fr/>
 - et spécialement: <https://www.apple.com/hk/en/iphone/business/profiles/mayo-clinic/>

(dernière consultation: 5 mars 2018)

- **Site de la Tribune** : www.latribune.fr
 - **BOYER Philippe**, *De l'influence du Big data sur les élections américaines*, La Tribune, 25 février 2016, En ligne: <https://www.latribune.fr/opinions/tribunes/de-l-influence-du-big-data-sur-les-elections-americales-553346.html> (dernière consultation: 5 mars 2018)
 - **CUNY Delphine**, *Big Data is Big Business vraiment*, La Tribune, 3 avril 2013, <http://www.latribune.fr/technos-medias/internet/20130403trib000757290/-big-data-is-big-business.-vraiment-.html> (dernière consultation: 5 mars 2018)
 - **NORMAND Grégory**, *Wikileaks: cinq choses à savoir sur la surveillance de la CIA*, La Tribune, 8 mars 2017, En ligne: <http://www.latribune.fr/economie/international/wikileaks-cinq-choses-a-savoir-sur-la-surveillance-de-la-cia-656436.html> (dernière consultation: 5 mars 2018)
- **Site de Wikileaks**: <https://wikileaks.org>
 - *Darkmatter*, 23 Mars 2017, En ligne: <https://wikileaks.org/vault7/darkmatter/> (dernière consultation: 5 mars 2018)
- **Site de YouTube (contenu vidéo en ligne)**: www.youtube.com
 - **MEILLASSOUX Marc**, *Nothing to Hide*, Film Documentaire, 2017, En ligne: https://www.youtube.com/watch?time_continue=385&v=djwzEIV7gE (dernière consultation: 5 mars 2018)
 - **SCHMIDT Eric**, PDG de Gogle, à propos de la vie privée, interview donnée à la chaîne CNBC, En ligne: <https://www.youtube.com/watch?v=A6e7wFDHzew> (dernière consultation: 5 mars 2018)

Table des annexes

Annexe 1:

Naissance et chronologie des lois « informatiques et libertés » en Europe et à l'international dans les années 70 - 80

Annexe 2:

Démarche détaillée pour mener un Privacy Impact Assessment

Annexe 3:

La Démarche PSSI

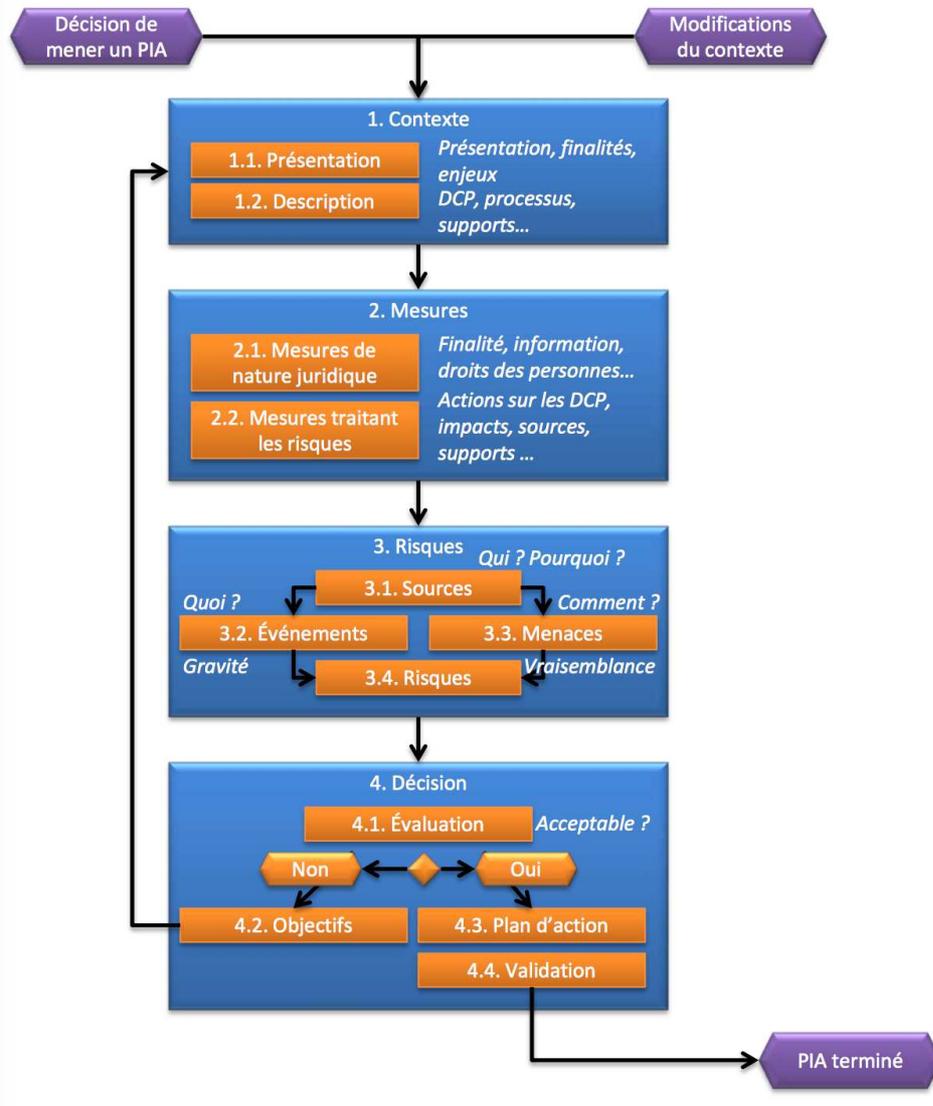
Annexe 1

**Naissance et chronologie des lois « informatiques et libertés »
en Europe et à l'international dans les années 70 - 80**

Land de HESSE (R.F.A.)	Loi sur la Protection des données	7.10.1970
ALLEMAGNE	Bundesdatenschutzgesetz	27.01.1977
ANGLETERRE	Data Protection Act	11.11.1984
AUSTRALIE		1988
AUTRICHE	Datenschutzgesetz	18.10.1978
	Austrian Data Protection Act	1.07.1987
CANADA	Loi sur la protection des renseignements personnels	
	Loi sur l'accès aux documents	7.07.1982
DANEMARK	Danish Private Registers etc. Act n°293	08.06.1978
	Danish Public Authorities' Registers Act n°294	
	(amendée le 1.04.1988)	
FINLANDE	Personal Data File Act & Personal Data File Decree	30.04.1987
FRANCE	Loi n°78-17, Informatique et Libertés	6.1.1978
HOLLANDE	Wet Personenregistraties	28.12.1988
HONGRIE	Data protection and freedom of information bill	(projet de loi)
IRLANDE	Data Protection Act	13.07.1988
ISLANDE	Loi sur la collecte systématique de données personnelles	25.05.1981
	Loi sur la protection des données	1.06.1986
JAPAN	Act for Protection of Computer Processed Personal Data Held by Administrative Organs	16.12.1988
LUXEMBOURG	Loi réglementant l'utilisation des données nominatives dans les traitements informatiques	31.03.1979
NORVÈGE	Act relating to Personal Data Registers etc.	9.06.1978
SUEDE	Data Act	11.05.1973
	(amendé le 1.07.1979 & 1.07.1982)	
U.S.A.	Data Act (Public Law 93-579, 93rd Congress, S. 3418)	31.12.1974
	+ Loi sur la criminalité informatique	1986
Conseil de l'Europe	Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n°108)	16.1.1981
O.C.D.E.	Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel	23.09.1980

