UNIVERSITÉ DU QUÉBEC À MONTRÉAL

DROITS HUMAINS ET SURVEILLANCE ÉTATIQUE ANTI TERRORISTE : AU DELÀ DU DROIT À LA VIE PRIVEÉ

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAITRISE EN DROIT

PAR
CLAIRE STREHAIANO

DÉPARTEMENT DES SCIENCES JURIDIQUES

DÉCEMBRE 2020

REMERCIEMENTS

Je tiens en premier lieu à remercier mon directeur de recherche le Professeur Bruce Broomhall pour tous ses conseils éclairants, son écoute attentive, son soutien, sa patience et bien sûr tout le travail de relecture et de commentaire de ce mémoire. Je suis allée voir le Professeur Broomhall obstinée à travailler sur le sujet de la surveillance étatique et je n'aurais pu espérer une meilleure aide pour me guider à travers les différentes implications du sujet et la nécessité de l'adapter aux exigences d'un mémoire de maitrise.

Je tiens également à remercier les commentateurs du mémoire, les Professeurs Oliver Barsalou et Hugo Cyr, pour toutes leurs recommandations et questions sur la présentation du projet de mémoire, qui m'ont été d'une aide précieuse. Leur expertise et intérêt pour le sujet m'ont permis d'aborder de nombreux points qui ne l'auraient pas été sans leurs suggestions.

Je suis très reconnaissante envers la fondation J.A De Sève de m'avoir généreusement accordé une bourse d'excellence à la session d'hiver 2020, qui en parallèle du soutien financier, m'a confortée dans la pertinence de mon sujet de recherche.

D'autre part, je dois beaucoup à mes proches, qui ont su m'épauler durant ces deux années de maîtrise. Je tiens premièrement à exprimer toute ma reconnaissance envers mes parents, Anne et Jean, pour leur soutien infaillible dans tous mes projets, même ceux qui impliquent de s'expatrier sur un autre continent pour étudier le droit international. J'ai toujours à cœur de trouver les mots justes, mais je n'en connais aucun qui soit suffisamment fort pour les remercier.

Je remercie aussi ma grande sœur Lucie, que je pouvais toujours appeler dans mes moments de doute, pour sa grande capacité d'écoute et sa compassion. Je suis également très reconnaissante de la présence à mes côtés de mon compagnon Fabien, pour tous ses encouragements et sa patience que je ne peux décrire que comme céleste. Enfin, je remercie ceux avec qui j'ai passé de longues journées de recherche et de rédaction, mes camarades de maîtrise, Léa, Clara et Jean-Baptiste, pour leurs conseils sur ce mémoire et surtout pour leur amitié.

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

CCPA	California Consumer Privacy Act
CEDH	Cour européenne des droits de l'homme
CJUE	Cour de justice de l'union européenne
FISA	Foreign Intelligence Surveillance Act
GCHQ	Government Communications Headquarters
NSA	National Security Agency
OCDE	Organisation de coopération et de développement économiques
ONU	Organisation des nations unies
PGP	Pretty Good Privacy
PIDCP	Pacte international relatif aux droits civils et politiques
RGPD	Règlement général sur la protection des données
UE	Union européenne
VPN	Virtual Private Network

RÉSUMÉ

Ce mémoire traite du sujet crucial et contemporain de la surveillance étatique dans le contexte de la lutte-antiterroriste. Nous montrons que ces objectifs de *sécurité nationale* sont utilisés comme prétexte par les gouvernements pour une surveillance automatisée de masse, dont l'ampleur et l'intensité résultent en la surveillance permanente de chaque individu. Nous présentons l'évolution des techniques de surveillance, notamment l'utilisation des technologies *Big Data* et étudions ainsi les effets d'un tel degré de surveillance sur l'exercice des droits de la personne. Après avoir constaté le caractère néfaste de ces effets, nous répondons à la question de la pertinence du cadre juridique du droit à la vie privée, en montrant ses multiples failles. Nous explorons ensuite les cadres juridiques alternatifs au droit à la vie privée, à savoir les autres droits de la personne consacrés en droit international et un droit relativement récent : celui de la protection des données personnelles, spécifiquement dans leur capacité à prendre en compte les enjeux de la surveillance automatisée. Enfin, après avoir relevé les avantages et les lacunes de ces règles de droit, nous évoquons les solutions possibles, juridiques et extra-juridiques, pour faire face à la surveillance de masse.

Mots clés: droit à la vie privée, droits de la personne, droit international des droits de la personne, protection des données personnelles, surveillance de masse, lutte anti-terroriste, *surveillance studies*.

ABSTRACT

This Master's thesis is dedicated to the crucial and burning topic of state surveillance in the context of counterterrorism. We show that the objectives of *national security* are used as an excuse to justify automated mass surveillance. The scope and intensity of this surveillance result in the continuous surveillance of every individual. We explain how surveillance techniques have evolved, notably with the use of *Big Data* and study the effects of this new surveillance on the exercise of one's human rights. After observing the harmful nature of these effects, we answer the question of the right to privacy legal framework's suitability, by revealing its multiple loopholes. We thus explore the alternative legal frameworks, such as the other human rights established in international law and the relatively new legal field of data protection, specifically regarding their capacity to address the issues of automated surveillance. Lastly, after we have shown the advantages and shortcomings of these regulations, we mention possible solutions, inside and outside of the legal realm, to face mass surveillance.

Keywords: right to privacy, human rights, international human rights law, personal data, mass surveillance, counter-terrorism, personal data protection, surveillance studies.

INTRODUCTION

Le sujet de ce mémoire porte sur la surveillance étatique de masse et la façon dont elle est justifiée et amplifiée par la lutte anti-terroriste. Nous analyserons les aspects juridiques de ce sujet en étudiant les normes applicables et les effets de cette surveillance sur les droits de la personne, en particulier le droit au respect de la vie privée, tels que consacrés en droit international.

Par lutte anti-terroriste, on entend les mesures mises en place par l'Etat pour empêcher, prévenir et anticiper les actes terroristes, ainsi que la poursuite et la répression de leurs auteurs. Nous prenons également en compte les discours gouvernementaux et médiatiques liés à cette lutte-antiterroriste. Parmi ces mesures, c'est la surveillance qui est l'objet de notre étude. Le mot surveiller signifie dans le langage commun l'action de veiller particulièrement et avec autorité sur quelque chose ou quelqu'un[1]. David Lyon, auteur majeur des *Surveillance studies*[2], définit la surveillance contemporaine comme « la collecte d'informations, habituellement (mais pas toujours) suivi de leur analyse et utilisation pour des buts de gouvernance sociale, environnementale, économique ou politique[3] ». Parmi les différents types et objectifs de la surveillance,

---

[1] *Le Littré*, Seconde édition, 1878, *sub verbo* « Surveiller »; *Dictionnaire de l'Académie française*, 8ème édition, *sub verbo* « Surveiller ».

[2] « Etudes la surveillance » notre traduction. Champ d'études interdisciplinaire consacré à l'étude et à la critique des mesures de surveillance.

[3] Florent Castagnino, « Critique des surveillances studies. Éléments pour une sociologie de la surveillance » (2018) Vol. 42:1 Déviance Société 9 citant; Kirstie Ball, Kevin D Haggerty et David Lyon, *Routledge handbook of surveillance studies*, coll Routledge international handbooks, Routledge, 2014 à

nous nous concentrerons sur la surveillance étatique, même si une telle division est difficile à faire car l'Etat collabore étroitement avec les entreprises : ainsi nous nous intéressons plus particulièrement à la surveillance qui a pour objet la lutte contre la criminalité et le contrôle social, plutôt que la surveillance opérée à des fins commerciales (*marketing* ciblé), même si cette surveillance est mentionnée au cours du mémoire.

La lutte anti-terroriste et la surveillance de masse sont deux phénomènes parallèles dont le lien n'est pas forcément évident, mais sont en réalité liés en ce qu'ils s'appuient l'un sur l'autre. C'est ce qui nous a tout d'abord interpellé et poussé vers ce sujet, la façon dont le premier justifie le second, alors que la surveillance est utilisée pour des objectifs bien plus larges que la seule lutte anti-terroriste et que ces effets sont particulièrement dangereux. De plus, l'efficacité des techniques de surveillance, pourtant intrusives et liberticides n'est pas prouvée. Le constat de l'ampleur de la surveillance et de ses effets néfastes nous ont conduit à nous interroger sur la légalité d'un tel système dans des Etats dont le régime politique est pourtant la démocratie.

Le contexte de cette recherche regroupe trois éléments. D'une part, l'objectif étatique de lutte anti-terroriste. Après les attentats de Septembre 2001, qui ont profondément changé la perception de la menace terroriste, les politiques gouvernementales ont pris un tournant sécuritaire. De nouvelles lois anti-terroristes ont vu le jour en réaction immédiate aux attentats dans l'ensemble des États, propulsées également par la résolution 1373 du Conseil de sécurité de des Nations Unies, qui demandait aux États

---

la p 1 « The collection, usually (but not always) followed by analysis and application of information within a given domain of social, environmental, economic or political governance ».

de faire état des mesures prises pour lutter contre le terrorisme dans un délai imparti[4]. Si la légitimité de l'objectif n'est pas remise en question, il a pu être constaté qu'il s'agit d'une porte-ouverte à de nombreuses violations de droits de la personne[5], si bien que la Commission des droits de l'Homme des Nations Unies a mis en place un poste de rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste en 2005[6] et le mandat a été renouvelé trois fois depuis[7], ce qui illustre la pertinence de la question. Vingt ans après, la multiplication des attentats et par conséquent celles des déclarations d'état d'urgence n'a pas cessée. Le régime de l'état d'urgence permet aux États des dérogations à certaines libertés, mais est encadré par plusieurs critères, le premier étant d'être limité dans le temps, ce qui n'est régulièrement pas respecté par les États et les mesures censées être temporaires deviennent des lois régulières[8].

---

[4] Conseil de sécurité, *Résolution 1373 sur la menace à la paix et à la sécurité internationales résultant d'actes terroristes*, Doc NU S/RES/1373 (2001).

[5] Michael Head, « Counter-terrorism laws: A threat to political freedom, civil liberties and constitutional rights critique and comment » (2002) 26 Melb Univ Law Rev 666; Imran Awan, « The erosion of civil Liberties: Pre-charge detention and counter-terror laws » (2011) 84 Police J 272.

[6] Commission des droits de l'homme, *Résolution 2005/80 sur la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU E/CN4/RES/2005/80 (2005).

[7] Conseil des droits de l'Homme, *Résolution 15/15 sur la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste: mandat du Rapporteur spécial sur des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU A/HRC/RES/15/15 (2010); Conseil des droits de l'Homme, *Résolution 22/8 sur la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste: mandat du Rapporteur spécial sur des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU A/HRC/22/L15 (2013); Conseil des droits de l'Homme, *Résolution 31/3 sur la Protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste : mandat du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU A/HRC/RES/31/3 (2016).

[8] Fionnula Ni Aoláin, *Rapport de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, concernant les difficultés que présentent pour les droits de l'homme les états d'urgence dans le contexte de la lutte contre le terrorisme*, Doc NU A/HRC/37/52 (2018).

En parallèle, on assiste depuis plusieurs décennies à une croissance exponentielle des technologies de communication et de collecte de données. Cet engouement pour les technologies utilisant l'intelligence artificielle et l'automatisation se traduit par des investissements majeurs, de fonds aussi bien publics que privés, dans le développement de technologies de plus en plus perfectionnées. Ce sont ces mêmes technologies qui vont permettre une surveillance à grande échelle. De pair avec le développement des nouvelles technologies, l'utilisation quotidienne d'Internet par les individus et la production de données conséquente est sans précédent. Le succès relativement récent des réseaux sociaux a créé une ère du partage, où publier des informations sur soi ou ses opinions est banalisé.

Ainsi, ce qui pouvait autrefois être considéré comme relevant de la vie privée ne le sera plus forcément aujourd'hui et dans le même temps des informations qui auraient pu paraître anodines peuvent être bien plus révélatrices lorsqu'elles sont traitées au moyen des technologies dites *Big Data.* Le terme désigne aussi bien la quantité de données numériques collectées que les technologies qui permettent la collecte, le traitement et l'analyse de ces données[9]. En définitive, par le développement de nouvelles technologies et moyens de communication, ainsi que l'utilisation que les individus en font au quotidien, les conceptions de ce qu'est la vie privée ont changé.

Dernièrement, le sujet de la surveillance de masse a pris de l'ampleur dans les médias et le débat public, initié par les révélations d'Edward Snowden, ancien consultant de la

[9] Antoinette Rouvroy, « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives. » [2016] Bureau du comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [STE n°18] 1 à la p 11.

NSA, en 2013[10]. Une énorme de quantité de documents, destinés à l'usage interne par les employés de la NSA, a été transmise aux journalistes Laura Poitras et Glenn Greenwald et ainsi communiquée dans les médias[11]. Cette documentation a révélé une partie de l'ampleur de la surveillance d'Interne, de téléphones portables et autres moyens de communications opérée par la NSA, aussi bien sur les citoyens américains que sur ceux du reste du monde[12]. Depuis, d'autres lanceurs d'alertes ont également pris la parole sur l'étendue de la surveillance dont ils ont pu être témoins. Ce qui revient également régulièrement dans l'actualité est la vulnérabilité des technologies de sauvegarde des données utilisées : pas une semaine ne passe sans qu'une nouvelle fuite de données soit annoncée. Les failles de sécurité des systèmes de collecte et de stockage de données inquiètent et mettent en lumière l'incertitude quant au traitement et à la diffusion des données partagées. Afin d'étudier notre sujet au sein de ce contexte particulier, nous étudierons en grande partie des textes faisant partie des *Surveillance studies*.

Les *Surveillance studies* sont un champ d'études multidisciplinaire consacré à l'étude de la surveillance, rassemblant des auteurs majoritairement anglophones. La multidisciplinarité est justifiée par la complexité et l'ampleur du phénomène de la surveillance[13].

---

[10] Ewen Macaskill et Gabriel Dance, « The NSA files decoded / Edward Snowden's surveillance revelations explained », *The Guardian* (1 novembre 2013), en ligne : The Guardian <http://www.theguardian.com/world/the-nsa-files> (consulté le 28 février 2020).

[11] *Ibid*.

[12] *Ibid*.

[13] Castagnino, *supra* note 3 aux pp 16-17.

Les idées de Michel Foucault imprègnent ce mouvement, notamment celles développées dans *Surveiller et punir*[14] comme la critique du *panoptique*[15], architecture de prison développée par Jeremy Bentham, composée d'une tour centrale permettant de surveiller les détenus sans que ceux-ci puissent savoir quand ils sont surveillés[16]. Le terme panoptique est fréquemment réutilisé par les auteurs des *Surveillance studies* pour expliquer la surveillance contemporaine[17], même si certains auteurs invitent à un dépassement de la notion[18]. On retrouve également l'utilisation du concept foucaldien de la *gouvernementalité* comme mode de gouvernance[19], ce qui a donné naissance à l'idée de *gouvernementalité algorithmique*[20]. Un élément de la gouvernementalité est de viser le contrôle des populations ; à ces fins, la gouvernementalité algorithmique peut être divisée en trois étapes, selon les travaux de la chercheuse Antoinette Rouvroy[21]. Le premier temps est celui de la récolte et de la conservation automatisée en quantité massive de données non triées, aussi appelée « *dataveillance* »[22]. Ensuite, ces données vont être traitées de manière automatisée de manière à faire émerger des corrélations subtiles entre celles-ci : on appelle ce traitement *datamining*[23]. Ces deux

---

[14] Michel Foucault, *Surveiller et punir Naissance de la prison*, Gallimard, coll Tel, 1975.

[15] Michel Foucault, « Le panoptisme » dans *Surveiller et punir*, Gallimard, coll Tel, 1975, 229.

[16] Jeremy Bentham et Miran Božovič, *The panopticon writings*, 2e éd, coll Radical Thinkers, Verso Books, 2011.

[17] David Lyon, *Theorizing surveillance: the panopticon and beyond*, Cullompton, Willan Publishing, 2006.

[18] Kevin D Haggerty et Richard V Ericson, « The surveillant assemblage » (2000) 51:4 Br J Sociol 605.

[19] Michel Foucault, *« La gouvernementalité » ; cours du Collège de France, année 1977-1978 : « Sécurité, territoire et population* », 4e leçon, 1er février 1978), septembre-décembre 1978; Pierre Lascoumes, « La Gouvernementalité : de la critique de l'État aux technologies du pouvoir » [2004] 13-14 Portique Rev Philos Sci Hum.

[20] Antoinette Rouvroy et Thomas Berns, « Gouvernementalité algorithmique et perspectives d'émancipation » (2013) n° 177:1 Reseaux 163 à la p 10.

[21] *Ibid* aux pp 5-9.

[22] *Ibid* à la p 5.

[23] *Ibid* à la p 7.

premières étapes permettent ainsi aux détenteurs de ces savoirs d'avoir une action sur les comportements des individus ou groupes qui sont les sujets des données collectées : à partir d'un profilage, ces informations pourront permettre de prédire ou influencer les comportements des individus concernés [24]. Cette volonté de maitriser tous les évènements liés à la lutte contre la criminalité par une surveillance intensive de tous les individus est caractéristique d'une « culture de contrôle [25]».

Ces objectifs ne sont pas ouvertement dévoilés et lorsqu'il s'agit des gouvernements, l'intensité de la surveillance est justifiée comme nécessaire pour la lutte contre le terrorisme. Le contraste frappant entre le degré de contrôle permis par la surveillance contemporaine de masse et les différentes libertés qui sont garanties aux individus par le droit international des droits de la personne, nous a conduit à nous interroger sur l'efficacité du droit quant à la protection de la population des effets néfastes de cette surveillance. Nous tenterons ainsi par nos recherches de répondre à la question suivante : Le cadre juridique des droits de la personne, notamment celui du droit à la vie privée, est-il adapté pour faire face à la surveillance étatique anti-terroriste de masse, telle qu'elle est opérée par les États des Five-Eyes ?

Pour ce faire, nous avons procédé à une recherche documentaire, afin de parvenir à une compréhension des enjeux de la surveillance étatique à travers les lectures d'auteurs des *Surveillance studies* et autres académiciens, en majorité des professeures et professeurs de droit. Il s'agit d'un mémoire juridique, sans prétention d'être un travail interdisciplinaire, mais qui reste ouvert aux concepts pertinents empruntés à d'autres

---

[24] *Ibid* aux pp 8-9.

[25] Voir David Garland, *The culture of control : crime and social order in contemporary society*, OUP, 2002.

disciplines[26] pour expliquer la surveillance, notamment les sciences sociales et les sciences politiques dans le cadre du champ d'études des *Surveillance studies*. L'ouverture vers ces autres disciplines nous permet de rendre compte de l'étendue des effets de la surveillance, au-delà de ses implications juridiques[27]. Le premier chapitre est entièrement dédié à cette documentation, complétée par des exemples d'actualité et données statistiques lorsque celles-ci illustrent le propos, en établissant des liens entre les thèses de différents auteurs afin d'identifier les enjeux du sujet et problématiques qui devront ensuite être traitées par le droit.

Le second chapitre est ainsi dédié à l'analyse du droit à la vie privée en droit international. Lorsque que le droit au respect de la vie privée est évoqué, à moins qu'il ne soit précisé de quel texte il s'agit, il est question du droit au respect de la vie privée tel qu'il est prévu dans le *Pacte international relatif aux droits civils et politiques*[28]. A noter toutefois que les définitions entre les différents instruments internationaux de droits humains ne sont pas flagrantes, mais qu'elles seront abordées dans le sous-chapitre sur la définition de la vie privée. La définition du droit à la vie privée est un thème important dans la littérature des *Surveillance studies* en ce qu'elle est largement critiquée, notamment pour son caractère vague et indéfini justement.

L'étude du droit est centrée autour de la norme de droit international, même si plusieurs jurisprudences ou lois nationales sont mentionnées : nous limitions nos exemples à

---

[26] Véronique Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, 2e édition, coll Méthodes du droit, Dalloz, 2016 aux pp 159-170.

[27] David Lyon, *Surveillance studies : An overview*, Polity Press, 2007 à la p 21.

[28] *Pacte international relatif aux droits civils et politiques*, 16 décembre 1966, 999 RTNU 171 (entrée en vigueur : 23 mars 1976).

ceux des États des *Five-Eyes* [29] (Canada, États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande) et à la France, ainsi qu'à la jurisprudence européenne. Ce choix s'explique par la volonté d'étudier la surveillance au sein de régimes démocratiques et ainsi d'en souligner les incompatibilités[30]. De plus, la focalisation sur un nombre restreint de pays avec des systèmes juridiques et politiques comparables, possédant des capacités informatiques importantes, puis qui coopèrent entre eux en matière de surveillance, nous permet de conserver une cohérence et de centrer la recherche sur le droit international plutôt que sur une comparaison des différents cadres juridiques pouvant s'appliquer à la surveillance. Si l'objet du mémoire n'est pas d'établir une comparaison, parce que nous évoquerons tout de même des lois, des jurisprudences et des procédures d'États différents, nous gardons à l'esprit les principes directeurs de la recherche en droit comparé, notamment l'importance de réintégrer les termes dans leur contexte juridique, politique, économique et social[31].

L'objet du mémoire est de dévoiler une évolution que nous considérons comme néfaste pour les pays des Five-Eyes sur les libertés des individus et d'étudier les mécanismes prévus en droit pour appréhender ces effets. Ainsi, nous prendrons appui sur les textes de doctrine pour rendre compte des enjeux entourant la surveillance contemporaine. Nous montrerons d'abord que les techniques de surveillance ont grandement évolué et présenterons les caractéristiques de la surveillance automatisée qui la rendent si dangereuse. Nous étudierons ensuite les raisons d'être de cette surveillance, sa relation avec la lutte anti-terroriste et les stratagèmes des lois réprimant le terrorisme,

---

[29] Ewen Macaskill et Gabriel Dance, *supra* note 10.

[30] Nous excluons ainsi les États dans lesquels la surveillance est la composante de régimes totalitaires ou autoritaires, où les droits fondamentaux tels que consacrées par le droit international sont notoirement violés.

[31] Béatrice Jaluzot, « Méthodologie du droit comparé : bilan et prospective » (2005) 57:1 Rev Int Droit Comparé 29 à la p 35.

promulguées massivement à la suite des attentats du 11 septembre. Nous explorerons ensuite l'idéologie de cette surveillance et ses différents effets. Après avoir pris la mesure des différents défis que pose l'encadrement juridique de cette surveillance, sans adopter une analyse législative comparative compréhensive, nous examinerons les lois et politiques des *Five Eyes*. Après avoir mis en lumière les différentes forces et faiblesse du droit à la vie privée, nous envisagerons ensuite les autres cadres juridiques applicables tels que le droit international des droits de la personne et le droit à la protection de ses données personnelles. Enfin, après avoir présenté les failles communes de ces cadres juridiques, nous présenterons les différentes solutions possibles aux manquements du cadre légal entourant la surveillance.

CHAPITRE I

LA SURVEILLANCE AUTOMATISÉE ET LA LUTTE ANTI-TERRORISTE

Dans ce chapitre, nous étudierons dans un premier temps la notion de surveillance et les concepts qui l'entourent (1.1), pour ensuite la lier à lutte anti-terroriste et plus largement à la lutte contre la criminalité (1.2), qui est un des objectifs de l'État et une justification d'outils de surveillance intensive. Nous pourrons ainsi élaborer sur les effets et l'idéologie de cette surveillance de masse (1.3).

1.1. La notion de surveillance et son évolution

Afin de mieux comprendre la surveillance contemporaine, il convient de revenir dans un premier temps aux origines de la surveillance étatique. Nous choisissons ici de nous concentrer sur les grands mouvements de cette évolution en sélectionnant quelques périodes historiques, afin de souligner certaines différences ou similitudes au regard de la surveillance que nous vivons aujourd'hui, que ce soit par les moyens utilisés, dans le contexte historique et politique ou par l'objectif poursuivi. Après avoir présenté ces changements majeurs, nous nous attacherons à définir la surveillance, en nous appuyant sur les écrits des auteurs des *Surveillance studies.* Enfin, en partant des idées et concepts qui structurent la surveillance, nous distinguerons la surveillance traditionnelle et la surveillance contemporaine. Pour ce faire, nous étudierons la

différence des moyens utilisés pour la surveillance et montrerons à quel point ils modifient sa définition théorique.

1.1.1. L'évolution historique de la surveillance étatique : de la surveillance traditionnelle à la surveillance automatisée

La surveillance des citoyens par l'État remonte à l'Antiquité. La première forme d'un système secret de surveillance peut être retracée au premier siècle avant notre ère, lors duquel l'empereur Auguste a mis en place le premier service de poste national : le *cursus publicus* [32]. Le système était en fait destiné à être un service de renseignement[33]. L'objectif poursuivi par la mise en place du service était d'être informé de toutes les communications dans chaque province, afin de pouvoir prédire les rébellions [34]. L'empereur était lui-même à la tête de ce service [35]. Les moyens mis en place furent conséquents. Les coursiers furent d'abord des volontaires, pour ensuite devenir des professionnels. Le réseau nécessita également la construction de routes, puis se développa par la voie navale. La mise en place d'autant de moyens financiers démontre l'importance qui était accordée au renseignement.

Au XVIIIe siècle en France, une autre institution de surveillance a vu le jour : le cabinet du secret des postes, couramment appelé « Cabinet noir ». L'institution a été mise en

---

[32] Hans-Georg Pflaum, « Essai sur le cursus publicus dans le Haut-Empire » (1940) 14:1 Mémoires présentés par divers savants étrangers à l'Académie 189.

[33] *Ibid* à la p 213.

[34] *Ibid*.

[35] William Smith et William Wayte, *A dictionary of Greek and Roman antiquities*, John Murray, London, 1890, *sub verbo* « cursus publicus », en ligne : A Dictionary of Greek and Roman Antiquities <http://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.04.0063:entry=cursus-publicus-cn> (consulté le 11 février 2020).

place sous Louis XIV[36] ; plusieurs employés, d'abord quatre, puis une vingtaine[37], étaient chargés d'ouvrir le courrier, afin d'intercepter tout message séditieux. Les lettres étant cachetées, il fallait d'abord prendre l'empreinte du cachet, puis il fallait amollir le cachet avec de l'eau tiède, pour ensuite cacheter la lettre à nouveau une fois lue[38]. L'auteur de l'entrée Cabinet noir dans le Grand dictionnaire universel qualifie cette entreprise d'« inquisition épistolaire»[39]. Ses activités auraient perduré jusqu'à la fin du XIX siècle, après l'extension de la réforme postale britannique à la France, qui impliqua l'institution du port-payé à bas prix et par conséquent l'augmentation considérable du nombre de lettres[40].

L'invention de nouveaux moyens de communication bénéficia à l'espionnage lors des guerres mondiales du XXe siècle, où la surveillance intensive est ici légitimée par des objectifs militaires en temps de conflit armé international[41]. Les inventions

---

[36] Pierre Larousse, *Grand dictionnaire universel du XIXe siècle*, Tome 3, 1867, *sub verbo* « cabinet noir », en ligne : Grand dictionnaire universel du XIXe siècle <https://gallica.bnf.fr/ark:/12148/bpt6k507258> (consulté le 11 février 2020).

[37] *Ibid*.

[38] *Ibid*.

[39] *Ibid*.

[40] Alexis Belloc, *Les postes françaises : recherches historiques sur leur origine, leur développement, leur législation*, Paris, 1886 à la p 504, en ligne : <https://gallica.bnf.fr/ark:/12148/bpt6k94475s> (consulté le 14 février 2020).

[41] Sébastien-Yves Laurent, *Le secret de l'État. Surveiller, protéger, informer XVIIe-XXe siècle*, Nouveau Monde, 2015; Andreas Marklund, « Communications surveillance during World War I », *Encyclopédie pour une histoire nouvelle de l'Europe* (2016), en ligne : Encyclopédie pour une histoire nouvelle de l'Europe <http://ehne.fr/en/node/1305> (consulté le 4 avril 2020); Elizabeth Bruton et Paul Coleman, « Listening in the dark: audio surveillance, communication technologies, and the submarine threat during the First World War » (2016) 32:3 Hist Technol 245; Daniel Münzner, « The surveillance of friends: MI5 and friendly aliens during the Second World War » (2014) 13:2 J Intelligence Hist 131.

technologiques de l'époque sont mises au service de l'État : le télégramme, la mise sur écoutes des câbles téléphoniques et la mise sur écoute de certains appartements[42].

Cependant le système de surveillance étatique le plus cité de la première moitié du XXe siècle s'est déroulé après la seconde guerre mondiale dans l'ancienne République Démocratique Allemande (RDA), où la Stasi[43] a notoirement traqué les opposants à l'occupation soviétique, en mettant en place un système de surveillance dont l'intensité était sans précédent. C'est en février 1950, seulement quelques mois après la proclamation de la RDA que le Ministère pour la Sécurité Nationale, connue sous le nom de Stasi, a été fondé[44].

La Stasi a un grand nombre d'employés, mais la collecte d'informations est aussi faite en grande partie par des informateurs volontaires[45]. Les raisons de leur implication sont multiples ; elles peuvent être idéologiques, mais les informateurs tirent surtout des avantages de leur coopération[46]. Une des stratégies de la surveillance mise en place par la Stasi est qu'elle ne se base pas sur la force ou la mise en place de lois et d'obligations (même si la force est également employée quand le premier moyen échoue), mais sur le consentement de la population[47]. La volonté de la Stasi était de créer un système de surveillance panoptique discipliné, qui remplacerait la terreur staliniste par des citoyens

---

[42] *Ibid*.

[43] Le terme est une contraction de l'allemand « *Staatssicherheit* », le nom du Ministère, littéralement traduit par la « sécurité de l'État ».

[44] Andreas Lichter, Max Löffler et Sebastian Siegloch, « The long-term costs of government surveillance: Insights from Stasi spying in east Germany » (2019) Discussion Paper No.19-049 ZEW-Center for European Economic Research à la p 7.

[45] *Ibid*.

[46] *Ibid* à la p 8.

[47] Steven Pfaff, « The limits of coercive surveillance: Social and penal control in the German Democratic Republic » (2001) 3:3 Punishm Soc 381 à la p 282.

« autosurveillés[48]», autonomes et socialistes[49]. Au sein de ce régime politique totalitaire, la fonction de ce ministère était très nettement le contrôle social et ce en éliminant toute dissidence. Ce pari sur l'auto-restriction plutôt que sur la coercition, c'est selon l'analyse de Foucault, celui fait par l'État moderne pour remplacer le pouvoir absolu et inefficace du monarque[50].

Quant aux effets de la surveillance opérée par la Stasi sur la population, une corrélation a pu être établie entre l'intensité de la surveillance et le taux de participation aux élections : l'intensité de la surveillance réduit la probabilité que les individus participent aux élections[51]. Il en est de même pour l'intérêt et l'engagement politique[52].

Les moyens techniques disponibles évoluent drastiquement à l'aube du XXIe siècle avec la naissance et le développement d'Internet. Dès les années 1950 et 1960, l'augmentation de sondages et enquêtes a cherché à rendre la société de masse d'après-guerre intelligible en tant que consommateurs pour les chercheurs, les enquêteurs politiques et les mercaticiens[53]. Arrivé aux années 1980, l'enregistrement des transactions des consommateurs telles que les achats par carte de crédit et les appels téléphoniques était largement automatique.

---

[48] Notre traduction de l'anglais *self-policing*, qui pourrait aussi se traduire par « autocontrôlés » dans ce contexte.

[49] Pfaff, *supra* note 47 à la p 382.

[50] Foucault, *supra* note 14 aux pp 154-155.

[51] Lichter, Löffler et Siegloch, *supra* note 44 à la p 20.

[52] *Ibid*.

[53] Sarah Myers West, « Data capitalism: Redefining the logics of surveillance and privacy » (2019) 58:1 Bus Soc 20 à la p 25.

Certains lient l'essor de la surveillance des données à l'éclatement de la «*dotcom bubble*[54]». La *dotcom bubble*[55] est le nom donné à la bulle spéculative autour des compagnies Internet au cours des années 1990, qui a fini par éclater sous la forme d'un krach boursier en 2001. La réelle valeur du commerce électronique était minimale, mais l'intérêt des investisseurs était grandissant[56]. La combinaison d'attentes croissantes et d'une migration vers Internet plus lente qu'anticipée, a conduit à l'éclat de la bulle *dotcom*[57]. Après la chute, les compagnies cherchent de nouveaux moyens d'exploiter Internet. Il avait été constaté qu'une grande quantité de données étaient disponibles via le commerce électronique ; chaque clic et chaque courriel créait une trace, mais à l'époque personne ne savait comment elles pourraient être utiles[58]. Les analystes prédisaient alors que ces données pourraient devenir une ressource importante[59].