Annexe 2

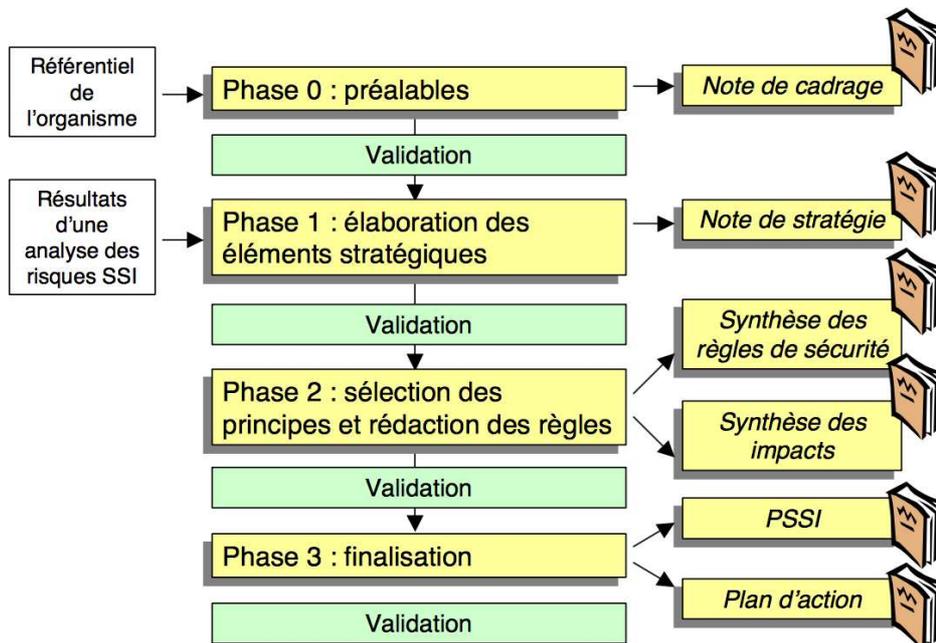
Démarche détaillée pour mener un PIA



(Source: CNIL, PIA, La méthode - Etude d'impact sur la vie privée (EIVP), Privacy Impact Assessment (PIA) - Comment mener une EIVP, un PIA - Contexte, mesures, risques décision, Edition 2015, Disponible en ligne à l'adresse suivante: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf>, p.8)

Annexe 3

La Démarche PSSI



Source: Premier Ministre, SGDSN, Direction centrale de la sécurité des systèmes d'information, sous direction des opérations, bureau conseil, Guide pour l'élaboration d'une politique de sécurité de système d'information (PSSI) -Section 2 Méthodologie, version du 3 mars 2004, p.6, disponible en ligne à l'adresse suivante: <https://www.ssi.gouv.fr/uploads/IMG/pdf/pssi-section2-methodologie-2004-03-03.pdf>

Index des principaux auteurs

A.

AGAMBEN Giorgio: 419, 440, 471

AMSELEK Paul: 84, 471

AUBERT Nicole: 233, 234, 471, 484

AUBY Jean-Bernard: 396, 483

B.

BAUMAN Zygmunt: 430, 472

BAUSARDO Thomas: 67, 88, 484

BECK Ulrich: 61, 472

BENTHAM Jeremy: 11, 22, 53, 129, 193, 213-217, 222, 223, 233, 380-382, 401, 424, 425, 442, 446, 458, 465, 472, 486

BIGO Didier: 61, 472

BOUILLOUD Jean-Philippe: 233, 484

BOURDIEU Pierre: 232, 428, 434, 441, 472, 493, 537

BRETON Philippe: 44, 164, 165, 169, 472, 473

C.

CARBONNIER Jean: 413, 473

CASILI Antonio: 376

CASSIN Barbara: 141, 170, 473, 531

CATALA Pierre: 235, 237, 284, 354, 359, 361, 362, 367, 370, 473, 485

CHARBONNEAU Bernard: 27, 35, 473, 474

CHOMSKY Noam: 232, 441, 474

CITTON Yves: 433 - 435, 474, 485, 486

CONSTANT Benjamin: 30, 272, 474, 526

CORNU Marie: 363, 474

CREPON Marc: 143, 145, 474

D.

DANET Jean: 61, 485

DEBORD Guy: 426, 435, 474

DELEUZE Gilles: 22, 217 - 219, 353, 387, 427, 475, 485, 493

DELMAS-MARTY Mireille: 35, 88, 149, 155, 417, 424, 460, 475, 531, 534

E.

ELIAS Norbert: 441, 475

ELLUL Jacques: 11, 27, 71 - 73, 85, 87, 129, 137, 141, 145, 164, 170, 174, 184, 220, 221, 407, 465, 467, 474, 475

F.

FOREST David: 42, 100, 476, 493

FOUCAULT Michel: 22, 123, 124, 126, 142, 216, 234, 385 - 388, 399, 418, 424, 425, 428, 429, 431, 446, 451, 476

FRANCK Georg: 433, 486

FRAYSSINET Jean: 26, 83, 230, 245, 261, 356, 361, 486, 493

G.

GANASCIA Jean-Gabriel: 55, 176, 180, 402, 476

GAUTRAIS Vincent: 205 - 207, 476

GENTOT Michel: 82, 113, 487

H.

HABERMAS Jürgen: 395, 400, 477

HARDT Michel: 23, 477

HAVEL Vaclav: 143, 477

HEGEL Friedrich: 409, 477

HEIDEGGER Martin: 23, 66, 69 - 73, 137, 453, 477

HOBBS Thomas: 29, 48, 381, 382, 398, 402, 477

HUNYADI Mark: 229, 234, 487

J.

JAMIN Christophe: 372, 487

JERPHAGNON Lucien: 188, 493

K.

KESSOUS Emmanuel: 186, 434, 477
KITCHIN Rob: 404, 405, 487, 526
KYROU Ariel: 128, 130, 213, 223, 487

L.

LARRIERE Stéphane: 415, 488
LASCH Christopher: 184, 186, 189, 434, 477
LAVAL Christian: 356, 380 - 382, 410, 418, 420 - 422, 430, 431, 439, 458, 465, 488, 493
LAVENUE Jean-Jacques: 43, 130, 307, 308, 311, 312, 478, 488
LIANOS Michalis: 438 - 440, 442, 478
LIPPMANN Walter: 441, 478
LYON David: 42, 52 - 55, 63, 439, 453, 472, 478

M.

MACHIAVEL Nicolas: 139, 478
MATTELART Armand: 42, 102, 103, 105, 111, 114, 133, 149, 478, 479
MAZABRAUD Bertrand: 386, 419 - 422, 459, 489
MICHEA Jean-Claude: 43, 152, 153, 186, 407 - 411, 479
MOROZOV Evgeny: 85, 406, 412, 414 - 416, 463, 479, 535, 537
MULONE Massimiliano: 138, 150, 154, 489

N.

NYE Joseph: 13, 100, 101, 134 - 136, 139, 140, 479, 489, 525

O.

OCHOA Nicolas: 75, 83, 341, 483
ORSI Fabienne: 363, 372, 474, 489
OST François: 37, 39, 44, 45, 47, 444, 447, 448, 451 - 453, 460, 480

P.

PEUGEOT Valérie: 368, 373, 490

POLONY Natacha: 38, 480

PORQUET Jean-Luc: 71, 73, 480

POSTMAN Neil: 38, 39, 46, 466, 480

POTTE-BONNEVILLE Mathieu: 122, 123, 126, 127, 490

Q.

QUESSADA Dominique: 58, 59, 123, 490

R.

RAMONET Ignacio: 176, 537

RIESEL René: 152, 153, 480

RIGAUX François: 389, 390, 442, 443, 491

ROUSSEAU Jean-Jacques: 50, 396, 398, 442, 444, 480

ROUVROY Antoinette: 191, 192, 235, 322, 326, 327, 354, 355, 391, 392, 406, 446 - 448, 450 - 452, 456, 460, 461, 491, 534, 539

S.

SADIN Eric: 27, 34, 115, 122, 123, 130, 167, 168, 193, 219 - 222, 404, 429, 480, 490, 491

SCHILLER Herbert: 108, 480, 481, 511, 537

SCHUMPETER Joseph: 95, 415, 481

SENNETT Richard: 400, 401

SFEZ Lucien: 27, 49 - 51, 66, 481

SIMONE Raffaele: 43, 146, 425, 430, 481

SKINNER Burrhus: 170, 171, 481

SLOTEDIJK Peter: 23, 66, 432, 481

SOFSKY Wolfgang: 63, 175, 229, 398, 399, 401, 481

STIEGLER Bernard: 27, 36, 166, 167, 219, 389, 392, 406, 481, 539

SUPIOT Alain: 44, 45, 289, 291, 421, 422, 444 - 447, 481

T.

TARDE Gabriel: 66, 118, 230, 283, 382, 393, 434, 482

THOREAU Henri-David: 70, 406, 413, 482

TOCQUEVILLE Alexis: 43, 145, 152, 411, 425, 430, 465, 475

TOSEL André: 9, 10, 416 - 418, 420, 421, 449, 450, 492

TURK Alex: 82, 133, 137, 176, 195 - 197, 205, 208, 212, 213, 276, 283, 436, 441, 482, 493, 525

V.

VAN ZOONEN Liesbet: 191, 263, 404, 492

VIAL Stéphane: 65, 84, 482

VION-DURY Philippe: 43, 431, 432, 452 - 454, 456, 482

W.

WARREN SAMUEL: 21, 398, 492

WEBER Max: 39, 54, 66, 75, 93 - 97, 99, 166, 230, 482

WEIL Simone: 70, 92 - 94, 483

WIENER Norbert: 101, 104, 105, 114, 164, 355, 483

Index des notions principales

A.