C'est ainsi que certaines technologies ont été recyclées après le krach pour la surveillance, comme par exemple les *cookies*[60]. Ces traqueurs étaient à l'origine conçus pour permettre à un site de vente en ligne de se « souvenir » des éléments dans le panier d'achat d'un visiteur[61]. Certains avaient déjà alerté sur les potentielles utilisations de cette technologie, les cookies avaient été décrits comme des « interrogateurs silencieux », ayant la capacité de cibler les utilisateurs individuellement[62]. Les entreprises tierces

---

[54] Eli Ofek et Matthew Richardson, « Dotcom mania: The rise and fall of internet stock prices » (2003) 58:3 J Finance 1113 aux pp 1113-1114.

[55] *Ibid.*

[56] West, *supra* note 53 à la p 25.

[57] *Ibid*.

[58] *Ibid* à la p 26.

[59] *Ibid*.

[60] *Ibid* à la p 27.

[61] *Ibid*.

[62] *Ibid*.

ont ensuite commencé à payer pour la permission de placer des cookies sur des pages appartenant à d'autres sites, ce qui créa la possibilité de suivre les utilisateurs dans leurs mouvements sur Internet[63]. Ces outils technologiques commerciaux ont fait l'objet d'une reprise par l'État pour ses propres objectifs.

L'étude historique des moyens utilisés pour la surveillance n'est pas anodine, parce que ceux d'aujourd'hui diffèrent profondément de ce qui était fait à une époque pré-digitale. Avant l'émergence de technologies de surveillance, il existait une certaine prévisibilité de ce qui pouvait être récolté : on a une idée de l'information qui risque d'être interceptée quand on écrit une lettre. On peut prendre ses précautions. Parce que la collecte d'information en masse permet à un algorithme de faire des corrélations que le sujet des données n'est pas en mesure de faire, l'intrusion est double. C'est la collecte de ce que je sais qui est secret, ce que je veux cacher, mon intimité et au-delà de ça, de ce que je ne sais même pas encore de moi-même ; ce qui m'incrimine et joue en ma défaveur sans même que je sois informé de la cause de cette discrimination, que ce soit pour du crédit ou pour de l'assurance santé, ou mon placement sur des listes de personnes qui sont susceptibles de commettre une infraction.

Comme nous le verrons dans les parties suivantes, c'est l'émergence d'une surveillance globale qui fonctionne en partenariat, que ce soit entre États ou entre l'État et le secteur privé.

---

[63] *Ibid* à la p 28.

1.1.2. La définition poreuse de la surveillance

Le champ d'études au sein duquel peut être définie et analysée la surveillance porte le nom de *Surveillance studies*. Ce domaine d'études a émergé en tant que tel dans les années 1950 et a pris de l'ampleur, aussi bien dans son traitement par les universitaires, que dans l'attention qui lui a été accordée par l'opinion publique, après les attentats du 11 septembre[64]. Ce champ multidisciplinaire regroupe un grand nombre de théories et de concepts. Nous n'en ferons pas une énonciation exhaustive mais sélectionnons les cadres qui vont nous permettre d'appréhender et d'expliquer au mieux la surveillance contemporaine.

Dans son ouvrage *Surveillance studies : An overview*, David Lyon propose la définition suivante pour la surveillance : « *the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction*[65]». On peut cependant s'interroger sur le caractère encore pertinent de la mention d'une focalisation comme caractéristique de la surveillance, au vu des principes contemporains de collecte en masse de données. Reste que la surveillance est toujours articulée en fonction d'objectifs spécifiques[66]. Ces objectifs varient, mais elle est majoritairement, dans la lignée de Foucault, liée au contrôle[67]. La surveillance implique généralement une différence de pouvoir et renforce un déséquilibre en faveur des plus puissants[68]. On peut ainsi distinguer l'agent de la surveillance, celui qui exerce la

---

[64] Gary T Marx, « Surveillance studies » dans James D Wright, dir, *International encyclopedia of the social & behavioral sciences (Second Edition)*, Oxford, Elsevier, 2015, 733 à la p 734.

[65] David Lyon, *supra* note 27 à la p 14.

[66] *Ibid*.

[67] Marx, *supra* note 64 à la p 735.

[68] *Ibid*.

surveillance, du sujet de la surveillance, celui qui est surveillé[69]. Le rôle d'agent de la surveillance peut ensuite être subdivisé entre utilisateur premier ou secondaire des données récoltées[70].

Leman-Langlois identifie trois caractéristiques de la surveillance[71]. Premièrement, elle peut être décrite de manière générale comme un processus d'acquisition d'information[72]. Deuxièmement, l'acquisition d'information porte sur des « objets sociaux », soit les individus et les objets dont ils sont responsables[73]. Troisièmement, l'objectif est l'obtention d'un bénéfice extérieur à la simple collecte d'information[74].

Marx propose lui une définition très large de la surveillance. Elle serait le regard ou l'attention envers autrui, autrui pouvant être une personne ou un groupe, avec comme caractéristique centrale la collecte de données qui peuvent être rattachées à des individus[75]. La volonté de vouloir trouver une définition qui s'applique à toutes les situations de surveillance résulte en une définition dont tous les termes sont indéterminés[76]. Il convient de se demander si, étant donné que la surveillance est un phénomène d'une grande ampleur, qui peut prendre diverses formes et être opéré pour

---

[69] *Ibid* à la p 737.

[70] *Ibid*.

[71] Stéphane Leman-Langlois, *Sphères de surveillance*, coll Régulation sociale, Montréal, Les Presses de l'Université de Montréal, 2011 aux pp 10-11.

[72] *Ibid* à la p 10.

[73] *Ibid*.

[74] *Ibid* à la p 11.

[75] Marx, *supra* note 64 à la p 734.

[76] Castagnino, *supra* note 3 à la p 22.

des objectifs multiples, il n'est pas nécessaire de subdiviser le concept de surveillance en plusieurs types de surveillances.

Le terme panoptique revient régulièrement dans la littérature des études de la surveillance. Il désigne à l'origine une architecture de centre pénitentiaire imaginée par Jeremy Bentham, permettant à un seul surveillant d'observer chaque cellule, sans que les détenus puissent voir quand ils sont surveillés[77]. Ainsi, même s'ils ne sont pas surveillés en permanence, le fait qu'ils ne sachent pas quand ils sont surveillés les oblige à se comporter comme s'ils l'étaient en permanence. Cette architecture suit l'idée de Bentham selon lequel le pouvoir doit être visible mais invérifiable[78].

Selon Michel Foucault, qui a ensuite théorisé ce concept dans le cadre de ses études sur le pouvoir et la gouvernementalité, l'effet majeur du panoptique est « d'induire chez le détenu [la personne surveillée] un état conscient et permanent de visibilité, qui assure le fonctionnement automatique du pouvoir[79]». Cette structure permet ainsi à la surveillance d'être « permanente dans ses effets, même si elle est discontinue dans son action[80]». Ainsi, le panoptique est un dispositif important, car il désindividualise et automatise le pouvoir[81].

Si la métaphore du panoptique est un concept fondamental au sein des *surveillance studies*, certains invitent à un dépassement de cette notion, considérée comme obsolète

---

[77] Bentham et Božovič, *supra* note 16.

[78] Foucault, *supra* note 14 à la p 235.

[79] Michel Foucault, *supra* note 15 à la p 234.

[80] *Ibid*.

[81] *Ibid* à la p 235.

au vu de la structure de la surveillance contemporaine[82]. En effet, l'architecture originale du panoptique, puis sa reprise par Foucault, suggère un seul poste d'observation central. Pour Bentham, c'est le surveillant du centre pénitentiaire qui occupe cette place ; pour Foucault, c'est l'État. Mais cette image n'est plus parfaitement adéquate quand on sait que les acteurs sont multiples et qu'il n'y a pas forcément de liens d'autorité entre l'agent de la surveillance et les sujets de la surveillance. Pour pallier cette représentation erronée, Haggerty et Ericson ont développé le concept de « *surveillant assemblage*[83] ». Ici, l'idée d'un centre de surveillance est substituée par celle d'une multitude d'éléments surveillants, organisés selon une structure non hiérarchique et dont la puissance réside dans les diverses connexions qui peuvent être faites[84].

Une seconde critique apportée par Castagnino sur l'utilisation du concept de panoptique pour décrire la surveillance, est que, surtout si l'on en suit l'interprétation faite par Foucault, l'attention est emmenée sur les effets négatifs de la surveillance[85]. Cela rejoint une critique plus générale adressée aux auteurs des *surveillance studies*, qui est celle d'une ontologie négative postulée[86]. Il y trouve un postulat qui considère la surveillance comme quelque chose de dangereux en soi, ce qui signifie que les analyses concluront forcément au caractère liberticide des pratiques de surveillance[87]. Il y ajoute que certains textes présentent un regard sur les nouvelles technologies qui s'approche de la technophobie et appelle à une approche plus nuancée des nouvelles

---

[82] Castagnino, *supra* note 3 à la p 24.

[83] Haggerty et Ericson, *supra* note 18 aux pp 608-610.

[84] Castagnino, *supra* note 3 à la p 24.

[85] *Ibid*.

[86] *Ibid* à la p 13.

[87] *Ibid*.

technologies en précisant que la surveillance n'est pas dangereuse parce qu'elle est technologique[88].

1.1.3. L'entrée dans l'ère post-panoptique : l'oxymore de Snowen (*Target everyone*)

La différence entre la surveillance « traditionnelle » et la surveillance « automatisée » n'est pas la simple utilisation de nouvelles technologies, mais la combinaison de plusieurs caractéristiques[89]. La première est que la focalisation sur les métadonnées autant que sur le contenu[90]. Les métadonnées sont les données à propos des données, c'est à dire les données qui décrivent ou définissent une autre donnée ; elles sont souvent générées automatiquement[91]. Par exemple, les métadonnées peuvent être des données à propos de la localisation, de la provenance de données, la durée, le moment ou le volume d'une communication, 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 à un réseau[92].

La seconde spécificité de cette nouvelle surveillance est qu'elle opère sur un principe de « collecte en masse, accès en détail [93]». La collecte de données en masse est permise par l'utilisation d'un ensemble de technologies appelé les « Big Data ». Le terme Big Data renvoie autant aux masses de données numériques complexes à accumulation

---

[88] *Ibid* à la p 25.

[89] Paul Bernal, « Data gathering, surveillance and human rights: recasting the debate » (2016) 1:2 J Cyber Policy 243 à la p 246.

[90] *Ibid*.

[91] Rouvroy, *supra* note 9 à la p 8.

[92] *Ibid*.

[93] Bernal, *supra* note 89 à la p 246.

rapide, qu'à l'ensemble des techniques logicielles d'analyse de ces données (par exemple : *Data mining*, *machine learning*, *social network analysis*, *predictive analytics*)[94]. L'objectif poursuivi par l'utilisation de ces technologies d'analyse est la détection de relations subtiles, qui seraient autrement restées imperceptibles, entre des données hétérogènes récoltées dans des contextes différents[95]. Ces corrélations vont permettre de faire surgir des catégories, des modèles ou des profils[96].

La troisième particularité de cette surveillance est qu'elle fonctionne en coopération entre l'État et les collecteurs de données commerciales[97]. On peut ajouter que les États coopèrent aussi entre eux lorsqu'il s'agit d'échanger des informations issues de la surveillance. L'exemple le plus cité d'une telle alliance interétatique est l'alliance des *Five Eyes*, créée par un accord entre le Canada, les Etats-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande, qui prévoit un échange d'informations d'intelligence[98]. Le traité était destiné à être secret mais son existence a été publiée au sein des révélations d'Edward Snowden de 2013[99]. De nouvelles révélations sur des alliances de surveillance entre États continuent de faire surface, comme par exemple

---

[94] Rouvroy, *supra* note 9 à la p 11.

[95] *Ibid*.

[96] *Ibid*.

[97] Bernal, *supra* note 89 aux pp 246-247.

[98] « Privacy international files lawsuit to compel disclosure of secretive 1946 surveillance sgreement », *Privacy International* (1 novembre 2017), en ligne : Privacy International <https://privacyinternational.org/press-release/116/privacy-international-files-lawsuit-compel-disclosure-secretive-1946-surveillance> (consulté le 28 février 2020); David Lyon, *Surveillance after Snowden*, Polity Press, 2015 à la p 8 ; « Five Eyes Integration and the Law », (22 avril 2015), en ligne: *Priv Int* <http://privacyinternational.org/fr/node/1672> (consulté le 10 juin 2020). : la nature de cette entente est non juridique, dans le sens où il ne s'agit pas formellement d'un traité, rendu public, mais d'une entente entre les services de renseignements de plusieurs États.

[99] Ewen Macaskill et Gabriel Dance, *supra* note 10.

récemment sur l'alliance européenne « Maximator » dont les 5 membres sont l'Allemagne, le Danemark, la France, les Pays-Bas et la Suède[100].

Dans le contexte de la surveillance des données (*dataveillance*[101]), on peut distinguer trois phases[102]. La première phase est celle de la collecte des données. La seconde phase est celle de l'analyse des données par l'algorithme. Ces deux premières phases sont automatisées. La troisième phase est celle de l'intervention humaine, où un individu va prendre connaissance des trouvailles de l'algorithme[103]. Une question récurrente est donc celle du moment où débute réellement la surveillance : est-ce dès la collecte des données, ou alors faut-il qu'il y ait une intervention humaine ?

La surveillance contemporaine a pu être qualifiée de « post-panoptique[104] », pour désigner notamment une surveillance qui s'appuie sur la prédiction plutôt que sur l'observation[105]. Cette prédiction des comportements humains est permise par l'utilisation des technologies des Big Data. Le caractère post-panoptique pourrait aussi se situer davantage dans la façon dont les individus cèdent leurs données personnelles. En effet, une question importante en droit qui sera explorée dans le second chapitre de ce mémoire est celle de savoir si les individus communiquent volontairement leurs données personnelles. Cela peut être pour en tirer certains avantages, comme par

---

[100] Bart Jacobs, « Maximator: European signals intelligence cooperation, from a Dutch perspective » (2020) 0:0 Intell Natl Secur 1.

[101] Jose van Dijck, « Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology » (2014) 12:2 Surveill Soc 197.

[102] Bernal, *supra* note 89 à la p 249.

[103] *Ibid*.

[104] Zygmunt Bauman et David Lyon, *Liquid surveillance: a conversation*, coll Polity conversations series, Cambridge, UK ; Malden, MA, Polity Press, 2013 aux pp 49-67.

[105] Kyle Kubler, « State of urgency: Surveillance, power, and algorithms in France's state of emergency » (2017) 4:2 Big Data Soc 1 à la p 7.

exemple pour obtenir des réductions avec une carte de fidélité, ou pour l'obtention de services toujours plus personnalisés. De plus, l'émergence des réseaux sociaux et de tous les moyens connectés par lesquels nous documentons et partageons notre quotidien crée aussi une quantité gigantesque de données, ce qui a pu être expliqué par le concept de « société de l'exposition [106]».

L'intensité de cette surveillance et la variété des moyens employés sont souvent justifiées par les gouvernements par la nécessité d'assurer la « sécurité nationale » et souvent plus précisément, la lutte contre le terrorisme du XXIe siècle.

1.2. La transformation de la lutte anti-terroriste

Il convient de contextualiser la lutte anti-terroriste, tout d'abord en présentant certaines évolutions du terrorisme lui-même. Nous étudierons ensuite la cadre juridique de la lutte anti-terroriste et la façon dont il s'est construit en réponse précipitée à l'ampleur des attaques terroristes et aux nouvelles méthodes des organisations terroristes. Après avoir établi ce lien, nous montrerons comment ce terrorisme nouveau est utilisé comme justification absolue du recours à une surveillance intensive de l'ensemble de la population.

1.2.1 Le terrorisme post 9.11 : un phénomène ancien, une ampleur nouvelle

Le terrorisme n'est pas un phénomène nouveau : de nombreux attentats ont eu lieu partout dans le monde avant le début du XXIe siècle. Cependant, les attentats du 11

---

[106] Bernard E Harcourt, *Exposed: Desire and disobedience in the digital age*, Harvard University Press, 2015.

septembre 2001 ont profondément changé la perception du terrorisme, en particulier pour les occidentaux. A la suite de ces attaques, une multiplication de la fréquence des attentats dans le monde a pu être observée, ainsi que la revendication d'une grande partie des attentats par une même entité, l'État islamique, bien qu'il convient de rappeler que c'est loin d'être la seule forme de terrorisme contemporaine, même si c'est celle qui retient le plus l'attention des gouvernements, des médias et donc du public.

Si le développement des nouvelles technologies de l'information a permis une expansion de la surveillance, ce développement sert aussi les organisations terroristes[107]. Les groupes terroristes utilisent Internet pour diverses raisons qui ont été catégorisées par de nombreux auteurs[108]. En premier lieu, la diffusion d'information subjective et de propagande. On parle aussi de « *psychological warfare* » par la diffusion, notamment, de vidéos choquantes d'exécution d'otages[109]. Le fait que les organisations terroristes puissent librement diffuser leurs messages sur le Web, se passant des critères de sélection qui pourraient s'appliquer sur des chaînes d'information, leur donne une liberté de façonner leur image sans précédent[110].

Deuxièmement, internet est largement utilisé par les organisations terroristes pour leur financement[111]. La troisième utilisation est la communication au sein des groupes ou entre groupes, qui est maintenant plus rapide, plus économique et plus sécurisée grâce

---

[107] Maura Conway, « Terrorism and the internet: New media—new threat? » (2006) 59:2 Parliam Aff 283 à la p 783.

[108] Gabriel Weimann, « www.terror.net : How modern terrorism uses the internet » Special Report 116 U S Institute of Peace 1; Timothy L Thomas, « Al Qaeda and the internet: The danger of "cyberplanning" » (2003) 33:1 Parameters 112; John Curtis Amble, « Combating terrorism in the new media environment » (2012) 35:5 Studies in Conflict & Terror 339.

[109] Conway, *supra* note 107 à la p 285.

[110] *Ibid* à la p 284.

[111] *Ibid* à la p 285.

à de nouvelles technologies d'information[112]. La quatrième des utilisations principales est le recrutement et la propagande de radicalisation[113]. Les groupes terroristes peuvent également, au même titre que les entreprises et les États, collecter un grand nombre d'information. Les technologies de collection et d'analyse de données sont aussi utilisées par les organisations terroristes[114].

Un tournant du XXIe siècle a également été le traitement médiatique des attentats et des menaces terroristes. La couverture des attentats par les médias est massive. Il a pu être démontré largement que les médias jouent un rôle de premier plan dans la peur du crime et la perception du risque de la population[115]. En études de la communication, la théorie de « *cultivation hypothesis* » suggère que la fréquence de consommation de médias qui insistent de manière disproportionnée sur la violence et les événements extrêmes, conduit les auditeurs à avoir une vision du monde déformée, qui reflète ce qui est présenté à la télévision plutôt que la réalité[116].

La façon dont les médias construisent leurs reportages sur le terrorisme peut avoir de sérieuses implications politiques, comme le soutien accru de politiques punitives et des restrictions aux libertés civiles qui n'auraient pas été soutenues autrement[117]. Certaines études ont permis de démontrer un lien entre le risque perçu que soi ou ses proches puissent être victimes d'un attentat et le nombre d'heures passées à écouter les chaînes

---

[112] *Ibid* à la p 287.

[113] *Ibid* à la p 289.

[114] *Ibid* à la p 290.

[115] Ashley Marie Nellis et Joanne Savage, « Does watching the news affect fear of terrorism? The importance of media exposure on terrorism fear » (2012) 58:5 Crime Delinquency 748 à la p 749.

[116] *Ibid*.

[117] *Ibid* à la p 763.

d'information à la télévision[118]. Par ailleurs, on peut noter que le fait que les revenus des chaînes télévisées dépendent du nombre d'auditeurs peut les inciter à publier des images ou opinions plus choquantes pour augmenter leur auditorat[119].

L'ampleur prise par les organisations terroristes et les changements dans leurs modes d'opération, ainsi que la façon dont les attentats et menaces sont relayés dans les médias, ont également eu une incidence sur le cadre juridique qui régit la lutte anti-terroriste et la protection des droits des personnes accusées de terrorisme.

1.2.2. Le cadre juridique de la lutte anti-terroriste marqué par l'urgence

Pour une majorité marquée de l'opinion experte, le terrorisme ne fait pas partie des crimes de droit pénal international[120] et il n'y a donc pas de définition du terrorisme qui peut être universellement employée en droit international[121]. La lutte contre le terrorisme a fait l'objet de plusieurs conventions internationales. Mais il revient aux États de criminaliser le terrorisme dans leur propre législation[122]. Le droit international des droits humains régit l'atteinte qui peut être permise par ces mesures. Une des difficultés concernant la lutte contre le terrorisme en droit international est justement le manque d'une définition complète et globale du terrorisme[123]. La conséquence de ce

---

[118] *Ibid* aux pp 759-761.

[119] *Ibid* à la p 764.

[120] Jan Klabbers, *International law*, 2nd edition, Cambridge UK ; New York, Cambridge University Press, 2017 à la p 243 ; Neil Boister, « "Transnational Criminal Law"? » (2003) 14:5 Eur J Int Law 953 à la p 962; Kai Ambos, *Treatise on International Criminal Law: Volume 1: Foundations and General Part*, Oxford, New York, Oxford University Press, 2013 à la p 54..

[121] Andrea Bianchi, dir, *Enforcing international law norms against terrorism*, 1st edition, Oxford, Hart Publishing, 2005 à la p 146.

[122] *Ibid* à la p 11.

[123] Ni Aoláin, *supra* note 8 à la p 3.

manque d'une définition unifiée est l'adoption de définitions très larges du terrorisme par les États, ce qui met en péril le respect des droits humains.

Le droit international

Le droit international reconnaît le caractère permissible de certaines restrictions à certains droits et libertés pendant des situations d'urgence et autorise les gouvernements à prendre les mesures qui sont nécessaires, proportionnées, et consistantes avec les obligations de droit international[124]. Ce n'est donc pas en soi l'état d'urgence qui est problématique, mais le non-respect des limites imposées à cet effet par le droit international.

Il y a deux régimes possibles pour restreindre les libertés : celui de la dérogation, et celui des limitations[125]. Premièrement, s'agissant de la dérogation. Une caractéristique commune aux traités internationaux de droits humains majeurs est qu'ils prévoient explicitement des dérogations en temps de crise. Chaque traité requiert que l'ampleur de la menace doive être exceptionnelle et affecter la capacité fondamentale de l'État de fonctionner de manière effective[126]. Avant qu'un État invoque une dérogation, deux conditions fondamentales doivent être remplies : la situation doit être une urgence qui menace la vie de la nation et l'État doit avoir officiellement proclamé un état d'urgence[127].

---

[124] *Ibid*.

[125] Viktor Mavi, « Limitations of and derogations from human rights in international human rights instruments » (1997) 38 Acta Juridica Hung 107.

[126] Ni Aoláin, *supra* note 8 à la p 4.

[127] *Ibid* à la p 5.

Par exemple, les mesures dérogatoires au PIDCP doivent être limitées aux exigences de la situation[128]. Les tribunaux interprètent cette exigence comme étant applicable à la durée, l'aire géographique et le champ matériel de l'état d'urgence[129]. Il a également été précisé par le Comité des Droits de l'Homme qu'une urgence pourra justifier une dérogation seulement si les circonstances pertinentes sont d'une nature exceptionnelle et temporaire[130]. Il incombe à l'État de prouver que ces conditions ont été remplies[131].

En parallèle, le régime des limitations peut aussi être employé. La Déclaration universelle des droits de l'Homme et les traités de droits humains autorisent les États à restreindre partiellement la pleine jouissance des droits humains par des clauses de limitation, dont l'étendue est spécifiée et pour des objectifs raisonnables quand certaines conditions sont remplies[132]. Les limitations doivent premièrement être nécessaires. Deuxièmement, elles doivent affecter minimalement les droits : ce principe porte le nom de l'alternative la moins restrictive. Troisièmement, l'État doit démontrer une proportionnalité entre les moyens et les objectifs clairement exprimés et enfin quatrièmement, les limitations doivent être cohérentes avec les autres droits fondamentaux et non-discriminatoires dans leurs objectifs et leurs pratiques[133].

---

[128] PIDCP *supra* note 28 art 4.

[129] Ni Aoláin, *supra* note 8 à la p 4.

[130]Comité des droits de l'Homme, *Observation générale n°29 : États d'urgence (article 4)*, Doc NU CCPR/C/21/Rev1/Add11 (2001) au para 2.

[131] Jaime Oràà, *Human rights in states of emergency in international law*, Oxford, Clarendon Press, 1992 à la p 21.

[132] Ni Aoláin, *supra* note 8 à la p 4.

[133] Voir Alexandre Kiss, « Permissible limitations on rights » dans *The International Bill of Rights: the Covenant on Civil and Political Rights*, Louis Henkin, New York, Columbia University Press, 1981.

Les limitations sont conceptuellement plus étroites que les dérogations et ont été pensées pour atteindre des objectifs spécifiques pour certains but démocratiquement justifiables[134]. Par exemple, un droit peut être limité lorsqu'il entre en conflit avec un autre droit[135]. Certains droits, nommés droits absolus ne peuvent pas voir leur violation justifiée, comme la prohibition de la torture par exemple[136].

Le droit national

Pour la majorité des États, l'autorité de l'exercice des pouvoirs d'urgence se trouve dans leur Constitution [137] . Une caractéristique commune des constitutions est d'énumérer les circonstances qui méritent la proclamation d'un état d'urgence. Le législatif délègue ensuite des pouvoirs spéciaux à l'exécutif pour répondre aux exigences d'une urgence particulière. Généralement, ce modèle permet à ces pouvoirs spéciaux d'expirer une fois l'urgence finie[138]. En pratique, le défi pour la protection des droits humains a été l'absorption d'un statut d'urgence dans le cadre législatif ordinaire, incluant la législation anti-terroriste, qui normalise l'exception[139].

On parle dans ce cas d'états d'urgence cachés ou *de facto*, lorsque bien que les mesures ne soient pas prises dans le cadre légal de l'état d'urgence, mais par une loi ordinaire,

---

[134] Ni Aoláin, *supra* note 8 à la p 4.

[135] Klabbers, *supra* note 120 à la p 125.

[136] *Ibid* à la p 123.

[137] Ni Aoláin, *supra* note 8 à la p 6.

[138] *Ibid*.

[139] John Ferejohn et Pasquale Pasquino, « The law of the exception: A typology of emergency powers » (2004) 2:2 Int J Const Law 210 aux pp 210-239.

leur étendue et leur caractère est exceptionnel[140]. Ainsi, la déclaration officielle d'un état d'urgence est contournée[141].

Cela dit, même lorsque l'état d'urgence est déclaré, certains risques sont présents pour la protection des droits humains. Premièrement, la définition du terrorisme est souvent très large, couplée aux termes « extrémisme » et « radicalisation », qui sont aussi indéterminés[142].

Par exemple au Canada, l'article 83.01 du *Code criminel* définit le terrorisme comme un acte commis « au nom — exclusivement ou non — d'un but, d'un objectif ou d'une cause de nature politique, religieuse ou idéologique[143] » en vue d'intimider la population « quant à sa sécurité, entre autres sur le plan économique, ou de contraindre une personne, un gouvernement ou une organisation nationale ou internationale à accomplir un acte ou à s'en abstenir[144]». Ainsi, cette définition inclut le fait de causer des dommages matériels considérables et perturber gravement ou de paralyser des services, installations ou systèmes[145]. Certains auteurs soulignent ainsi que si une majorité des personnes pourraient s'entendre sur le fait que le terrorisme peut être

---

[140] Ni Aoláin, *supra* note 8 aux pp 9-10.

[141] *Ibid* à la p 10.

[142] *Ibid*.

[143] *Code Criminel*, Canada, LRC 1985, c. C-46 art 83.01.

[144] *Ibid*.

[145] Gouvernement du Canada Ministère de la Justice, *Commémoration des victimes d'actes terroristes*, coll Justice pénale, 2015, en ligne : <https://www.justice.gc.ca/fra/pr-rp/jp-cj/victim/rr09_6/p3.html> (consulté le 13 mars 2020).

défini comme des actions violentes et arbitraires qui ciblent délibérément les civils, les lois incluent bien plus d'éléments[146].

Au même titre au Royaume-Uni, le terrorisme est défini dans la *British Terrorism Act* (2006), comme l'utilisation des mesures conçues pour influencer le gouvernement ou pour intimider la population ou une partie de la population dans le but de faire progresser une cause politique, religieuse ou idéologique[147].

Une autre inquiétude au sujet des lois-antiterroristes est la rapidité avec laquelle elles sont promulguées. La réponse juridique et administrative du gouvernement américain a été immédiate après les attentats du 11 septembre ; en un mois, une nouvelle loi antiterroriste était entrée en vigueur, régissant les pouvoirs de la police, des tribunaux et le traitement des suspects : le *PATRIOT Act*[148]. En un an, un nouveau département était créé : Homeland Security, dont le mandat est d'empêcher, de protéger contre et de répondre aux attaques terroristes[149]. Les dispositions du *PATRIOT Act* ont suscité de vives critiques, notamment celle de faire entrer en vigueur un état d'urgence permanent[150].

Les Etats-Unis ne sont pas les seuls à avoir connu un tel mouvement législatif après les attentats du 11 septembre. La plupart des pays ont émis de nouvelles lois antiterroristes qui élargissent les pouvoirs des forces de l'ordre et qui durcissent les peines. C'est le

---

[146] David Lyon, *Surveillance after September 11*, coll Themes for the 21st century, Malden, Mass, Polity Press in association with s 2Blackwell Pub Inc, 2003 à la p 49.

[147] *British Terrorism Act*, 2000, s2.

[148] *Ibid*.

[149] Lyon, *supra* note 146 à la p 49.

[150] Voir notamment Jean-Claude Paye, « A Permanent state of emergency » (2006) 58:6 Mon Rev 29.

cas par exemple du Canada, où la loi anti-terroriste[151] promulguée en réponse aux attaques de 2001 est venue accorder de nouveaux pouvoirs aux institutions canadiennes et été très controversée, notamment pour sa large définition du terrorisme[152]. Dans le même sens, on peut aussi citer la législation de l'Australie, où le gouvernement Howard a introduit en juin 2002 un ensemble de propositions de lois restrictives des droits et libertés[153]. La Nouvelle-Zélande a également passé une loi antiterroriste en 2002[154]. Le Canada, l'Australie et la Nouvelle-Zélande n'étaient pas victimes de menaces terroristes à cette époque : ce sont les attentats aux Etats-Unis qui ont été présentés comme la justification de ces lois[155]. Le Conseil de sécurité des Nations Unies a contribué au caractère précipité de ces législations[156] en adoptant à l'unanimité la résolution 1373[157] le 28 septembre 2001, placée sous le Chapitre VII de la Charte des Nations Unies. Par cette résolution, il demande aux États de collaborer d'urgence pour prévenir et réprimer les actes de terrorisme, en devenant partie à l'ensemble des conventions et protocoles internationaux relatifs au terrorisme[158], mais également en

---

[151] *Loi antiterroriste,* Parlement du Canada S.C. 2001, c. 41.

[152] Voir notamment Kent Roach, *September 11: Consequences for Canada*, McGill-Queen's Press - MQUP, 2003.

[153] Security Legislation Amendment (Terrorism) Bill (2002) (Cth); Criminal Code Amendment (Suppression of Terrorist Bombings) Bill (2002) (Cth); Suppression of the Financing of Terrorism Bill (2002) (Cth); Border Security Legislation Amendment Bill 2002 (Cth); Telecommunications Interception Legislation Amendment Bill (2002) (Cth) Head, *supra* note 5 à la p 667.

[154] Terrorism Suppression Act, Nouvelle-Zélande, 2002 ; Alex Conte, « Counter-terrorism law in New Zealand » dans Alex Conte, dir, *Human rights in the prevention and punishment of terrorism: Commonwealth approaches: The United Kingdom, Canada, Australia and New Zealand*, Berlin, Heidelberg, Springer, 2010, 185.

[155] Head, *supra* note 5 à la p 674.

[156] Chantal Oudraat De Jonge, « Les Nations Unies et la lutte contre le terrorisme » [2004] GE.04-00125 Forum du désarmement, en ligne : Forum du désarmement <http://digitallibrary.un.org/record/517048> (consulté le 2 août 2020).

[157] *Résolution 1373, supra* note 4.

[158] *Résolution 1373, supra* note 4, art 3(d). ; *Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs*, 14 septembre 1963, 704 RTNU 10106 (entrée en vigueur 4 décembre 1969). ; *Convention pour la répression de la capture illicite d'aéronefs*, 16 décembre 1970,

prenant des mesures législatives sur leur territoire pour lutter contre le terrorisme[159]. Le Conseil de sécurité crée également un comité spécial qui est chargé d'examiner les rapports demandés aux États, faisant état des mesures prises visant à lutter contre le terrorisme en application de la résolution, dans un délai donné de 90 jours[160]. Le caractère urgent des mesures législatives est ainsi dicté par le Conseil de sécurité.