Acceptabilité: 175, 182, 232, 300, 429, 440, 483, 493

Accountability: 7, 158, 295, 296, 308, 310, 312, 485, 514

Administration: 48, 53, 54, 67, 75, 77 - 80, 97, 103, 147, 152, 157, 161, 170, 180, 195, 212, 261, 267, 304, 356, 364, 395, 403, 410, 443, 480, 517, 518, 520, 522, 525, 527

Adresse IP: 236 - 245, 252, 253, 255, 257, 263, 278, 340, 342, 345, 488, 528, 529

Agence Française de Normalisation (AFNOR): 17, 311 - 313, 528 1

Agence Nationale de Sécurité des Systèmes d'information (ANSSI): 303

Algorithme: 54, 57, 87, 121, 125, 196, 204, 221, 230, 280, 298, 343, 352, 404, 406, 412, 414, 415, 447, 453, 521, 522, 527, 533, 534

Anonymisation: 304, 306, 307, 342, 345, 347 - 353, 362, 404, 515

Anthropocène: 27, 30, 35, 36, 474

Anticipation: 43, 96, 155, 303, 356, 460

Appropriation: 63, 231, 354, 359, 361 - 366, 370, 375, 376, 401, 490

Attention: 42, 48, 49, 52 - 57, 108, 119, 124, 147, 176, 177, 179, 180, 182, 183, 185, 186, 188, 191, 235, 259, 301, 347, 369 - 371, 377, 378, 388, 395, 424, 425, 429, 430, 432 - 436, 438, 439, 442, 446, 449 - 451, 453, 458 - 460, 463, 474, 477, 485, 486

Autodétermination: 397

Autorité administrative indépendante: 197

B.

Banalisation: 39, 55, 57, 100, 101, 114, 115, 119, 121, 122, 129, 133, 134, 142, 147, 156, 164, 165, 172, 181, 189, 285, 382, 401, 441, 486

Bien commun: 233, 359, 363 - 365, 370 - 373, 376, 474, 489

Bien-être: 14, 15, 46, 92, 94, 98, 150, 260, 264, 266, 274, 277, 285, 288, 380, 382 - 385, 396, 405, 407 - 410, 417, 420, 422, 429, 430, 433, 449, 454, 457, 465 - 468, 476, 484, 485, 488, 489

Biométrie: 34, 120, 126, 129, 162, 181, 208 - 210, 259, 278, 349, 350, 353, 392

Biopouvoir: 235, 285, 380, 385 - 389, 392, 393, 405 - 407, 409, 420

Biopouvoir algorithmique: 235, 285, 380, 385, 386, 389, 392, 393, 405, 407, 409

C.

Charte des Droits fondamentaux: 277 - 279, 288, 321, 495

Commission nationale de l'informatique et des libertés (CNIL): 13, 17, 31, 34, 41, 42, 54, 59, 82, 100, 113, 114, 125, 185, 195, 197, 199, 202 - 204, 209 - 211, 241 - 244, 258, 259, 261, 263, 269, 276, 278, 283, 299 - 301, 312, 323, 343 - 350, 403, 436, 457, 483, 500, 509, 515, 519, 521, 528, 529, 543

Comportementalisme: 170, 450 - 453, 456, 463, 465, 491

Consentement: 58, 121, 145, 146, 182, 198, 201, 215, 232, 259, 261, 264, 277, 300, 313 - 321, 326, 365, 367, 368, 372, 405, 429, 438, 441, 474, 514

Contrôle social: 5, 11, 24, 41, 44, 47, 53, 57, 90, 128, 176, 213, 217, 219, 233, 234, 259, 377, 378, 392, 395, 401, 405, 423 - 436, 438 - 440, 442, 449 - 451, 453, 458 - 460, 463, 478, 531, 537

Contrôle social attentionnel: 57, 259, 449 - 451, 453, 458 - 460, 463

Convention Européenne des Droits de l'Homme: 98, 277

Convention STE: 199, 341, 494

Cour de Justice de l'Union Européenne (CJUE): 17, 239, 242, 243, 249, 251 - 253, 255 - 257, 259, 261, 266, 270, 280, 281, 327, 328, 345, 506, 528

Cour des Comptes: 91, 455 - 457, 522

Cour Européenne des Droits de l'Homme (CEDH): 17, 211, 212, 248, 250, 274, 275, 288, 505

Crise de la culture: 56, 164, 165, 170, 172, 174, 175, 183, 184, 186, 471

Culture de la peur: 89, 90, 143, 145, 147, 474

Culture du narcissisme: 165, 184, 186, 189, 428, 477

Cybernétique: 8, 101, 102, 104, 114, 416, 463, 477, 483

D.

Data-panoptisme: 193, 213, 214, 217, 219, 222, 223, 229, 380, 429, 431

Démocratie: 29, 38, 41 - 43, 48, 57, 61, 62, 93, 95, 97 - 99, 101, 129, 143 - 145, 159, 232, 291, 356, 382, 408, 412, 415, 417, 425, 441, 472, 474, 475, 481

Déshumanisation: 24, 89, 468

Dignité: 21, 45, 170, 171, 411, 433, 445, 461, 481

Domestication: 23, 29, 430, 432, 448, 481

Donnée personnelle (Droit des données personnelles): 5, 12, 13, 23, 25, 26, 30 - 32, 41, 42, 45, 48, 52, 55 - 58, 62, 69, 75, 78, 81 - 83, 86, 100, 106, 107, 111, 113, 119, 120, 122, 130, 168, 175, 176, 180, 181, 186, 189 - 195, 197, 198, 200, 201, 203, 205 - 207, 209, 213, 220, 223, 235 - 246, 248,

251, 255, 257, 258, 260 - 263, 266, 267, 269, 271 - 276, 279, 283, 284, 286 - 289, 291, 293, 295 - 297, 299, 300, 305 - 326, 328 - 331, 333 - 338, 340 - 342, 345 - 361, 363 - 368, 370 - 373, 375, 376, 379, 391, 397, 404, 417, 420, 423, 436, 457, 465, 467, 468, 477, 483, 487 - 491, 498, 510, 518, 520, 528, 529, 533

Donnée sensible: 248, 258, 315

Dressage: 149, 238, 244, 430, 431, 453

Droit à l'information: 105, 201, 202, 325, 360, 361

Droit-Créance: 155

Droit de la consommation: 365

Droit Libéral: 58, 407, 409, 411, 412, 416 - 422, 443

Droit Privé: 14, 420, 432, 438, 449, 475

Droit Public: 155, 365, 394, 397, 486, 490

Droit sur l'information: 360, 361

E.

Etat de droit: 24, 42, 155, 156, 409, 412, 413, 416 - 422, 449

Etat de droit libéral: 412, 416 - 421

Etude d'impact sur la vie privée: 299, 529, 543

F.

Fichier: 11, 19, 25, 26, 54, 59, 75 - 79, 82, 83, 86, 105, 107, 120, 175, 194 - 197, 199, 200, 212, 224, 239, 240, 243, 245, 246, 251, 252, 257 - 259, 263, 274, 306, 356, 367, 401, 413, 486, 500, 519, 520, 525, 527, 529

Fiction: 7, 22, 25, 27, 37 - 40, 43, 46, 47, 49 - 51, 66, 83, 102, 128, 218, 356, 393, 404, 416, 432, 445, 468, 474, 476, 487

Fiction instituante: 27, 37, 47, 49 - 51, 468

Fluidité: 189, 211, 377, 417, 421, 428, 438

Flux: 8, 26, 103, 104, 111, 112, 116, 167, 183, 222, 225, 261, 266, 267, 269, 289, 295, 328, 343, 344, 380, 382, 405, 413, 415, 417, 420, 511, 519

G.

Globalisation: 41, 42, 69, 100, 102, 107, 113, 114, 149, 233, 479

Gouvernance: 5, 43, 46, 96, 124, 138, 150, 153, 154, 259, 289, 291, 293, 295, 296, 306, 323, 331,

364, 384, 403, 405, 414, 422, 426, 430, 439, 443, 481, 488, 524

Gouvernementalité: 59, 134, 136, 142, 145 - 147, 152, 156, 175, 176, 182, 184, 189, 191, 232, 259, 285, 326, 354, 355, 382, 392, 409, 419, 420, 426 - 430, 448, 451, 467, 468, 491

Gouvernementalité algorithmique: 259, 326, 355, 392, 448, 451, 468, 491

Gouvernementalité par la peur: 134, 136, 142, 145 - 147, 152, 156, 175, 176, 182, 184, 189, 232, 382, 409, 427, 467

Groupe de l'Article 29: 248, 249, 321, 323, 324, 329 - 331, 348, 349

I.