Si l'on peut identifier le 11 septembre 2001 comme étant le point de départ de lois anti-terroristes particulièrement restrictives des libertés, le terrorisme ne cesse d'être brandit en prétexte pour légitimer des mesures intrusives en matière de vie privée.

---

860 RTNU 12325 (entrée en vigueur : 14 octobre 1971). ; *Convention pour la répression des actes illicites dirigés contre la sécurité de l'aviation civile*, 23 septembre 1971, 974 RTNU 14118 (entrée en vigueur : 26 janvier 1973). ; *Convention sur la prévention et la répression des infractions contre les personnes jouissant d'une protection internationale, y compris les agents diplomatiques*, 14 décembre 1973, Résolution de l'Assemblée générale 3166 (XXVIII) (entrée en vigueur : 20 février 1977). ; *Convention internationale contre la prise d'otages*, 17 décembre 1979, 1316 RTNU 21931 (entrée en vigueur : 3 juin 1983). ; *Convention sur la protection physique des matières nucléaires*, 26 octobre 1979, 1456 RTNU 24631 (entrée en vigueur : 8 février 1987). ; *Protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale*, 24 février 1988, 1589 RTNU 14118 (entrée en vigueur : 6 août 1989). ; *Convention pour la répression d'actes illicites menés contre la sécurité de la navigation maritime*, 10 mars 1988, 1678 RTNU 29004 (entrée en vigueur : 1er mars 1992). ; *Protocole à la Convention du 10 mars 1988 pour la répression des actes illicites contre la sécurité des plateformes fixes situées sur le plateau continental*, 10 mars 1988, 1678 RTNU 29004 (entrée en vigueur : 26 juin 1992). ; *Convention sur le marquage des explosifs plastiques et en feuilles aux fins de détection*, 1er mars 1991, S/22393, (entrée en vigueur : 21 juin 1998). ; *Convention internationale pour la répression des attentats terroristes à l'explosif,* 15 décembre 1997, 2149 RTNU 37517, (entrée en vigueur : 23 mai 2001). ; *Convention internationale pour la répression du financement du terrorisme*, 9 décembre 1999, 2178 RTNU 38349 (entrée en vigueur : 10 avril 2002). ; *Convention internationale de 2005 pour la répression des actes de terrorisme nucléaire*, 13 avril 2005, 2220 RTNU 39481 (entrée en vigueur : 7 juillet 2007). ; *Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale*, 10 septembre 2010, (entrée en vigueur : 1er juillet 2018). ; *Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs*, 10 septembre 2010, (entrée en vigueur : 1er juillet 2018). ; *Protocole portant amendement de la Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs*, 4 avril 2014, (entrée en vigueur 1er janvier 2020).

[159] *Résolution 1373, supra* note 4, art 1.

[160] *Ibid* au para 6.

1.2.3 La justification d'une surveillance intensive

La période post-9/11 a été qualifiée de période d'« hyper législation», en ce que les lois antiterroristes se sont accumulées en réponse à ces attentats[161]. Les raisons d'une telle quantité sont multiples ; dans un premier temps pour répondre à des menaces crédibles, également pour rassurer la population et en agissant en réaction à des pressions politiques nationales et internationales[162]. Par là même, pour certains gouvernements qui désiraient s'accrocher à une certaine forme de contrôle social qui semblait leur échapper dans un monde « mondialisé », une nouvelle débouchée a pu être trouvée dans la législation anti-terroriste[163]. L'idée déjà présente de contrôle à grande échelle, que ce soit aux frontières ou dans les aéroports par exemple, trouvait désormais sa raison d'être après la chute des deux tours[164].

De nombreuses mesures immédiates ont été prises après les attentats aux Etats-Unis, diplomatiques ou sécuritaires, mais ont eu des effets à long terme sur la façon dont la surveillance est opérée[165]. Les termes « caméras de surveillance », « données biométriques », « cybersurveillance » étaient soudainement sur toutes les lèvres, se proposant comme des solutions contre de nouvelles attaques[166]. En matière de

---

[161] Andrew Ashworth et Lucia Zedner, *Preventive justice*, OUP Oxford, 2014 à la p 172.

[162] *Ibid*.

[163] Lyon, *supra* note 146 à la p 5.

[164] *Ibid*.

[165] Lyon, *supra* note 146 à la p 13.

[166] *Ibid* à la p 18.

nouvelles technologies de surveillance, l'administration américaine a présenté relativement rapidement sa proposition de « *Total Information Awareness*»[167].

La « guerre contre le terrorisme » a été déclarée par de nombreux gouvernements après les attentats de septembre 2001, mais elle est quasiment réutilisée après chaque attaque terroriste [168] . Cette expression est problématique parce que certaines mesures exceptionnelles peuvent être légitimées en temps de guerre ; elles le sont seulement justement pour leur caractère exceptionnel, on leur suppose une courte durée. Cependant, la lutte contre le terrorisme est sans fin prévisible[169]. Le terme de "guerre" permet également de réduire la remise en question de cette surveillance, on détourne le regard des moyens employés, pour les concentrer sur un ennemi commun.

On peut aussi noter l'utilisation fréquente de l'argument de la sécurité nationale à la menace terroriste dans les discours des gouvernements quand ils parlent de la nécessité de la surveillance. Surveillance et sécurité sont présentés comme un couple indissociable, où le premier est nécessaire pour garantir l'autre. Les partisans d'une surveillance intensive arguent que c'est une approche excessivement prudente de la surveillance des citoyens américains qui aurait été une des raisons de l'échec à détecter les terroristes du 11 septembre[170]. Ce type d'arguments sert à légitimer une surveillance sans contrôle. Le manque de contrôle judiciaire et par là l'allègement des procédures

---

[167] *Ibid*.

[168] Bianchi, *supra* note 121 aux pp 307-308.

[169] Lyon, *supra* note 146 à la p 41.

[170] Nick Taylor, « To find the needle do you need the whole haystack? Global surveillance and principled regulation » (2014) 18:1 Int J Hum Rights 45 à la p 52; citant Jonathan Forgang, « "The right of the people": The NSA, the FISA Amendments Act of 2008, and foreign intelligence surveillance of Americans overseas » (2009) 78:1 Fordham Law Rev 217 à la p 224.

sont présentés par les gouvernements comme un avantage et traduit en termes d'efficacité et suit principalement une logique de rendement[171].

La question de la nécessité de la collecte de données en masse, plutôt que des données sur des suspects en particulier a été abordée dans un rapport du *UK Independent Reviewer of Terrorism Legislation*[172]. Une collection massive permet ainsi aux autorités d'économiser leurs ressources et une rapidité d'accès à l'information, qui n'est pas possible lorsqu'il faut attendre un mandat pour une cible spécifique[173]. Pourtant les preuves d'une telle utilité ne sont pas apportées. Dans la décision de 2013 *Klayman v. Obama*, la Cour a notamment relevé : « l'incapacité du gouvernement [américain] à citer ne serait-ce qu'un seul cas dans lequel l'analyse des données collectées en masse par la NSA avait empêché une attaque terroriste imminente [174]».

Si les gouvernements emploient fréquemment la justification de la sécurité nationale, ce qui est réellement entendu par la sécurité demeure vague, indéterminé et suppose une urgence, qui met ainsi fin aux débats politiques[175]. C'est un terme « parapluie », et

---

[171] Daragh Murray et Pete Fussey, « Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data » (2019) 52:1 Isr Law Rev 31 à la p 37.

[172] *Ibid*; David Anderson, *Report of the bulk powers review*, Independent Reviewer of Terrorism Legislation, coll Web ISBN 9781474136921, UK Parliament, 2016, en ligne : <https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review> (consulté le 4 février 2020).

[173] Murray et Fussey, *supra* note 171 aux pp 37 et 40.

[174] *Klayman v Obama*, 2013 United States District Court, District of Columbia; Eliza Watt, « 'The right to privacy and the future of mass surveillance' » (2017) 21:7 Int J Hum Rights 773 à la p 782.

[175] Lucia Zedner, *Security*, Routledge, 2009 à la p 12; Lyon, *supra* note 146 à la p 110.

cette imprécision permet à de nombreuses politiques et mesures d'être justifiées au nom de la sécurité[176].

1.3. Les effets et l'idéologie de la surveillance de masse (*mass surveillance*)

Une des principales interrogations à l'égard de la surveillance est celle de ses effets. On ne parvient souvent pas à préciser ce qui est réellement en danger dans une société de surveillance. Que voulons nous protéger en cherchant à limiter la surveillance à ce qui est strictement nécessaire ? C'est une question à laquelle nous tenterons de répondre au mieux dans cette partie, en montrant d'abord que si l'idée que l'on se fait de la vie privée nous conduit à chercher les effets de la surveillance sur l'individu, ceux-ci sont difficiles à évaluer parce qu'ils conduisent l'individu à ne pas agir. Ainsi nous montrerons ensuite que les effets de la surveillance sont multiples sur l'ensemble de la société et empêchent l'exercice de la démocratie. Enfin, nous étudierons l'idéologie de la surveillance contemporaine, à travers les thèses de plusieurs auteurs, pour comprendre les enjeux derrière l'utilisation des *Big Data*.

1.3.1. La difficulté de mesurer les effets sur l'individu

La cause de la protection de la vie privée et de la vigilance par rapport à la surveillance est souvent réduite, en ce qu'on lui reproche de ne pas avoir d'effets visibles ou concrets. L'effet de la surveillance le plus mentionné est ce qui a été nommé « *chilling effect* », que l'on peut définir comme étant présent lorsqu'une personne s'empêche de participer à certaines activités, à cause des conséquences perçues de l'éventuelle observation de

---

[176] *Ibid* aux pp 18-19.

ces activités[177]. Cela inclut par exemple, le fait de s'abstenir de faire des recherches sur un sujet qui pourrait être sensible, communiquer avec une personne en particulier, ou se présenter ou non à un événement militant. Ce phénomène restreint ainsi directement les libertés d'expression et d'association[178]. Cependant toute la difficulté réside dans la preuve à apporter, car l'identification d'un *chilling effect* nécessite en fait la mesure d'un « non-événement »[179].

Les potentiels *chilling effects* demeurent une question qui anime les discussions et continue à être étudiée en études des droits de la personne[180]. L'idée a gagné en importance depuis les révélations de Snowden de 2013 et le lien avec la lutte anti-terroriste est de plus en plus souligné[181].

Quelques études ont cherché à mesurer ce *chilling effect*, notamment une étude pionnière en la matière de 1975 de l'université Stanford qui parlait de « *psychological breach of the First Amendment* » pour décrire l'effet de la surveillance[182]. Après avoir

---

[177] Murray et Fussey, *supra* note 171 à la p 43.

[178] *Ibid* à la p 44.

[179] *Ibid* à la p 45.

[180] *Ibid* à la p 44 citant; Martin Scheinin, *Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, A/HRC/13/37, Conseil des Droits de l'Homme, Assemblée Générale des Nations Unies, 2009; *Digital Rights Ireland c Minister for Communications et autres,* Affaires jointes C-293/12 et C-594/12, No ECLI:EU:2014:238, [2014] CJUE ; *Tele2 Sverige AB c Post-och telestyrelsen and Secretary of State for the Home Department c Tom Watson et autres,* Affaires jointes C-203/15 et C-698/15*,* No ECLI:EU:C:2016:970, [2016] CJUE [*Tele2 Sverige AB*].

[181] Glenn Greenwald, *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*, Hamish Hamilton, 2014.

[182] Murray et Fussey, *supra* note 171 à la p 44 citant; Gregory L White et Philip G Zimbardo, *The chilling effects of surveillance: Deindividuation and reactance*, TR-Z-15-ONR, Stanford Univ CA Dept of Psychology, 1975, en ligne : <https://apps.dtic.mil/dtic/tr/fulltext/u2/a013230.pdf> (consulté le 13 avril 2020).

constaté dans un premier temps que la surveillance engendre l'anxiété et l'inhibition des participants, il avait été observé qu'ils se comportaient de façon à se « désindividualiser », en augmentant leur anonymat et en adaptant leur comportement pour ne pas avoir l'air en dehors de la norme[183]. Bien que ses conclusions soient intéressantes, l'étude a été faite sur un petit échantillon et date d'une époque « pré-digitale », ce qui restreint son application aux formes plus complexes et contemporaines de surveillance[184].

Plus récemment et à plus grande échelle, l'organisation PEN America a interrogé 520 auteurs américains sur leur écriture depuis les révélations de Snowden[185]. L'étude de 2013 a montré qu'une grande partie des écrivains était inquiétée par la surveillance étatique et par conséquent, pratiquait un niveau important d'auto-censure[186]. Ainsi, ils étaient un sur six à déclarer éviter d'écrire à propos, ou de parler de sujets dont ils pensaient qu'ils pourraient faire d'eux des cibles de surveillance[187].

Il faut aussi souligner que les mesures de surveillance anti-terroristes touchent particulièrement certains individus. Il a pu être constaté à de multiples reprises que les investigations ciblaient de manière disproportionnée les personnes de confession musulmane et d'origine arabe[188]. Cette discrimination sur le groupe social, la communauté religieuse, ou la nationalité, parmi d'autres, se justifie souvent par des

---

[183] Murray et Fussey, *supra* note 171 à la p 44; White et Zimbardo, *supra* note 181 à la p 5.

[184] Murray et Fussey, *supra* note 171 à la p 44.

[185] *Ibid* à la p 47 citant; PEN America, *Chilling effects: NSA surveillance drives U.S. writers to self-censor*, 2013, en ligne : <https://pen.org/research-resources/chilling-effects/> (consulté le 13 avril 2020).

[186] PEN America, *supra* note 185 aux pp 4-8.

[187] *Ibid* à la p 6.

[188] Lyon, *supra* note 146 à la p 53.

amalgames faites par certaines forces de l'ordre et certains gouvernements. La surveillance particulière des minorités dans le cadre de la lutte contre la criminalité n'est pas spécifique à la lutte anti-terroriste et on retrace historiquement ces schémas de pensée dans le colonialisme[189] et l'esclavage[190]. Ces pratiques peuvent conduire à une internalisation de la suspicion ; les personnes ciblées peuvent se sentir obligées d'expliquer des comportements parfaitement acceptables, éviter des activités ou associations légitimes, par peur que ces actions soient mal interprétées[191]. Le *chilling effect* de la surveillance est donc d'autant plus présent chez les personnes victimes de ces discriminations[192].

Cela dit, peu d'individus vont vraisemblablement ressentir une perte de vie privée à un moment précis : c'est plutôt une perte graduelle à travers un éventail d'activités, affectant l'ensemble de la population[193]. Cela présente un problème qui est plus difficile à adresser directement en droit[194].

1.3.2 L'impact social d'une surveillance généralisée

Le *chilling effect* engendré par la surveillance intensive peut altérer le fonctionnement d'une démocratie participative[195]. D'une part en dissuadant le vote, mais aussi en

---

[189] Voir à ce sujet Ahmad H Sa'di, « Colonialism and surveillance » dans *Routledge handbook of surveillance studies*, Routledge, 2012 aux pp 151-158.

[190] Voir à ce sujet Simone Browne, « Race and surveillance » dans *Routledge handbook of surveillance studies*, Routledge, 2012 aux pp 72-79.

[191] Lyon, *supra* note 146 à la p 53.

[192] *Ibid*.

[193] Taylor, *supra* note 170 à la p 48.

[194] *Ibid*.

[195] Murray et Fussey, *supra* note 170 à la p 144.

limitant le militantisme. A cause d'une large définition du terrorisme, tous ceux qui ne sont pas pleinement satisfaits du *statu quo* et qui auraient l'intention d'altérer les structures politiques, économiques ou sociales, sont considérés comme suspects et souvent placés sur les listes visant à traquer les potentiels terroristes[196].

La surveillance intensive transforme, voire empêche la démocratie. La littérature dystopique associe le totalitarisme et la surveillance intensive et c'est aussi une des caractéristiques d'un régime totalitaire d'opérer une surveillance intensive pour traquer les dissidents. Cependant la surveillance intensive existe aussi au sein des régimes dits démocratiques. Dans son article intitulé '*What privacy is for'*, la professeure Julie Cohen soutient que la vie privée est une composante structurelle indispensable des systèmes politiques de démocratie libérale[197]. Elle décrit la société contemporaine comme étant une « société modulée[198]» où la surveillance n'est pas, contrairement à ce qui est visible dans un régime totalitaire, évidente, violente et usant de la force ; elle est ici ordinaire et c'est ce caractère ordinaire qui fait sa force extraordinaire[199]. La démocratie est mise en péril par une surveillance intensive du peuple qui l'empêche de s'exprimer pleinement et de participer aux institutions démocratiques.

Il y a également certaines données qui sont dangereuses pour la démocratie. Cette dangerosité a notablement été illustrée par l'affaire Cambridge Analytica[200]. Les consultants politiques Cambridge Analytica, qui travaillent avec le parti Républicain

---

[196] Lyon, *supra* note 146 à la p 54.

[197] Julie Cohen, « What privacy is for » (2013) 126:7 Harv Law Rev 1904 à la p 1905.

[198] Notre traduction de « modulated society » *Ibid* à la p 1915.

[199] *Ibid*.

[200] « The Cambridge Analytica files », *The Guardian* (2020 2018), en ligne : The Guardian <https://www.theguardian.com/news/series/cambridge-analytica-files> (consulté le 1 avril 2020).

américain depuis 2012, ont récupéré des données collectées frauduleusement par Aleksandr Kogan à travers son entreprise Global Science Research[201]. Les données initiales ont été récoltées en présentant des faux 'tests de personnalité' sur la plateforme Facebook[202]. Il a ensuite été révélé que Facebook avait remis les données personnelles de plus de 87 millions d'utilisateurs à Cambridge Analytica[203]. De plus, même pour les non-utilisateurs de la plateforme, les technologies de traçage dont l'entreprise disposait ont permis de collecter les données venant de tous les sites disposant d'un logo Facebook, celui qui permet d'« aimer » ou partager la publication via la plateforme par exemple, que l'on trouve sur la plupart des sites journalistiques[204].

Ce que cette collecte massive a permis à Cambridge Analytica était de pouvoir cibler les personnes qui n'étaient pas fixées sur leur vote et de leur suggérer des articles de propagande sur les candidats par lesquels l'entreprise a été employée, ciblés en fonction de leur activité sur Internet[205]. Si cette technique, appelée le « micro-*targeting* », n'est pas nouvelle, les technologies récentes lui permettent de manipuler la population à un niveau alarmant[206]. Les membres de l'exécutif de Cambridge Analytica se sont ainsi vantés du résultat de plusieurs élections, notamment celle du Président Trump en 2016[207]. Cette utilisation des *Big Data* est particulièrement préoccupante pour les

---

[201] Hal Berghel, « Malice domestic: The Cambridge Analytica dystopia » (2018) 51:5 Computer 84 à la p 84.

[202] *Ibid*.

[203] Jim Isaak et Mina J Hanna, « User data privacy: Facebook, Cambridge Analytica, and privacy protection » (2018) 51:8 Computer 56 à la p 58.

[204] *Ibid*.

[205] Alex Hern, « Cambridge Analytica: how did it turn clicks into votes? », *The Guardian*, sect News (6 mai 2018), en ligne : The Guardian <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> (consulté le 17 avril 2020).

[206] Berghel, *supra* note 201 à la p 86.

[207] *Ibid* à la p 85.

élections libres, d'autant plus qu'elles ont servi à mettre au pouvoir des dirigeants d'extrême droite bien au-delà des frontières des Etats-Unis[208]. Ces pratiques remettent en question le sens du droit de vote, qui est censé donner le pouvoir au peuple de choisir ses représentants. Une propagande si personnalisée ne peut pas permettre aux électeurs de faire un réel choix et pose la question de la ligne à tracer entre la persuasion et la manipulation des électeurs[209].

La surveillance telle que pratiquée a une deuxième incidence majeure sur l'ensemble de la société : l'étouffement de la créativité. Les défenseurs d'une surveillance robuste au détriment de la protection de la vie privée arguent qu'une protection rigoureuse de la vie privée est rétrograde et accusent ceux qui la défendent d'empêcher l'innovation[210]. En réalité, des conditions où la vie privée est diminuée détériorent la capacité d'innover[211]. Premièrement, parce que l'innovation requiert une capacité de perspective critique sur son environnement[212]. Deuxièmement, parce pour innover il faut de la place pour réfléchir, alors elle sera davantage possible dans un environnement qui accorde de l'importance et qui préserve ces espaces d'intimité[213]. Par conséquent une société qui laisse les infrastructures de surveillance se multiplier sans contrôle ne peut pas espérer maintenir une tradition d'innovation[214].

---

[208] *Ibid* à la p 87.

[209] *Ibid* à la p 86.

[210] Cohen, *supra* note 197 à la p 1904.

[211] *Ibid* à la p 1918.

[212] *Ibid*.

[213] *Ibid*.

[214] *Ibid*.

Les effets sur la créativité d'une surveillance trop proche, où les individus ne peuvent pas bénéficier de ces espaces où ils sont réellement seuls, ont pu être démontrés à plusieurs reprises. La surveillance au travail des employés par leurs employeurs est une pratique qui ne cesse d'augmenter. Pourtant des études ont montré très tôt que le fait d'être électroniquement surveillé au travail avait des effets adverses sur la productivité, la créativité et le niveau de stress des employés[215].

Cette absence d'espace privé peut être reliée à ce que le professeur Harcourt a appelé la « mortification du soi[216]». Le concept regroupe plusieurs éléments, dont le manque d'un espace qui soit réellement à soi. Cela peut être illustré par une étude qui a été menée sur des enfants dans plusieurs pensionnats anglais, où la surveillance était très intensive : par exemple, les professeurs avaient accès en temps réel aux activités faites sur l'ordinateur des élèves, de sorte à pouvoir leur dire « quitte ce site et fais tes devoirs » par exemple ; il y avait également des caméras de surveillance dans tout le pensionnat[217]. Les enfants vivaient difficilement le fait que tous leurs gestes soient observés et contrôlés puis ont exprimé le besoin d'avoir « *a backstage area of emotional release* »[218]. Cette connaissance omniprésente prive les personnes surveillées d'un endroit où elles peuvent se sentir en sécurité[219]. Elle affecte également la confiance en soi, le sentiment de vulnérabilité, celui d'être contrôlé et de ne pas

---

[215] Bernard E Harcourt, *supra* note 106 à la p 218; M J Smith et al, « Employee stress and health complaints in jobs with and without electronic performance monitoring » (1992) 23:1 Appl Ergon aux pp 17-27; G. L. Rafnsdóttir et M. L. Gudmundsdottir, "EPM technology and the psychosocial work environment," 3 New Technology, Work and Employment 2011 aux pp 210–221.

[216] Notre traduction de « mortification of the self » ; Bernard E Harcourt, *supra* note 106.

[217] *Ibid* aux pp 219-220 citant; Michael McCahill et Rachel Finn, « The social impact of surveillance in three UK schools : "angels", "devils" and "teen mums" » (2010) 7:3/4 Surveillance and Society à la p 278.

[218] Bernard E Harcourt, *supra* note 106 à la p 221.

[219] *Ibid*.

pouvoir prendre ses propres décisions[220]. Privé d'un espace intime, cette surveillance conduit aussi à un détachement de soi, par habitude d'être constamment observé[221].

La mortification de soi n'est pas vécue seulement dans les espaces clos de surveillance, comme les pensionnats ou les institutions pénitentiaires. Elle est engendrée par la surveillance quotidienne de nos activités sur Internet, et particulièrement le contraste entre d'un côté une collecte de données massives qui permet de connaître extensivement l'utilisateur et de l'autre côté, l'absence d'informations qu'a l'utilisateur à propos de la collecte et l'utilisation de ses données[222]. Ce qui est « mortifiant », c'est l'incapacité de contrôler notre propre information.

1.3.2. L'idéologie de la surveillance contemporaine

Une des critiques ou mise en gardes principales à l'égard des *Big Data* est que contrairement à leur apparence d'être simplement le reflet du monde, les données ne peuvent pas être neutres : il y a toujours une idéologie derrière la collecte et l'utilisation qui en est faite[223]. Les technologies des *Big Data* que nous avons pu évoquer précédemment, qui permettent l'analyse et la prédiction des comportements humains, sont au service d'une construction plus globale, qui anime aussi bien les institutions étatiques que les entreprises, appelée « *surveillance capitalism*[224]».

---

[220] *Ibid* à la p 219.

[221] *Ibid* à la p 229.

[222] *Ibid* à la p 217.

[223] Cohen, *supra* note 197 à la p 1925; Rouvroy, *supra* note 9 à la p 11.

[224] Shoshana Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, First edition, PublicAffairs, 2019.

Le concept a été créé par la professeure Shoshana Zuboff et désigne une ordre économique basé sur la surveillance, où les données sont des biens qui confèrent un pouvoir sans précédent à ceux qui les possèdent. Si pour certains cet état des choses est une continuité logique de l'industrialisation et de la mondialisation, Zuboff distingue le capitalisme de la surveillance comme une mutation véreuse du capitalisme[225], qui dépasse infiniment la sphère des intérêts purement économiques[226].

La matière première de ce système est constituée des données personnelles des individus.Leur collecte permet à ceux qui les utilisent non seulement de s'enrichir, mais également d'avoir le monopole des informations et de la connaissance[227]. Ceux qui profitent de ces données, ce sont les États et les méga-corporations, qui ont pour objectif d'obtenir le plus d'informations possible. On assiste ainsi à la naissance d'un nouveau colosse commercial qui crée de la richesse par la prédiction, l'influence et le contrôle des comportements humains[228].

Pour Zuboff, la concentration de richesse, de savoir et de pouvoir par les capitalistes de la surveillance est telle qu'elle menace la démocratie, les libertés et l'avenir de l'humanité[229]. Cette maîtrise habile de la division du pouvoir est illustrée par la métaphore des deux textes[230]. Les mécanismes du capitalisme de la surveillance imposent la production de deux textes électroniques[231]. Concernant le premier texte,

---

[225] « *Rogue mutation of capitalism* » *Ibid*.

[226] Shoshana Zuboff, traduit par Jonathan Chalier, « Le capitalisme de la surveillance : Un nouveau clergé » [2019] 5 Esprit 63 à la p 70.

[227] *Ibid* à la p 75.

[228] *Ibid*.

[229] *Ibid* à la p 63.

[230] *Ibid* aux pp 67-71.

[231] *Ibid* à la p 70.

nous, la population, en sommes ses auteurs et lecteurs : il est composé de ce que nous y inscrivons en ligne, c'est à dire nos publications, articles de blog, vidéos, photos, conversations, musiques, histoires, observations, *likes*, *tweets* et tout cet ensemble de nos vies enregistrées et communiquées[232]. La contribution à ce premier texte est donc volontaire. Chaque personne a au moins le contrôle sur ce qu'elle publie.

Ce premier texte porte avec lui un « fantôme » : le premier texte fonctionne en réalité comme source d'approvisionnement pour le second texte, le texte fantôme[233]. Ce second texte est caché, sauf pour les capitalistes de la surveillance, à qui il appartient[234]. Il se nourrit des actions quotidiennes de manière automatique. C'est une accumulation croissante d'excédent comportemental et de ses analyses ; il en révèle plus sur nous-mêmes que nous ne pouvons savoir[235]. Il devient de plus en plus difficile et sans doute impossible, de se retenir d'y contribuer[236].

Ce qui concrètement va dans ce second texte, en plus des données du premier, ce sont les métadonnées liées à aux activités quotidiennes. Cela peut par exemple être la géolocalisation ou les heures de connexion à un réseau Wifi,la trace de chaque clic, chaque article recommandé dont la page a été ouverte, chaque publicité qui a été consultée. Le second texte est aussi composé des analyses et corrélations faites entre les données et va ainsi pouvoir faire émerger un profil, un ensemble de données liées à une personne, que l'on peut ici relier au concept du « data double » pour décrire cet

---

[232] *Ibid*.

[233] *Ibid* à la p 71.

[234] *Ibid*.

[235] *Ibid*.

[236] *Ibid*.

autre qui émerge de nos données[237]. Contrairement au premier texte, cette contribution est involontaire dans les faits, en dépit du nombre de fois qu'un usager normal peut cliquer sur « J'ai lu et j'accepte les conditions d'utilisation ». Le second texte existe à des fins de contrôle : il est à propos de nous, mais il n'est pas pour nous[238].

Une telle possession d'information est d'autant plus problématique qu'elle n'est accessible qu'à ceux qui ont déjà énormément de pouvoir par d'autres moyens. Le désir de contrôle par les États et entreprises alliées n'est pas nouveau : mais les capacités pour le faire sont inouïes. La surveillance est devenue relativement simple et peu coûteuse à l'échelle de grandes organisations, ce qui la rend attractive[239]. Désormais chaque entreprise de taille conséquente a un département de '*Predictive Analytics*', qui sert à prévoir les comportements des consommateurs en fonction de leurs habitudes afin de créer des stratégies de mercatique plus ciblées[240]. Cela suit l'objectif d'une consommation extrême.

Pour Cohen, la fin ultime de la surveillance, pour les États ainsi que pour les grandes corporations, est de produire des « citoyens-consommateurs » dociles et prévisibles, dont l'auto-détermination se déroule selon des trajectoires génératrices de profits[241]. Dans le même sens, la professeure Antoinette Rouvroy dans le cadre de ses travaux sur la gouvernementalité algorithmique, dénonce à propos des données une croyance en

---

[237] David Lyon, *supra* note 27 aux pp 87-88; citant Haggerty et Ericson, *supra* note 18.

[238] Zuboff et Chalier, *supra* note 226 à la p 72.

[239] Bernal, *supra* note 89 à la p 248.

[240] Bernard E Harcourt, *supra* note 106 à la p 195.

[241] Cohen, *supra* note 197 à la p 1917.

leur vérité[242]. Rouvroy parle de « fiabilité sans vérité[243]» en ce qu'un grand nombre de décisions sont prises sur la base des données récoltées par un algorithme sans que l'on cherche à déterminer leur exactitude. La logique est celle de « rendement, de l'optimisation, pas du tout de la vérité, de la validité et encore moins de la légitimité[244]». Les *Big Data* sont utilisées selon les agendas intéressés des acteurs économiques puissants[245].

---

[242] Rouvroy, *supra* note 9 aux pp 11-15; Antoinette Rouvroy, *Gouvernementalité algorithmique et idéologie technique des big data: Interview réalisée par Thomas Gouritin*, 7 mars 2018, en ligne : <https://researchportal.unamur.be/fr/publications/gouvernementalit%C3%A9-algorithmique-et-id%C3%A9ologie-technique-des-big-da> (consulté le 14 juin 2019).

[243] Rouvroy, *supra* note 9 à la p 11.

[244] *Ibid* à la p 14.

[245] Cohen, *supra* note 197 à la p 1925.

CHAPITRE II

LES FORCES ET FAIBLESSES DU DROIT A LA VIE PRIVÉE ET SES ALTERNATIVES POUR FAIRE FACE A LA SURVEILLANCE DE MASSE

Dans ce chapitre, nous étudierons dans un premier temps le cadre juridique du droit à la vie privée et son évolution en examinant sa capacité à se saisir des enjeux liés à la surveillance (2.1). Après avoir relevé les différentes lacunes de ce cadre juridique, nous étudierons les cadres juridiques alternatifs, à savoir les autres droits de la personne consacrés en droit international et le cadre de la protection des données personnelles (2.2). Nous présenterons enfin les solutions possibles, en dehors du droit positif, pour faire face à la surveillance de masse (2.3).

2.1. Le droit à la vie privée à l'épreuve des nouvelles technologies de surveillance

Durant ces dernières années ont été développées des nouvelles technologies de surveillance qui étaient inimaginables au moment où le droit à la vie privée a été défini dans les instruments internationaux. L'idée ici est de déterminer si le droit à la vie privée, tel que défini et interprété en droit positif, permet d'adresser adéquatement les effets causés par la surveillance contemporaine. Dans un premier temps, nous étudierons la définition du droit à la vie privée et les limites qu'une telle définition contient. Deuxièmement, nous verrons que certaines de ces limites sont compensées par l'interprétation souple du texte du droit à la vie privée qui a pu être faite par les tribunaux, notamment les juridictions européennes. Enfin, nous présenterons les

modifications des attentes en matière de vie privée des personnes, en particulier à une ère où le partage d'informations personnelles et les outils de *quantified self* semblent être la norme : la protection de la vie privée telle qu'elle est entendue en droit est-elle en mesure de protéger les individus?