Information: 8 - 11, 17 - 19, 23, 25, 26, 29 - 32, 34, 39 - 41, 44, 45, 48 - 50, 53 - 57, 63, 67, 68, 75 - 82, 86 - 89, 91, 92, 97, 100 - 122, 124, 130, 133, 135 - 138, 140, 141, 145, 148, 149, 151, 154, 155, 157, 161 - 174, 176 - 181, 186, 188, 189, 191, 193 - 195, 197 - 203, 205, 209 - 211, 213, 215 - 221, 223, 230 - 232, 235 - 241, 243, 244, 247 - 250, 254 - 256, 261 - 268, 270, 276, 278, 283, 285, 286, 288, 289, 300 - 307, 312, 316, 317, 319, 320, 325, 327, 329, 330, 334, 335, 339 - 341, 343, 347, 348, 351 - 365, 367, 369, 372, 375, 376, 379, 380, 391, 393, 397, 401 - 405, 412, 413, 415, 417, 420, 425, 433, 434, 436 - 438, 440, 442, 443, 449, 451, 455, 457, 467, 473, 478, 484 - 489, 491, 492, 497, 503, 510 - 512, 514, 515, 519, 520, 522 - 528, 530, 544

Infrastructure: 13, 111, 112, 115 - 118, 135, 137, 178, 302, 303, 392, 403, 510, 516

Interconnexion: 10, 31, 34, 57, 64, 86, 121, 145, 169, 195, 196, 198, 217, 224, 236, 252, 255, 283, 335, 405

Intérêt légitime: 314, 317, 319 - 321

Interopérabilité: 10, 64, 86, 121, 221, 255

Intrusivité: 133

ISO: 18, 225, 311 - 313, 348, 538

L.

Label - Labellisation: 311, 312, 329, 403, 530

Libéralisme: 111, 138, 153, 356, 377, 379 - 382, 388, 389, 394, 406 - 409, 411, 417, 420, 424, 426, 429, 431, 438, 441, 449, 453, 465, 468, 488, 537

Liberté d'expression: 8, 55, 105, 124, 125, 154, 207, 288, 397, 443, 450

Liberté de circulation: 8, 33, 57, 101, 106, 107, 111 - 115, 252, 266, 267, 278, 287, 291, 294, 314, 331, 333 - 342, 350, 351, 364, 366, 370, 375, 411, 417, 468, 496, 517, 538

M.

Marchandisation: 5, 113, 138, 148, 154, 156 - 158, 161, 163, 187, 189, 333, 335, 375, 401, 468, 489

Marché du numérique: 41, 120, 121, 134, 167, 191, 220, 221, 271, 285, 333, 338

Marché économique: 80, 83, 105 - 108, 112, 113, 115, 150, 177, 179, 218, 220, 232, 289, 331, 334, 338, 340, 351, 370, 380, 411, 415, 420, 424, 465

Métadonnée: 58, 236, 237, 246 - 252, 254 - 257, 263, 279 - 281, 340, 532

Métadroits: 322, 325, 326

Monstre Doux: 43, 130, 146, 390, 430, 465, 481, 488

Mythe: 37, 38, 44, 56, 133, 164, 165, 169, 177, 182, 188, 371, 429, 431, 436, 441, 449, 450, 472

N.

Narcisse: 133, 165, 177, 179, 182, 183, 185, 187 - 190, 449, 493

Nation: 50, 90, 93 - 101, 104 - 106, 108 - 111, 274 - 281, 383 - 385, 387, 395 - 400, 408, 409, 415 - 417, 458, 465

Neutralité technologique: 197, 205 - 208, 210, 211, 476

Normalisation: 17, 36, 39, 165, 172, 191, 220, 235, 285, 311, 312, 385, 400, 401, 424, 435, 443, 445, 446, 448, 451 - 454, 456 - 459, 465, 468, 469, 528, 538

Norme: 43, 45, 58, 225, 227, 229, 289, 311 - 313, 348, 377, 379, 381, 387, 397, 401, 409, 423, 425, 428, 431, 432, 437 - 439, 445 - 448, 450, 451, 454, 458, 461, 465, 467, 499, 528

Nudge: 45, 443, 450 - 456, 458, 460, 465, 482

O.

Objectivation: 232, 424, 442, 443, 448 - 450, 463, 469

Opérateur d'importance vitale: 18, 301, 304

P.

Panoptique: 11, 22, 29, 30, 48, 53, 55, 124, 127 - 129, 149, 193, 213 - 215, 217, 220, 222, 233, 380 - 382, 387, 405, 428, 429, 431, 435, 439, 458, 465, 472, 488

Partenariat: 13, 29, 117, 139, 159, 161, 163, 179

Patrimonialisation: 365, 368 - 370

Patriot Act: 90, 96, 499

Personnalité: 89, 107, 186, 276, 294, 353, 366, 444, 445, 447, 463, 511

Phénomène: 5, 25, 26, 28 - 30, 33 - 35, 37, 38, 41, 47, 51, 52, 54 - 56, 59, 62 - 66, 68 - 70, 72 - 74, 76, 84, 86, 88, 89, 92 - 95, 97, 99 - 101, 119 - 121, 128, 129, 133, 136, 145, 168, 172, 181, 184, 189, 217, 220, 221, 231, 270, 285, 354, 375, 379, 388, 391, 395, 408, 412, 413, 415, 421, 423, 432, 434, 442, 448, 450, 467

Philistin: 40, 165, 172, 173, 179, 187, 188, 382

Plasticité sociale: 30, 72, 146, 182, 184, 190, 191, 235, 467

Précaution: 155, 156, 204, 223, 226 - 232, 234, 460, 473, 487, 518, 523, 531

Prévention: 24, 36, 47, 61, 62, 73, 74, 88, 89, 91, 96, 98, 99, 127, 150, 151, 153 - 156, 162, 163, 187, 224, 227, 229, 232, 257, 262, 274, 277, 285, 287, 293, 294, 314, 356, 364, 370, 384, 423, 497, 501, 522, 523

Privacy by design: 12, 306 - 310, 313, 353, 488

Privacy Shield: 12, 13, 58, 322, 328 - 331, 515, 539

Privatisation: 150, 153, 156 - 159, 163, 393, 398 - 401, 403, 405, 418, 486

Propriété: 104, 106, 154, 225, 239, 255, 273, 279, 281, 341, 356, 361, 363 - 366, 368 - 373, 393, 396, 397, 428, 437, 444, 490, 503, 504

Q.

Qualification: 128, 130, 191, 237 - 239, 242, 244, 248, 251, 258, 283, 284, 287, 340, 345, 347, 351, 354, 358, 359

R.

Rationalisation: 29, 48, 73, 75, 92 - 97, 100, 105, 161, 166, 221, 285, 386, 388, 389, 426, 463

Règlement général de protection des données personnelles: 12, 293, 297, 308, 313, 322, 326, 328, 334, 336 - 338, 350, 364, 367, 404

Régulation: 14, 76, 104, 111, 112, 118, 135, 151, 153, 154, 164, 267, 289, 291, 293, 312, 313, 329, 331, 355, 364, 370, 372, 380, 394, 415, 417, 422, 429, 443, 444, 450, 451, 457, 463, 490, 522

Renseignement: 23, 42, 56, 67, 68, 74, 75, 88, 90, 96 - 99, 125, 126, 146, 167, 207, 208, 230, 246, 248, 249, 251, 270, 280, 281, 330, 343, 351, 358, 367, 502, 504, 505, 508, 515, 520, 525, 530

Responsabilisation: 27, 29, 138, 154, 294 - 296, 298, 312, 322, 325, 385, 423, 451, 459, 460, 466, 489

Risque: 7, 14, 24, 38, 49, 61, 62, 67, 78, 84, 87, 88, 94, 96, 99, 112, 115, 120, 129, 152, 162, 176, 181, 189, 200, 202 - 204, 210, 212, 223, 225 - 232, 243, 245, 249, 253, 257, 259 - 261, 268, 273, 274, 283, 285, 295 - 301, 303 - 305, 309, 323, 324, 329, 331, 336, 342, 348, 350, 356, 364, 384,

404, 409, 410, 413 - 415, 418, 421, 423, 440, 443, 448, 451, 453, 460, 469, 472, 529, 543

S.