2.1.1. La définition de la vie privée en droit positif et ses limites

Le droit au respect de la vie privée est reconnu par les principales conventions internationales en matière de droits de la personne. Il est ainsi garanti par la Déclaration universelle des droits de l'Homme[246], le Pacte international relatif aux droits civils et politiques[247], la Convention européenne des droits de l'Homme[248], et la Convention américaine relative aux droits de l'Homme[249].

La Déclaration universelle des droits de l'Homme prévoit en son article 12 que « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation[250]». La Déclaration universelle des droits de l'Homme, bien qu'elle soit le fondement du droit international des droits de la personne était, du moins au moment de sa rédaction[251], de nature

---

[246] *Déclaration universelle des droits de l'Homme*, Nations Unies, Assemblée générale, Résolution 217 (III) A, 10 décembre 1948 [DUDH] art 12.

[247] PIDCP*, supra* note 28 art 17.

[248] *Convention européenne des droits de l'Homme et des libertés fondamentales,* Conseil de l'Europe, STCE n°005, 4 novembre 1950 art 8.

[249] *Convention américaine relative aux droits de l'Homme (B-32), Pacte de San José,* Organisation des États américains, 22 novembre 1969 art 11 (entrée en vigueur : 18 juillet 1978).

[250] DUDH, *supra* note 246 art 12.

[251] Voir notamment, sur le statut coutumier de la DUDH : Marc Gambaraza, Le statut juridique de la Déclaration universelle des droits de l'Homme, Université Panthéon-Assas, 2013, en ligne : <https://docassas.u-paris2.fr/nuxeo/site/esupversions/82a62e10-5216-45a5-b1f9-87dc7a99746c?inline> (consulté le 2 août 2020).

déclaratoire[252]. Cela signifie que les droits énoncés doivent être complétés par d'autres instruments de droit international ou inscrite dans les lois nationales pour être applicables. Ainsi, le PIDCP confère un caractère obligatoire au droit au respect de la vie privée[253]. Le texte des articles concernant la vie privée est quasiment identique dans la Déclaration des droits de l'Homme et le PIDCP, si ce n'est l'ajout de l'adjectif "illégal" par le PIDCP au concept d'immixtion et atteinte arbitraire. Ainsi, les immixtions et atteintes ne peuvent avoir lieu qu'en vertu d'une loi, qui doit être conforme aux principes du PIDCP[254]. L'interprétation de l'article 17 du PIDCP se fait en deux temps. La première étape est de déterminer si les faits soulèvent un droit protégé par le premier paragraphe de l'article[255]. La seconde étape est d'établir si l'immixtion est illégale ou arbitraire.

Le respect du PIDCP est assuré par le Comité des droits de l'Homme qui étudie les rapports présentés par les États[256]. De plus, il peut recevoir des communications émanant des particuliers, à condition que l'État en question ait reconnu sa compétence[257]. Le Comité des droits de l'Homme a précisé dans sa seizième

---

[252] Voir notamment Roger Koudé Collectif, *La déclaration universelle des droits de l'homme a-t-elle encore un sens ?*, Revue d'études francophones sur l'Etat de droit et la Démocratie, coll Hors-série, Archives contemporaines, 2008 aux pp 70-71.

[253] Alain-Robert Nadeau, *Vie privée et droits fondamentaux : étude de la protection de la vie privée en droit constitutionnel canadien et américain et en droit international.*, Thesis, University of Ottawa (Canada), 2000 à la p 454.

[254] Comité des droits de l'Homme, *Observation générale n°16 : Article 17, droit au respect de la vie privée*, Doc NU HRI/GEN/1/Rev.1 (1988) au para 3; James Michael, *Privacy and human rights: an international and comparative study, with special reference to developments in information technology*, Paris, France; Aldershot, Hampshire, England, UNESCO ; Dartmouth Pub Co, 1994 à la p 20.

[255] Nadeau, *supra* note 253 à la p 456.

[256] PIDCP, *supra* note 28 art 41.

[257] *Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques*, Nations Unies, Assemblée générale, Résolution 2200 A (XXI), 16 décembre 1966 999, RTNU 302 (entrée en vigueur : 23 mars 1976).

observation générale[258] dédiée au respect de la vie privée que si la protection de la vie privée est « nécessairement relative[259] », toute immixtion doit être raisonnable[260] au regard des circonstances particulières et limitée à ce qui est nécessaire[261].

Ces limitations sont similaires dans les traités régionaux de droits de la personne. S'agissant du cadre juridique européen des droits de la personne, le droit à la vie privée est garanti par l'article 8 de la Convention européenne des droits de l'Homme[262]. L'article prévoit que : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». La formulation de la vie privée de l'article 8 diffère légèrement des articles de la Charte des droits de l'Homme, mais la différence principale réside dans la deuxième partie de l'article, qui énumère une liste de motifs légitimes pour lesquels une limitation du droit à la vie privée se verrait justifiée dans une société démocratique[263]. Ainsi sont mentionnés 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 et la protection des droits et libertés d'autrui[264]. Si ces motifs sont exclusifs, les thèmes sont très larges et de nombreuses mesures peuvent y être rattachées.

Notamment, la Cour européenne des droits de l'Homme avait considéré que des mesures en matière d'immigration peuvent être justifiées par la défense du bien-être économique du pays, au sens du paragraphe 2 de l'article 8, en raison de la densité de

---

[258] *Observation générale n°16 : Article 17, droit au respect de la vie privée*, *supra* note 254.

[259] *Ibid* au para 7.

[260] *Ibid* au para 4.

[261] *Ibid* au para 8.

[262] *Convention européenne des droits de l'Homme et des libertés fondamentales*, *supra* note 248 art 8.

[263] *Ibid*.

[264] *Ibid*.

la population, pour régulariser le marché du travail[265]. Pour donner un second exemple, concernant l'interdiction du port du voile intégral dans l'espace public, la Cour a pris en compte le fait que l'État défendeur considérait que le visage jouait un rôle important dans l'interaction sociale, et elle a donc admis que le voile cachant le visage fût perçu comme portant atteinte au droit d'autrui « d'évoluer dans espace de sociabilité facilitant la vie ensemble »[266]. Si ces interprétations ont restreint le champ d'application du droit à la vie privée, nous verrons, dans la partie suivante, que la Cour a pris autant de liberté lorsqu'elle a estimé que le droit à la vie privée devrait être priorisé et a ainsi contribué, dans la majorité des affaires reçues, à un élargissement de la notion.

Nous noterons également au niveau européen, la présence de la Charte des droits fondamentaux de l'Union européenne, où le droit au respect de la vie privée et familiale figure à l'article 7[267]. La particularité de cette charte par rapport aux autres instruments de droits humains est d'accorder un droit distinct à la protection des données personnelles, en son article 8[268]. Nous reviendrons plus en détail sur cet article et sur ses différences avec le droit au respect de la vie privée dans la seconde partie de ce chapitre.

Le système interaméricain protège également le droit à la vie privée. Dans la Convention américaine de sauvegarde des Droits de l'Homme, le droit à la vie privée apparaît à l'article 11 sous l'intitulé "Protection de l'honneur et de la dignité de la

---

[265] *Berrehab c Pays-Bas*, No 10730/84 [1988] CEDH au para 26; *Guide sur l'article 8 de la Convention – Droit au respect de la vie privée et familiale*, CEDH, coll Guides sur la jurisprudence, 2019 à la p 11, en ligne : <https://juridique.defenseurdesdroits.fr/index.php?lvl=notice_display&id=28431&opac_view=-1> (consulté le 27 avril 2020).

[266] *SAS c France*, No 43835/11 [2014] CEDH au para 122.

[267] *Charte des droits fondamentaux de l'Union européenne,* [2000], JO, 2012/C 326/02 art 7.

[268] *Ibid* art 8.

personne"[269]. Il est ainsi précisé au deuxième point de l'article que : « Nul ne peut être l'objet d'ingérences arbitraires ou abusives dans sa vie privée[270]», en ajoutant la vie de famille, le domicile et la correspondance[271]. Ici encore, l'objectif de l'article est essentiellement de protéger l'individu d'immixtions arbitraires.

En conclusion, on peut noter que le droit à la vie privée comprend une variété de champs tels que le respect du domicile, de l'intégrité physique ou morale et ce qui correspond davantage à la surveillance contemporaine ; la protection de l'information, qui inclut la protection des correspondances, des conversations téléphoniques et des données à caractère personnel. Si cette énumération de catégories comprises dans le droit à la vie privée, qui est celle faite dans les articles garantissant le respect de ce droit, donne une idée de son champ d'application, une définition exhaustive et complète de ce que l'on cherche à protéger est manquante. De nombreux auteurs relèvent que la conception traditionnelle de la vie privée, qui consistait principalement en la protection des correspondances et du domicile et des informations qui peuvent être considérées par une personne comme confidentielles (par exemple, un secret, une image embarrassante, ou une révélation qui nuit à la réputation) n'est plus pertinente.

S'il y a consensus sur le fait que cela fait partie de la vie privée, la vie privée telle qu'on la comprend aujourd'hui doit être plus que cela, pour deux raisons : dans un premier temps, la collecte et l'analyse d'informations a changé. Ce que l'on pouvait faire des informations que l'on possédait sur une personne il y a quelques décennies ne permettait pas de contrôler ou manipuler une personne au point où cela est rendu possible aujourd'hui. La deuxième raison, est le fait que des informations peuvent être

---

[269] *Convention américaine relative aux droits de l'Homme*, *supra* note 249 art 11.

[270] *Ibid*.

[271] *Ibid*.

extrêmement intimes ou personnelles sans que le sujet de l'information le réalise. Autrement dit, si l'on peut volontairement dévoiler certaines de nos informations que nous considérons anodines, elles peuvent devenir extrêmement révélatrices lorsqu'elles sont analysées en conjonction avec d'autres données, qui nous semblaient tout aussi inoffensives. La façon dont ces informations seront couplées, avec nos propres données passées ou futures, ou bien celles des autres, ou encore, les prédictions qui seront faites à partir de ces informations, il nous est impossible de les anticiper. Nous reviendrons plus en détail sur cette faille dans la partie 2.2.3. Il convient à présent, après avoir présenté la définition de la vie privée et relevé certaines de ses lacunes, de montrer l'interprétation qui en est faite par les tribunaux.

2.1.2 L'interprétation souple du droit à la vie privée par les tribunaux

Si les traités protégeant la vie privée n'offrent pas de définition précise et contemporaine de ce qui est entendu par « vie privée », le droit à la vie privée a l'avantage, comme la majorité des droits de la personne qui ont été classés parmi les droits civils et politiques, de bénéficier d'une bonne justiciabilité. En d'autres termes, de nombreux tribunaux sont compétents en la matière et vont accepter de se prononcer sur le respect du droit à la vie privée par les États. Le droit à la vie privée dispose ici d'un avantage, surtout si on le compare aux droits économiques et sociaux, en ce qu'il est reconnu comme un droit dans l'ordre international et dans la majorité des systèmes judiciaires nationaux. Nous présenterons donc l'interprétation faite par les tribunaux du droit à la vie privée, tel qu'il est consacré en droit international, au niveau régional, ou encore dans certaines lois et constitutions nationales.

La Cour européenne des droits de l'Homme a joué un rôle important en matière de définition de la vie privée. Elle a notamment dans l'affaire *Pretty c. Royaume Uni*[272] précisé que le droit au respect de la vie privée est une « notion *large* qui englobe, *entre autres*, des *aspects de l'identité physique et sociale* d'un individu, notamment le *droit à l'autonomie* personnelle, le *droit au développement personnel* et le *droit d'établir et entretenir des rapports avec d'autres êtres humains et le monde extérieur* [273]». Cette définition est particulièrement ouverte, et avait permis en l'espèce d'estimer que l'interdiction du suicide assisté relevait, entre autres, de l'article 8 de la Convention européenne des droits de l'Homme.

L'interprétation contextuelle du droit à la vie privée faite par les tribunaux permet, au moins partiellement, de pallier une règle de droit imprécise. Cette souplesse a permis à la Cour européenne des droits de l'Homme d'appliquer l'article 8 à la surveillance numérique, en dépit de l'absence mention expresse du caractère privé des données personnelles dans les instruments internationaux de droits de la personne. Dans l'affaire *Szabo et Vissy c. Hongrie*[274], il était reproché au gouvernement hongrois la création en 2011 d'une unité spéciale en matière de lutte contre le terrorisme au sein des forces de polices. Cette unité s'est vu doter de compétences en matière de perquisition de domiciles et de surveillance par l'enregistrement des communications électroniques. Les intéressés ont porté leur recours à la Cour constitutionnelle hongroise, qui a estimé que les opérations secrètes se justifiaient à des fins de sécurité nationale. Les requérants portent ensuite leur recours devant la Cour européenne des droits de l'Homme alléguant une violation de l'article 8 eu égard à l'ampleur et au

---

[272] *Pretty c Royaume-Uni,* No 2346/02, [2002], CEDH ; Frédéric Sudre, *Les grands arrêts de la Cour européenne des droits de l'homme*, 8e éd, Paris, PUF, 2017, nº 47.

[273] *Pretty c Royaume-Uni, ibid* au para 61.

[274] *Szabo et Vissy c Hongrie,* No 37138/14, [2016] CEDH.

caractère intrusif de telles mesures, et du risque potentiel de faire l'objet de mesures injustifiées.

La première étape de vérification est de déterminer si ces pouvoirs avaient une base légale ; en l'espèce, ils étaient en effet prévus par la loi, mais il n'y avait aucune condition à remplir pour pouvoir les appliquer, toute personne peut être surveillée. La Cour a rappelé que s'agissant de questions touchant aux droits fondamentaux, toute législation accordant un pouvoir discrétionnaire à l'exécutif dans le domaine de la sécurité nationale doit indiquer quelle est l'étendue de ce pouvoir discrétionnaire et les modalités de son exercice avec suffisamment de clarté. La Cour a donc jugé qu'il y avait un risque d'ingérences arbitraires, d'autant plus qu'il n'y avait aucun contrôle juridictionnel sur ces mesures.

Cette décision de la CEDH fait écho à la décision de la CJUE *Digital Rights Ireland* où les juges avaient mené une réflexion capitale sur les métadonnées, qui « prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées [et] les relations sociales de ces personnes »[275]. Après avoir souligné l'ampleur des conséquences que peut avoir une telle surveillance, la Cour avait rappelé le critère de "stricte nécessité" des mesures de collecte et de rétention, qui doit être examinée à la lumière des objectifs poursuivis ; ce passage de *Digital Rights Ireland* a directement été cité par la CEDH.

---

[275] *Digital Rights Ireland c Minister for Communications et autres, Affaires jointes C-293/12 et C-594/12*, [2014] CJUE.

Cet unisson des juges européens sur la question de la surveillance peut être rattaché à la volonté de l'Europe de faire front commun face aux enjeux de la surveillance et d'établir un cadre juridique clair et cohérent : ainsi, la Cour a également cité la *Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*[276], notamment en réaffirmant qu'une surveillance de masse porte atteinte aux piliers de la démocratie.

La CEDH s'était également prononcée dans l'affaire *Catt c. Royaume-Uni*[277] sur la définition problématique de l'extrémisme énoncée par les gouvernements et avait rappelé l'importance d'examiner le respect des principes de l'article 8 où les pouvoirs accordés à l'État sont obscurs, et créent un risque d'arbitraire, en particulier quand les technologies disponibles deviennent de plus en plus sophistiquées.

Pour faciliter les requêtes invoquant l'article 8 en cas de surveillance étatique, la CEDH a établi une règle confirmée dans *Roman Zakharov c. Russie* et basée sur l'approche de *Kennedy c. Royaume-Uni,* les requérants n'ont pas besoin de prouver qu'ils ont subi eux-mêmes des mesures de surveillance secrètes, car en raison du caractère secret de ces mesures la preuve pourrait être impossible à apporter: il suffit de prouver qu'il y a un risque d'ingérence arbitraire[278].

---

[276] *Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*, (2013/2188(INI)), Strasbourg, Parlement européen, 2014, en ligne : <https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//FR> (consulté le 23 juin 2020).

[277] *Catt c Royaume-Uni,* No 43514/15, [2019] CEDH.

[278] *Zakharov c Russie,* No 47143/06, [2015] CEDH, aux paras 170-172.