Safe Harbor: 12, 13, 57, 58, 261, 266 - 271, 322, 328, 330, 539

Savoir: 25, 36, 46, 58, 75, 77, 85, 100, 106, 108, 126, 138, 141 - 143, 145, 151, 169, 176, 178, 183, 188, 189, 210, 216, 253, 264, 265, 276, 294, 301, 318, 326, 337, 348, 351, 355, 359, 360, 363, 376, 378, 384, 385, 387 - 391, 397, 401, 426, 438, 443, 447, 451, 453, 475, 489, 491, 540

Sécurité: 17 - 19, 21 - 24, 28, 29, 31, 41, 42, 45 - 48, 51 - 53, 56, 57, 59, 61, 62, 67, 73 - 75, 79, 80, 86 - 88, 91, 94 - 98, 109, 120, 122, 124, 125, 127, 129, 130, 134 - 136, 138, 141 - 143, 145, 146, 148 - 165, 167, 168, 172, 175 - 178, 181 - 183, 185, 187 - 189, 200, 203, 204, 209, 211, 216, 220, 221, 224 - 226, 228, 230 - 232, 235, 240, 248, 258 - 260, 262 - 264, 266 - 268, 271, 273, 274, 276, 277, 279 - 281, 285, 287, 288, 293 - 306, 312 - 316, 321, 323, 329, 330, 333, 336, 338 - 340, 343, 348 - 350, 356, 363 - 365, 369, 371, 375, 380 - 382, 384, 387, 394, 395, 401, 402, 405, 407 - 409, 411, 414, 419 - 422, 429, 430, 434, 436, 438 - 441, 446, 449, 454, 458, 465 - 468, 474, 476, 489, 491, 492, 497, 501, 502, 504, 507, 508, 510, 514 - 516, 521 - 523, 532, 534, 536, 544

Smart: 13, 31, 40, 121, 139 - 142, 171, 191, 210, 219, 263, 333, 342, 345, 392, 393, 399, 402 - 405, 407, 411, 414, 441, 483, 487, 492, 525, 526

Smartification: 342, 392, 407, 414

Snowden: 25, 42, 55, 57, 67, 74, 88, 90, 124, 126, 237, 246, 248, 259, 265, 270, 450, 478, 484, 532

Société de l'information: 17, 50, 63, 100, 101, 103 - 111, 114, 115, 119, 120, 122, 124, 133, 135 - 138, 140, 148, 155, 164, 166, 169, 171, 174, 177, 179, 188, 189, 235, 283, 285, 358, 379, 391, 442, 443, 478, 491, 497, 511, 512, 520, 522, 523

Société de surveillance: 34, 42, 52, 91, 100, 114, 127, 129, 149, 428, 472, 476, 478, 510, 535

Solutionnisme: 85 - 88, 170, 226, 406, 412, 418, 465, 479

Sousveillance: 59, 122, 128, 130, 131, 176, 487, 493

Souveraineté: 9, 37, 80, 134, 142, 146, 263, 272, 379, 386 - 388, 390, 417 - 421, 427, 510

Storytelling: 14, 134, 138, 141, 142, 176, 434, 440, 474, 481

Subjectivation: 446, 448, 450

Surveillance diffuse: 5, 13, 26 - 34, 36 - 38, 40 - 42, 44, 46 - 52, 54 - 59, 61 - 66, 73, 74, 76, 84, 85, 87, 92, 96, 99, 101, 105, 111, 114, 115, 118 - 124, 126 - 130, 133 - 136, 138, 139, 142, 145 - 147, 149, 150, 152, 153, 156, 163 - 165, 167, 168, 172, 174, 175, 177, 182, 184, 185, 188 - 193, 198, 200, 204, 212 - 214, 217, 220 - 223, 229 - 231, 233, 235 - 237, 251, 252, 255, 257, 259 - 265, 270, 273, 281, 283, 285, 287 - 289, 291, 298, 317, 318, 321, 327, 331, 333 - 335, 340 - 342, 353 - 358,

362 - 366, 370, 371, 375 - 380, 382, 384 - 386, 389, 391 - 394, 396, 398, 399, 402, 405 - 409, 412, 413, 415 - 419, 421 - 426, 428 - 432, 435 - 437, 439 - 443, 447, 449 - 451, 453, 454, 456, 458, 460, 463, 465 - 469

T.

Totalisation: 168, 193, 213, 214, 217, 220 - 222, 226, 229, 235, 403, 430, 432, 463

Traçabilité: 36, 121, 130, 191, 193, 213, 219, 223 - 232, 234, 246, 252, 260, 304, 480

Trace: 23, 30, 32, 48, 56, 88, 119, 128, 130, 131, 149, 168, 176, 191, 193, 217, 219, 223 - 226, 230, 231, 235, 236, 246, 259, 260, 356, 389, 391, 392, 404, 437, 438

Traitement: 7, 12, 23, 26, 31, 33, 48, 49, 52, 57 - 59, 75, 77, 78, 81, 82, 84, 105, 107, 112, 113, 119 - 121, 126, 127, 129, 130, 145, 175, 178, 189, 191, 192, 194 - 204, 207, 208, 210 - 212, 217, 235, 236, 238 - 241, 243, 244, 246, 248 - 267, 269, 271, 274, 275, 277, 278, 283 - 285, 287, 288, 291, 293 - 302, 304 - 306, 308 - 330, 333, 336 - 344, 346 - 349, 351, 352, 356 - 358, 361, 368, 371 - 373, 376, 404, 405, 415, 430, 434, 448, 451, 457, 494, 496 - 498, 500, 503, 514, 515, 517, 519, 522, 525

Transparence: 30, 63, 158, 169, 198, 222, 223, 228 - 234, 285, 295, 393, 398 - 403, 405, 424, 457, 458, 465, 472

Tyrannie: 38, 39, 128, 153, 186, 215, 233, 234, 400, 407, 408, 471, 481, 484

U.

UNESCO: 19, 63, 108 - 111, 480, 494, 510 - 512, 530

Utilitarisme: 214, 379 - 381, 405, 406, 410, 418, 421, 422, 424, 429, 435, 438, 439, 441, 442, 449, 455, 463, 468

V.

Vertu: 37, 42, 46, 48, 95, 99, 104, 108, 113, 128, 129, 135, 140, 142, 153, 171, 184, 202, 231, 274, 277, 294, 309, 326, 328 - 330, 337, 372, 403, 408, 409, 419, 420, 447, 452 - 454, 456, 457, 459, 466, 489, 507, 512

Vie privée: 5, 7, 12, 17, 21, 23, 25 - 28, 30 - 34, 42, 45, 48, 57 - 59, 62, 63, 74, 76 - 79, 82, 83, 91, 98, 100, 107, 111 - 114, 122, 133, 168, 170, 176, 180 - 182, 190 - 192, 194, 195, 197 - 202, 204, 205, 207 - 210, 212, 213, 223, 236, 240, 246, 249, 250, 254 - 256, 259, 260, 262 - 265, 268, 270 - 281, 284, 286 - 289, 291, 295 - 297, 299 - 301, 306 - 308, 310 - 313, 316, 319, 322, 325, 331, 333 - 336, 338, 340, 341, 343, 347, 348, 350 - 354, 359, 362, 364 - 367, 369 - 371, 375, 376, 395, 397, 398, 401, 404, 420, 423, 436, 437, 443, 444, 448, 457, 465, 468, 478, 482, 484, 487, 490, 491, 497,

510, 511, 513, 516 - 518, 522, 529, 535, 540, 543

Vie privée différentielle: 347, 350 - 353

Visibilité: 11, 95, 130, 186, 214 - 217, 220, 232 - 234, 271, 293, 380, 391, 400, 401, 405, 419, 424 -
429, 439, 465, 471, 484

Tables des matières

Remerciements	3
Sommaire.....	5
Glossaire	7
Tables des sigles et abréviations.....	17
Introduction générale.....	21
Section 1: La vie privée ou l'enjeu du siècle de la surveillance diffuse	27
Paragraphe 1: De l'utilité d'une démarche objective quant au concept de surveillance diffuse	28
Paragraphe 2: De l'utilité de la compréhension des concepts d'anthropocène numérique et de moments historique décisif : le siècle de la surveillance diffuse	30
A. La philosophie de la surveillance diffuse.....	31
B. La surveillance diffuse:le nouvel ethos de la civilisation contemporaine	34
Section 2: La surveillance diffuse: une « fiction instituante »?	37
Paragraphe 1: Des mythes littéraires qui entourent le phénomène de surveillance	38
A. Les « prophéties » de Georges Orwell et de Aldous Huxley : « 1984 » Versus « Le meilleur des mondes »	38
B. Kafka, Little brother et la désinstitution progressive du Droit	43
Paragraphe 2: La surveillance diffuse: une fiction pleinement instituée dans nos sociétés	47
A. L'institutionnalisation progressive d'une fiction dans les sociétés contemporaines: la diffusion de la surveillance.....	47
B. La surveillance diffuse aujourd'hui: sens, portée et objet	51
1. De la surveillance... ..	52
2. ... A la surveillance diffuse.....	54
Partie 1 : Une intégration de la surveillance diffuse modérée sous l'empire de la loi de 1978 et de la directive de 1995	61
Titre 1: L'institutionnalisation progressive de la surveillance diffuse: naissance et développement d'un phénomène de société	63
Chapitre 1: La diffusion de la surveillance dans la société numérique	65
Section 1: Approche phénoménologique de la surveillance diffuse : un phénomène issu du phénomène technique	65
Paragraphe 1: Analyse de la diffusion mondiale de la surveillance: entre phénomène social et phénomène juridique.....	66
A. La diffusion de la surveillance dans les sociétés contemporaines	66
1. De quelques repères historiques nécessaires: la surveillance ou l'informatisation progressive de l'activité de renseignements	67

2. La filiation de la surveillance au phénomène technique	69
B. La surveillance diffuse: un phénomène juridique en devenir corrélé à l'émergence des législations informatiques et libertés	74
1. L'émergence des législations informatique et libertés comme facteur de diffusion de la surveillance	75
2. L'ambiguïté des législations informatique et libertés: entre protection de la personne fichée et protection d'un marché économique en devenir	80
Paragraphe 2: Des intentionnalités et des perceptions du phénomène de surveillance diffuse : entre technophilie et technophobie	84
A. Les intentionnalités positives du phénomène de surveillance diffuse: le paroxysme de la technophilie	84
1. La surveillance diffuse: une solution pour régler les maux de la société contemporaine	85
2. Illustration du solutionnisme technologique: la surveillance diffuse comme réponse au terrorisme	87
B. Les intentionnalité technophobiques et négatives de la surveillance diffuse: vers un monde rationalisé	92
1. La surveillance diffuse comme facteur de rationalisation et de désenchantement du monde	92
2. La légitimation de la surveillance diffuse: action rationnelle ou réaction d'opportunisme ?	96
Section 2: Approche pragmatique et démythifiée de la diffusion de la surveillance: un phénomène global et banalisé.....	99
Paragraphe 1: De la globalisation de la surveillance dictée par un impératif ancien: l'information une source de pouvoir	100
A. L'édification de la société de l'information comme prélude à la surveillance diffuse	101
1. Les théories de l'information et de la communication: fondement de la construction de la future société de l'information	101
2. L'information : un enjeu de pouvoir et de domination à l'international	104
B. La doctrine du free flow of information et la libre circulation de l'information: des mécanismes juridiques au service de la globalisation de la surveillance	107
1. Le rôle de l'UNESCO dans la reconnaissance d'une circulation libre et équilibrée de l'information	108
2. La liberté de circulation de l'information : une liberté économique structurante de la surveillance	111
Paragraphe 2: ... A la banalisation de la surveillance diffuse	114
A. La surveillance diffuse : un enchevêtrement de dispositifs socio-techniques présents dans l'espace privé et public conduisant à une banalisation de la surveillance	115
1. La pluralité technologique comme élément structurant de la surveillance.....	115

2. La banalisation de la surveillance diffuse	119
B. Les formes de la surveillance à l'épreuve de la surveillance diffuse.....	122
1. La polysémie de la surveillance diffuse.....	123
2. La double nature de la surveillance diffuse	127
Chapitre 2: Des acteurs multiples au service de l'institutionnalisation de la surveillance diffuse: l'élaboration d'une culture de la surveillance	133
Section 1: La surveillance diffuse et la convergence des intérêts des leaders du numérique et de leurs alliés institutionnels et politiques.....	134
Paragraphe 1: La convergence des intérêts des leaders du numérique et de leurs alliés institutionnels et politiques: une nouvelle forme de pouvoir au service de la surveillance diffuse.....	134
A. L'organisation de la surveillance diffuse par le secteur privé et le secteur public: entre storytelling et softpower	134
1. L'exercice d'un soft power par l'Etat: force de persuasion douce au service de la surveillance diffuse	135
2. Le storytelling ou la participation pleine et entière du secteur privé à la légitimation technologique	138
B. La gouvernementalité par la peur : facteur essentiel de la banalisation contemporaine de la surveillance diffuse	142
Paragraphe 2: La marchandisation de la sécurité: fondement et aboutissement de la convergence des intérêts du secteur public et du secteur privé dans le cadre de la surveillance diffuse.....	148
A. Le « droit à » la sécurité comme renouveau d'une convergence institutionnelle, politique et économique	149
1. Le droit à la sécurité comme symptôme d'une transformation du rôle de l'Etat rendue nécessaire par la surveillance diffuse	150
2. Le droit à la sécurité comme transformation profonde de la gouvernance dans nos société modernes.....	153
B. De la privatisation de la sécurité à sa marchandisation au service de la surveillance diffuse	156
1. Le choix de la gestion managériale de la sécurité par l'Etat comme prémices à sa marchandisation	156
2. La marchandisation de la sécurité et de la surveillance	161
Section 2: L'intégration de la surveillance diffuse par les individus: la culture de la surveillance et son apogée	163
Paragraphe 1: De l'homo-numericus au philistin consommateur de sécurité.....	165
A. L'homo-numericus ou la fascination pour les technologies de l'information et de la communication.....	165
1. Un acteur essentiel et adaptable.....	165

2. ... Poussé par la croyance en la toute puissance libératrice des technologies de l'information et de la communication	168
B. La banalisation des technologies de l'information et de la communication dans une société de masse : la philistin et la crise de la culture technicisée.....	172
1. La surveillance diffuse et la culture contemporaine « en crise ».....	172
2. Le conditionnement des masses à la consommation technologique	174
Paragraphe 2: Le mythe de Narcisse au service de la culture de la surveillance diffuse	177
A. L'individu narcissique: un individu dépersonnifié par les objectifs marchands.....	177
1. L'individu narcissique: une cible dans un marché économique....	177
2. ... en quête d'attention	179
B. ... Participant pleinement à l'économie de l'attention: de la malléabilité des individus à la plasticité sociale	182
1. Le mythe de Narcisse ou la ductilité des individus-consommateur de surveillance diffuse	182
2. La plasticité sociale engendrée par la surveillance diffuse ou l'aliénation des individus	184
Conclusion de Titre	189
Titre 2: Une intégration délicate de la surveillance diffuse dans la protection offerte au titre du droit des données personnelles sous l'empire de la loi de 1978 et de la directive de 1995	191
Chapitre 1: Un déficit de conscience des enjeux de la surveillance diffuse sous l'empire de la loi de 1978 et de la directive de 1995:.....	193
Section 1: La protection des données personnelles issue de la loi de 1978 et de la directive de 1995: une volonté de protéger l'individu par un champ d'application large.....	194
Paragraphe 1: Le respect de la vie privée appliqué aux données à caractère personnel	194
A. En amont du traitement de données à caractère personnel	194
1. Les principales définitions posées par la loi de 1978 et la directive de 1995	194
2. Les modalités de collecte et de traitement de données à caractère personnel	198
B. En aval du traitement de données à caractère personnel	200
1. Les droits des sujets du traitement : une ambition du législateur à donner aux individus la maîtrise de leurs données personnelles	201
2. La responsabilité liée au traitement et l'obligation de sécurisation.....	203
Paragraphe 2: Une protection envisagée en fonction du degré d'intrusivité technologique permettant de couvrir un large panel de situations: l'exemple des technologies biométriques	204
A. Le degré d'intrusivité technologique en théorie	205
1. La polysémie de la neutralité technologique	205
2. L'analyse du degré d'intrusivité technologique ou la question des usages technologiques	207

B. Le degré d'intrusivité technologique en pratique: l'exemple de la biométrie	208
1. Le degré d'intrusivité de la biométrie.....	208
2. Application de la neutralité technologique à la biométrie	210
Section 2: Un déficit de conscience des enjeux de la surveillance diffuse: l'érection d'un data-panoptisme permis par la totalisation numérique	213
Paragraphe 1: Le panoptique de Bentham: une grille d'analyse nécessaire pour comprendre le data-panoptisme	213
A. Du panoptique de Bentham... ..	214
1. Le principe d'inspection de Bentham à l'épreuve de la surveillance diffuse	214
2. L'importance du regard dans l'étude du panoptique par Foucault	215
B. ... Au Data-panoptisme: totalisation numérique et datafication de la vie même	217
1. L'information: un système de contrôle selon Deleuze.....	217
2. Le data-panoptisme ou la mise en données du monde pour un contrôle social invisible et invérifiable	219
Paragraphe 2: Le data-panoptisme et l'injonction de transparence pesant sur les individus	222
A. De la traçabilité des activités humaines au suivi de nos traces digitales... ..	223
1. De la traçabilité de l'individu et de sa réduction à une trace numérique.....	223
2. ... Par l'avènement en droit positif de la reconnaissance du principe de précaution	226
B. ... A l'injonction de transparence des individus posée par la surveillance diffuse.....	229
1. Traçabilité, principe de précaution et data-panoptisme ou l'injonction de transparence	229
2. Des effets de la transparence imposée	232
Chapitre 2: Un déficit d'effectivité globale des premières législations informatiques et libertés face à la surveillance diffuse	235
Section 1. L'insaisissabilité de la protection des données personnelles au vu de la surveillance diffuse	236
Paragraphe 1. L'élargissement progressif de la notion de données personnelles facteur de son ineffectivité	237
A. La délicate opération de qualification juridique de la donnée en tant que donnée personnelle: l'exemple des données d'identification techniques considérées comme des données personnelles	237
1. La qualification de l'adresse IP en tant que donnée à caractère personnel.....	238
2. ... Du fait de l'opération de traitement	241
B. Les données de connexion: des données devenues personnelles au vu de la surveillance diffuse	244
1. La métadonnée: une donnée de connexion	246
2. La qualification de la métadonnée en tant que donnée à caractère personnel	248

Paragraphe 2. La délicate détermination du champ d'application de la loi face à la notion de traitement de données personnelles dans le cadre de la surveillance diffuse.....	251
A. Les traitements de métadonnées: analyse de l'arrêt Tele2 Sverige rendu par la CJUE en 2016	252
B. L'interconnexion et l'interopérabilité des données comme réel problème posé par la surveillance diffuse	255
1. L'interconnexion et l'interopérabilité des données personnelles et non personnelles au coeur de la surveillance diffuse	255
2. Une volonté d'élargissement constante des premières législations informatiques et libertés comme facteur de leur manque d'effectivité	257
Section 2: Le constat nécessaire du déficit d'effectivité des premières législations informatiques et libertés tant au niveau du régime juridique de protection qu'au niveau international.....	260
Paragraphe 1: Le respect des principes fondamentaux de la protection des données personnelles en question	261
A. L'adéquation relative des principes fondamentaux de la protection des données personnelles à la surveillance diffuse	261
1. La problématique de la finalité du traitement et la surveillance diffuse.....	262
2. La délicate opération de recueil du consentement	264
B. L'inadéquation des flux transfrontières de données personnelles: la remise en cause du Safe Harbor par l'arrêt CJUE du 6 octobre 2015.....	266
1. Le Safe Harbor: un instrument international sous influence européenne	266
2. La remise en question des Safe Harbor	269
Paragraphe 2. La conception des données personnelles par référence à la vie privée: un choix heureux contre l'idéologie sécuritaire mais peu efficace dans son ensemble	272
A. La conception des données personnelles par référence à la vie privée.....	272
1. Le droit des données personnelles par référence à la vie privée.....	273
2. Un principe essentiel d'une société libre et démocratique non reconnu par la Constitution	275
B. Le principe de proportionnalité des législations Informatiques et Libertés: un principe permettant la balance entre deux intérêts antagonistes	277
Conclusion de Titre.....	283
Conclusion partielle.....	285
Partie 2: L'intégration parfaite de la surveillance diffuse dans l'évolution des notions juridiques de vie privée et de données personnelles	287
Titre 1: La désinstitution du droit des données personnelles et de la vie privée sous l'empire des nouveaux instruments européens.....	291
Chapitre 1: L'organisation d'une gouvernance des données personnelles au titre du règlement général sur la protection des données personnelles.....	293

Section 1: L'organisation d'une protection fondée sur la responsabilisation des acteurs: l'accountability ou la gouvernance des données personnelles	295
Paragraphe 1: L'intégration d'une logique risque dans le cadre de la protection des données personnelles: les études d'impact sur la vie privée	296
A. La prise en compte du risque lié au traitement de données personnelles dans le cadre de l'analyse d'impact sur la vie privée	296
1. Des traitements susceptibles de présenter des risques pour les droits et libertés des personnes physiques	297
2. L'organisation de l'étude d'impact sur la vie privée	299
B. Le renforcement de l'obligation de sécurisation des données : un élément positif dans l'intérêt du responsable de traitement	301
1. Une influence nette des politiques de cybersécurité	301
2. Le renforcement de l'obligation de sécurisation	304
Paragraphe 2: La réduction de la vie privée à un argument marketing: la privacy by design	306
A. Les origines d'une notion potentiellement dangereuse en terme de droits et libertés des personnes concernées par des traitements de données à caractère personnel	306
B. La possibilité de réduire la vie privée à un argument marketing : la privacy by design dans le règlement général de protection des données personnelles	308
1. Champ d'application de la privacy by design sous l'égide du règlement	309
2. Une tentative de réduction de la vie privée à un argument marketing ?	310
Section 2: Le règlement général de protection des données personnelles: un instrument dangereux en terme de sécurité juridique et de libertés.....	313
Paragraphe 1: Licéité du traitement de données personnelles et consentement de la personne concernée	313
A. La fin progressive du principe des traitements avec consentement	315
1. Les traitements concernés par le recueil du consentement préalable	315
2. La nouvelle définition du consentement	317
B. L'apparition d'un nouveau principe: les traitements sans consentement pour « intérêt légitime »	319
Paragraphe 2: Des gardes-fous existants mais inefficaces	322
A. L'ineffectivité de la responsabilisation des acteurs opérant des traitements de données personnelles	322
1. L'acteur majeur de la responsabilisation: le délégué à la protection des données personnelles	322
2. Des « métadroits » pour assurer une meilleure protection des individus : l'exemple du droit à l'oubli	325
B. Les transferts de données personnelles hors Union Européenne: l'exemple du Privacy Shield	328

Chapitre 2: L'organisation de la marchandisation de la vie privée par les nouveaux instruments européens: vers une désinstitution du droit au respect de la vie privée et de la protection des données personnelles au profit de la surveillance diffuse333

Section 1: L'organisation de la libre circulation des données non personnelles comme facteur d'intégration complète de la surveillance diffuse et de désinstitution du droit au respect de la vie privée335

Paragraphe 1 La proposition de règlement sur la libre circulation des données non personnelles: un instrument au service de la marchandisation de la vie privée335

A. La réduction progressive du droit des données à un droit économique335

1.L'élaboration progressive de la libre circulation des données336

2.Une consécration dans la proposition de règlement de 2017338

B. Une nouvelle vision européenne du statut juridique du marché des données ?340

Paragraphe 2: La volonté de la surveillance de construire des profils les plus individualisés possibles: analyse de l'arrêt JC Decaux du Conseil d'Etat du 8 février 2017342

A. L'analyse des comportements des individus par la mesure de fréquentation et d'audience : un dispositif en développement fondé principalement sur l'analyse de données non personnelles342

1.Le dispositif d'analyse de comportement des individus par la mesure de l'audience de panneaux publicitaires342

2.La qualification de l'adresse mac des smartphones en tant que personnelle: un contentieux pouvant être soumis à la même interprétation que le contentieux lié à l'adresse IP345

B. L'anonymisation des données personnelles: des mesures techniques inopérantes pour garantir la protection de la vie privée ?347

1.La question de l'anonymisation des données comme mesure technique de protection de la vie privée347

2.L'émergence du concept de vie privée différentielle ou la consécration de la perte de maîtrise des individus sur leurs données au profit du marché350

Section 2: Pour une appréhension de la surveillance diffuse au travers de la théorie juridique de l'information353

Paragraphe 1: La catégorie juridique des biens comme possible réponse du droit aux problématiques posées par la surveillance diffuse sur le droit des données354

A. De l'utilité du recours à la notion d'information pour appréhender autrement le droit des données355

1.Le brouillage de la frontière entre données personnelles et non personnelles par la surveillance diffuse355

2.La notion d'information saisie par le Droit357

B. La théorie juridique de l'information de Pierre Catala ou la possibilité de comprendre les données comme un bien juridique359

1. L'ébauche de l'application de la catégorie juridique des biens aux données360

2. Recherche d'une catégorie juridique des biens applicable à la notion d'information et potentiellement au droit des données	362
Paragraphe 2: L'appropriation des données: un droit chimérique ou une réalité en construction possible au vu de la surveillance diffuse ?	365
A. L'appropriation des données par application des mécanismes civilistes du droit des contrats	366
1. Des éléments de réponses contenus dans les nouveaux instruments européens	366
2. Les moyens possibles d'une organisation civiliste de la patrimonialisation des données	368
B. L'impossible appropriation des données entendues comme des biens communs	370
Conclusion du Titre	375
Titre 2: La désinstitution du Droit au profit de la nouvelle norme admise: la surveillance diffuse	377
Chapitre 1: La surveillance diffuse: entre désinstitution de la fonction du droit et mutation du Droit par la nouvelle norme admise	379
Section 1: L'influence de la surveillance diffuse sur la circulation et la fonction du droit	379
Paragraphe 1: La surveillance diffuse: un outil privilégié de l'utilitarisme des sociétés libérales contemporaines	380
A. L'utilité de la surveillance diffuse	380
1. La surveillance diffuse et le libéralisme économique	380
2. La surveillance diffuse: l'outil principal au service d'un pouvoir utilitariste	382
B. La transformation des modalités d'exercice du pouvoir: du biopouvoir de Foucault au biopouvoir algorithmique	385
1. Du Biopouvoir comme technique de pouvoir s'exerçant sur la vie des individus et des populations	386
2. ... Au biopouvoir algorithmique comme nouvelle technique de pouvoir engendrée par la surveillance diffuse	389
Paragraphe 2: La transformation des espaces sociaux par la surveillance diffuse comme perte de sens du droit ou reconnaissance d'une nouvelle fonction:	393
A. L'importance de la dichotomie entre l'espace public- espace privé pour le Droit	393
1. Circulation et fonction du droit dans l'espace public	394
2. Circulation et fonction du Droit dans l'espace privé	396
B. La nouvelle fonction du Droit engendrée par la surveillance diffuse: la participation à l'élaboration d'une transparence totale par la privatisation du public et la publicisation du privé	399
1. L'organisation de la transparence totale prise en charge par le Droit	399
2. La Smart-City comme illustration de la nouvelle fonction du Droit	402
Section 2: La consécration de la prise en compte par le Droit des objectifs du libéralisme exalté par la surveillance diffuse	406

Paragraphe 1: La surveillance diffuse, le libéralisme, le biopouvoir algorithmique et l'élaboration d'un « Droit libéral »	407
A. Des interactions entre le Droit et l'ambition du libéralisme à créer une « tyrannie du Bien »	407
B. La consécration d'un Droit Libéral.....	409
Paragraphe 2: De la « réglementation algorithmique » à « l'aberration du solutionnisme technologique » : la consécration d'un Etat de Droit Libéral ou la promotion du laissez-faire juridique	412
A. De la réalité possible de la réglementation algorithmique.....	413
1. Tentative de définition de la réglementation algorithmique	413
2. Réalisme de la réglementation algorithmique à travers l'Etat de Droit libéral	416
B. L'aberration du solutionnisme technologique: des risques de la réglementation algorithmique	418
1. L'Etat de Droit libéral: une gestion souveraine... ..	419
2.... L'Etat de Droit libéral ou la gestion des masses par le calcul d'utilité.....	421
Chapitre 2: La mutation du contrôle social par la surveillance diffuse et ses effets sur le Droit	423
Section 1: L'avènement d'un contrôle social positivé et pleinement intériorisé du fait de la surveillance diffuse: l'attention	424
Paragraphe 1: De la mutation du contrôle social par l'élaboration d'une économie de la visibilité	425
A. L'assujettissement de l'individu à la visibilité.....	425
B. La mutation du contrôle social par le libéralisme contemporain	426
Paragraphe 2: L'avènement d'un contrôle social positivé et pleinement intériorisé du fait de la surveillance diffuse: l'attention	429
A. L'attention: une nouvelle forme de contrôle social positivé.....	430
1. Le dressage et la domestication des individus	430
2. La totalisation d'un nouveau contrôle social: l'attention	432
B. Du mythe « je n'ai rien à cacher, je n'ai rien à me reprocher » comme pleine intériorisation du contrôle social	436
1. L'analyse du mythe « je n'ai rien à cacher je n'ai rien à me reprocher »: ou la crédulité des individus ?	436
2. L'affirmation d'un auto-contrôle des individus par l'intériorisation de l'attention ...	438
Section 2: L'objectivation des individus par la surveillance diffuse: transformation des sujets de droit et désinstitution du Droit.....	442
Paragraphe 1: La surveillance diffuse ou l'objectivation des individus	443
A. Du sujet de Droit	444
1. L'institutionnalisation par le Droit de l'individu en tant que sujet de Droit	444
2. L'imposition par le Droit de la conformité des comportements à la loi	445

B. ... Aux corps statistique: la réduction du sujet de Droit à un objet	447
Paragraphe 2: L'apparition d'une nouvelle forme de régulation par la surveillance diffuse: la technique des nudges comme symptôme de la perte de symbolicité du Droit et de sa désinstitution progressive.....	450
A. La production par la surveillance diffuse et le contrôle social attentionnel d'une nouvelle forme de normalisation: les nudges	451
1. Le nudge comme technique de normalisation manipulatrice des in-sujets.....	452
2. De deux exemples pratiques de mise en place du nudge: les compteurs Linky et les péages inversés	454
B. De la perte de symbolicité du Droit à sa désinstitution progressive.....	458
Conclusion de Titre.....	463
Conclusion Partielle.....	465
Conclusion Générale	467
Bibliographie	471
Table des annexes	541
Index des principaux auteurs	545
Index des notions principales	551
Tables des matières.....	561

La surveillance diffuse: entre Droit et Norme

Résumé

L'objectif de ce travail de recherches est de comprendre comment la surveillance diffuse s'intègre dans l'évolution des notions juridiques de vie privée et de données personnelles. A l'inverse de la littérature foisonnante sur le thème de la surveillance, il ne s'agit pas ici de mettre en avant la nécessité de trouver un équilibre entre la surveillance entendue dans sa dimension sécuritaire et la protection de la vie privée et des données personnelles, en ce qu'elle constitue une liberté fondamentale reconnue par les institutions françaises et européennes. Cette recherche d'une balance équilibrée entre sécurité et liberté doit nécessairement être dépassée pour comprendre le phénomène de surveillance diffuse. La surveillance n'est plus la simple activité de recherche de renseignements concernant un individu potentiellement dangereux. Elle s'inscrit plutôt dans la poursuite de ce que Hannah Arendt qualifie de « crise de la culture ». La surveillance diffuse est même l'une des caractéristiques de la culture contemporaine dominée par la peur, la consommation et l'aliénation par les technologies. Devenue la nouvelle norme sociale admise, la surveillance diffuse désinstitue le droit des données personnelles et la protection de la vie privée. Progressivement, elle désinstitue également le Droit au profit du libéralisme économique qu'elle porte en son sein.

Mots clefs français :

Surveillance, Surveillance diffuse, Vie privée, Donnée personnelle, Norme, Information, Désinstitution du Droit, Libéralisme, Contrôle social, Nudge, Economie de l'attention, Panoptique, Privacy by design

The diffuse surveillance: between Law and Norm

Abstract

The purpose of this research is to understand how diffuse surveillance fits into the evolution of legal concepts of privacy and personal data. Contrary to the abundant literature on the subject of surveillance, it is not a question here of highlighting the need to find a balance between surveillance in its security dimension and the protection of privacy and data, as a fundamental freedom recognized by French and European institutions. This search for a balance between security and freedom must necessarily be overcome to understand the phenomenon of diffuse surveillance. Surveillance is no longer just a search for information about a potentially dangerous individual. Rather, it is a continuation of what Hannah Arendt calls the « crisis of culture ». Diffuse surveillance is even one of the features of contemporary culture dominated by fear, consumption and alienation by technology. Having become the new accepted social norm, the diffuse surveillance deinstitutiones the right of the personal data and the protection of the private life. Gradually, it also deinstitutiones the Law to profit from the economic liberalism that it carries within it.

Keywords :

Surveillance, Diffuse surveillance, Privacy, Personal Data, Norm, Information, Deinstitution of Law, Liberalism, Social Control, Nudge, The « attention economy », Panopticon, Privacy by design

Unité de recherche/Research unit : CERAPS - UMR 8026 - CNRS, 1 place Déliot, BP 629, 59024 Lille Cedex, [ceraps\(at\)univ-lille2.fr](mailto:ceraps(at)univ-lille2.fr), <http://ceraps.univ-lille2.fr/>

Ecole doctorale/Doctoral school : Ecole doctorale des sciences juridiques, politiques et de gestion, n° 74, 1 place Déliot, 59000 Lille, ecodoc.univ-lille2.fr, <http://edoctorale74.univ-lille2.fr>

Université/University : Université Lille 2, Droit et Santé, 42 rue Paul Duez, 59000 Lille, <http://www.univ-lille2.fr>