Si les tribunaux peuvent statuer sur les lois anti-terroristes ou les mesures révélées, il reste une lacune : tout porte à croire que les décisions prises par les agences de surveillance “secrètes” ne sont pas soumises à une évaluation impartiale. C’est ainsi le cas de la NSA sous FISA par exemple, ou bien qu’il existe officiellement un tribunal qui examine les projets d’opération et donne ou non son aval, cependant un mandat n’est pratiquement jamais refusé[279].Le ‘secret d’État’ peut facilement être utilisé comme couverture pour contourner l’examen des activités d’un service de renseignement, en particulier dans un contexte de lutte contre le terrorisme. La solution ici n’est pas limpide, en ce qu’il peut y avoir des situations où l’opération doit en effet rester secrète. Une possibilité de solution émise par Cour européenne des droits de l’Homme est celle de l’évaluation a posteriori[280]. La Cour a affirmé l’importance d’un tel mécanisme dans l’affaire *Szabo et Vissy c. Hongrie* où elle a relevé les dangers de l’absence d’un tel contrôle au regard du respect de l’État de droit[281]. La solution est imparfaite. Elle aurait possiblement un effet dissuasif sur les services de renseignements, qui sauraient que leurs décisions seraient évaluées et qu’une collecte massive de données, sans discrimination, ne serait pas justifiable.

Le dernier arrêt majeur de la Cour européenne des droits de l’Homme en matière de surveillance numérique est *Big Brother Watch c. Royaume-Uni*[282], qui avait été très anticipé car il faisait suite aux révélations de Snowden. Le recours a été porté par

---

[279] David Kris, « Don’t read too much into the jump in rejected FISA applications », *Lawfare* (26 avril 2018), en ligne : Lawfare <https://www.lawfareblog.com/dont-read-too-much-jump-rejected-fisa-applications> (consulté le 7 août 2020).

[280] *Szabo et Vissy c Hongrie, No 37138/14,* [2016] CEDH, au para 79; Jean-Philippe Foegle, « Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse. » [2016] La Revue des droits de l’homme. Revue du Centre de recherches et d’études sur les droits fondamentaux, en ligne : <http://journals.openedition.org/revdh/2074> (consulté le 10 août 2020).

[281] *Szabo et Vissy c Hongrie, supra* note 274 au para 79.

[282] *Big Brother Watch et autres c Royaume-Uni,* No 58170/13, 62322/14 et 24960/15*,* [2018] CEDH.

plusieurs ONG de défense de droits fondamentaux, et visait le partage de renseignements avec des gouvernements étrangers l'obtention de données de communication auprès de fournisseurs de services de communication. Si l'arrêt, particulièrement détaillé, procède à une condamnation du système britannique de surveillance, il a pu être qualifié de « décevant » par les défenseurs des droits fondamentaux[283].

La première raison de cette déception est que l'examen de la Cour a porté sur une version du *Regulation of Investigatory Powers Act* qui a ensuite été modifiée en 2016 donc le régime en cours n'a pas été évalué, ce qui limite la valeur du jugement à une liste de « bonnes pratiques » à respecter par les États[284]. Après les arrêts qu'elle avait rendu sur le sujet de la surveillance, les commentateurs voyaient en cette requête l'opportunité pour la Cour de réellement condamner la surveillance de masse de manière générale : cependant elle a curieusement rappelé la marge d'appréciation dont bénéficient les états en matière de choix des modalités de surveillance des personnes susceptibles de commettre des actes de nature terroriste ou criminelle[285]. De manière similaire et en contradiction un de ses précédents arrêts[286], la Cour juge que, dans le cadre des mesures de surveillance « de masse », les individus n'ont pas à recevoir de

---

[283] Jean-Philippe Foegle, « La Cour européenne des droits de l'Homme procède à une condamnation en demi-teinte de la surveillance "de masse". » [2018] La Revue des Droits de l'homme Revue du Centre de recherches et d'études sur les droits fondamentaux à la p 18.

[284] *Ibid* à la p 5.

[285] *Ibid* à la p 11.

[286] *Zakharov c Russie, supra* note 278; Voir dans le même sens *Tele2 Sverige AB c Post-och telestyrelsen and Secretary of State for the Home Department c Tom Watson et autres, Affaires jointes C-203/15 et C-698/15,* No ECLI:EU:C:2016:970, [2016] CJUE [*Tele2 Sverige AB*].

notification a posteriori de l'existence d'une interception de leurs données personnelles[287].

L'opinion doctrinale, s'appuyant sur les tests habituellement appliqués en droit international des droits humains, que l'on retrouve au sein des systèmes judiciaires communautaires, à savoir les critères de légalité des mesures employées, du but légitime poursuivi et de la nécessité des mesures au regard du but, a pu arguer que la surveillance de masse telle que pratiquée est illégale en droit international[288]. C'est ce que défend la professeure Eliza Watt, en montrant à travers les exemples des programmes de surveillance PRISM et Tempora, employés respectivement par la NSA et le GCHQ, que les bases légales de ces pouvoirs sont inconnues et inaccessibles[289]. En plus de l'absence de prévisibilité de ces mesures, le but légitime peut être remise en question, particulièrement lorsque qu'il s'agit d'une 'sécurité nationale' indéfinie. Enfin, le principe de nécessité suppose que si un objectif justifie la restriction d'un droit fondamental, c'est la mesure la moins intrusive possible qui doit être prise[290]. L'ampleur de la surveillance, qui n'a virtuellement aucune limite, en particulier lorsqu'il s'agit de la surveillance de communications de non-citoyens par la NSA et le GCHQ[291], paraît ainsi nettement disproportionnée par rapport aux objectifs énoncés par les gouvernements.

Force est de constater que malgré un accord sur le fait que les mesures de surveillance ne doivent pas être arbitraires, les arguments pour une surveillance de masse n'ont pas

---

[287] *Big Brother Watch et autres c Royaume-Uni, supra* note 282 au para 317.

[288] Watt, *supra* note 174.

[289] *Ibid* à la p 780.

[290] *Ibid* aux pp 782-783.

[291] *Ibid* aux pp 776-778.

été clairement rejetés par les tribunaux. L'Europe reste au centre des débats en la matière, car ses tribunaux ont eu à traiter plus de cas de surveillance et avec plus de détails que n'importe quelle autre juridiction[292]. L'opportunité d'adresser de nouveaux enjeux est présente en ce que plusieurs affaires sont en cours devant la Cour européenne des droits de l'Homme sur le même sujet[293].

La jurisprudence a pu établir plusieurs critères et principes en ce qui concerne l'évaluation des mesures de surveillance. Certains tels que la possibilité de se pourvoir en justice lorsqu'il y a simplement un risque d'immixtion arbitraire ou l'exigence d'un contrôle indépendant des mesures des agences étatiques, permettent une protection plus robuste du droit à la vie privée. D'autre part, le recours à la marge d'appréciation des États notamment, ainsi que le manque d'indépendance de certains organes chargés d'évaluer les mesures de surveillance, tendent à autoriser des mesures de surveillance liberticides. Par conséquent, nous présenterons les arguments doctrinaux pour une refonte du droit à la vie privée, pour assurer une protection plus adaptée à une surveillance automatisée et de grande ampleur.

2.1.3. Une nécessaire refonte du droit au vu de l'évolution des attentes en matière de vie privée

La conception de la vie privée a évolué avec les nouvelles technologies : elle a dans un premier temps dépassé les espaces privés, en ne se limitant plus au seul domicile. Il a ensuite été compris que la vie privée ne concerne pas seulement les informations qui seraient considérées dans une conversation privée comme intimes, mais aussi un

---

[292] Murray et Fussey, *supra* note 171 à la p 32.

[293] *10 Human rights organization c Royaume-Uni,* No 960/15, [2016-en cours] CEDH ; *Privacy International c Royaume-Uni (UK 5EY FOIA),* No 606646/14, [2015-en cours] CEDH.

ensemble d'informations qui pourrait sembler anodin, ces données que l'on partage sans y réfléchir. Toutes les données peuvent devenir révélatrices face à des technologies de collecte de données de plus en plus intrusives, qui créent un environnement dans lequel les États et les entreprises sont en mesure d'analyser, de prédire et de manipuler le comportement des individus sur la base de leurs actions en ligne.

L'argument classique des opposants à une protection robuste de la vie privée qui se résume par "je n'ai rien à cacher" est sans cesse utilisé pour justifier des mesures de surveillance ayant pour objet la lutte contre la criminalité[294]. Il suppose que seulement les individus qui commettent des délits et crimes ont à se soucier de la surveillance. C'est également une expression que l'on retrouve communément dans les discours des gouvernements. Elle avait par exemple servi de slogan à une campagne pour le programme d'installation de caméras de surveillance dans les rues par le gouvernement britannique : « *If you've got nothing to hide, you've got nothing to fear*[295] ». L'argument est aussi important à considérer dans la mesure où il reflète l'opinion d'une grande partie de la population[296]. Pourtant, les individus n'ont jamais eu aussi peu de contrôle sur leurs informations, qui sont collectées quotidiennement. Pour plusieurs auteurs, cet argument rencontre autant de succès à cause d'une mauvaise définition et compréhension de ce qu'est la vie privée, en particulier lorsqu'elle est placée en opposition avec la sécurité. Ainsi, le renoncement à une partie de sa vie privée en

---

[294] Daniel Solove, « "I've got nothing to hide" and other misunderstandings of privacy » (2007) 44 San Diego Law Rev 745

[295] « Si vous n'avez rien à cacher, vous n'avez rien à craindre » (Notre traduction) ; Jeffrey Rosen, *The naked crowd: Reclaiming security and freedom in an anxious age*, 1 edition, Random House, 2004 à la p 36.

[296] Solove, *supra* note 294 aux pp 749-750.

échange d'une sécurité assurée par l'État est vu comme un choix utilitaire[297]. En suivant la même logique utilitariste, le droit à la vie privée étant un droit individuel, il est interprété par ses détracteurs comme promoteur de l'individualisme, là où la sécurité bénéficierait à l'ensemble de la population : ainsi, la perte de vie privée est vue comme un sacrifice à faire pour le bien commun[298].

Pour pallier une mauvaise définition de la vie privée, souvent critiquée en ce qu'elle ne lui laisse que peu de chance de triompher dans de tels débats, une autre forme de définition de la vie privée est recherchée. Ainsi, le professeur Daniel Solove, en se basant sur l'idée que « certains concepts n'ont pas une chose en commun, mais sont reliés entre eux de différentes façons[299] », a établi une taxonomie pour grouper tous les éléments liés à la vie privée[300], plutôt que chercher à les définir par un dénominateur commun[301]. Ce qui est entendu par « vie privée » est composé d'une multitude d'éléments, qui ne sont pas forcément reliés entre eux et le droit à la vie privée devrait être un ensemble de protections capable de recouvrir des problèmes différents. La taxonomie est ainsi divisée en quatre catégories que sont la collecte d'informations, le traitement d'informations, la dissémination d'informations et l'invasion, ensuite divisées en seize sous-catégories, dont notamment la surveillance, l'utilisation secondaire, l'insécurité, l'exposition, la distorsion[302]. La volonté derrière ce classement

---

[297] *Ibid* à la p 753.

[298] *Ibid* à la p 761.

[299] Ludwig Wittgenstein, *Philosophical investigations*, 3rd edition, traduit par G E M Anscombe, Englewood Cliffs, NJ, Pearson, 1973 aux paras 65-66 « some concepts do not have 'one thing in common', but are related to one another in many different ways. [...] instead of being related by a common denominator, some things share [...] a complicated network of similarities overlapping and criss-crossing: sometimes overall similarities, sometimes similarities of detail. ».

[300] Voir Daniel J Solove, « A taxonomy of privacy » (2005) 154:3 U Pa Rev 477.

[301] Solove, *supra* note 294 aux pp 755-756.

[302] Solove, *supra* note 300 aux pp 491, 504, 523, 548.

d'enjeux est de se dissocier d'un concept vague de vie privée, et de permettre de reconnaître des problèmes distincts qui ne sont pas pris en compte dans une définition telle qu'elles sont traditionnellement rédigées en droit[303]. La quête d'une définition traditionnelle de la vie privée demeure irrésolue, pendant que des préoccupations importantes méritent d'être examinées, mais sont ignorées car elles ne rentrent pas dans diverses conceptions préfabriquées de la vie privée[304]. Solove critique ainsi le fait que le droit ignore un ensemble de situations qui ne correspondent pas à une certaine définition de la vie privée[305].

De manière plus générale, il soulève le fait que le droit ait fréquemment de la difficulté à reconnaître les maux qui ne sont pas une blessure physique ou psychologique, ou une perte matérielle[306]. Cela rejoint la problématique de la détermination des effets de la surveillance, qui a pu être abordée précédemment notamment en ce qui concerne les *chilling effects*. Ainsi, la protection de la vie privée est rendue doublement difficile, par une définition floue de ce qui doit être protégé, et par la difficulté de prouver les préjudices causés par sa protection inadéquate.

L'argument « rien à cacher » trouve son origine dans une fausse présomption que la vie privée consiste en la dissimulation d'informations incriminantes, et qu'il est juste que ces informations soient dévoilées[307]. Cependant, le pouvoir donné à ceux qui détiennent et ont la capacité d'analyser une telle quantité d'informations est trop

---

[303] Solove, *supra* note 294 à la p 758.

[304] *Ibid* à la p 759.

[305] *Ibid*.

[306] *Ibid* à la p 769.

[307] *Ibid* à la p 764.

important pour faire confiance aveuglément aux gouvernements et entreprises[308]. Dans quelle mesure une agence telle que la NSA, relativement isolée du processus politique et de responsabilité pour ses actions, devrait avoir un pouvoir aussi important sur les individus[309] ?

Il peut raisonnablement être exigé une transparence sur l'usage et la collecte de données si précieuses, et une réelle responsabilité des organes en ayant fait un usage estimé abusif[310]. La question nécessite également une coopération internationale : les flux de données traversent toutes les frontières et un traité international aurait l'ampleur nécessaire pour définir des règles sur la collecte et l'analyse des données, c'est d'ailleurs l'avis du Professeur Joseph Cannataci, rapporteur spécial sur la vie privée des Nations Unies[311].

Si une protection appropriée du droit à la vie privée est indispensable, c'est parce que la surveillance de masse pose de grands dangers pour l'autonomie humaine : plus on connaît une personne, plus il est facile de la contrôler[312]. La possession d'une telle quantité d'informations implique la possibilité de faire perdre aux individus leur individualité[313]. Il y a un réel défi à relever pour encadrer les échanges de données d'une complexité grandissante. L'entre laçage des collectes de données par les acteurs publics et privées, et les nombreux exemples de piratages informatiques sur des larges

---

[308] Bernal, *supra* note 89 à la p 259.

[309] Solove, *supra* note 294 à la p 767.

[310] Taylor, *supra* note 170 aux pp 59-60.

[311] Guillaume Champeau, « Vie privée : le rapporteur spécial à l'ONU veut un traité international », *Numerama*, sect Société (26 août 2015), en ligne : Numerama <https://www.numerama.com/magazine/34013-vie-privee-le-rapporteur-special-a-l-onu-veut-un-traite-international.html> (consulté le 5 juillet 2020).

[312] Zuboff et Chalier, *supra* note 226 à la p 76.

[313] Bernard E Harcourt, *supra* note 106 à la p 217.

bases de données (*data breaches*) nécessite des règles recouvrant aussi bien les requêtes faites aux entreprises par les États que les façons dont ces données doivent être conservées[314]. Il faut pouvoir prendre en compte le fait que la surveillance a lieu dans une société d'exposition[315] composée d'individus qui veulent échanger sur Internet, qui partagent volontairement un grand nombre d'informations personnelles, dans l'espoir de créer des liens ou de s'exprimer sur les causes qui leurs sont chères. Mais en parallèle, les nouvelles technologies de surveillance confèrent à ceux qui les détiennent une grande capacité à profiter de ces données, qui sont si génératrices de profit et faciles à collecter[316].

La tâche n'est pas simple, mais il faut faire mieux. Pour éviter les dérives totalitaires, pour préserver l'individualité de chacun, pour ne pas renforcer des inégalités déjà de plus en plus contrastées : pour un immense nombre de raisons que ce mémoire a l'espoir de retranscrire, il y a besoin d'un cadre juridique plus juste pour encadrer la surveillance. Le droit à la vie privée n'est pas une contrainte extérieure imposée à la société, mais une composante interne de la société[317]. La protection de la vie privée est essentielle à un régime démocratique, car elle préserve et encourage l'autonomie morale des citoyens, un critère central de la démocratie[318]. Une société sans protection de la vie privée de ceux qui la composent suffoque : en protégeant les droits individuels, la société dans son ensemble peut recevoir les bénéfices de la création de zones libres

---

[314] Joseph Cannataci, *Le droit à la vie privée à l'ère du numérique, Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme*, A/HRC/3929, Nations Unies, Conseil des droits de l'Homme, 2018 aux paras 16 et 27.

[315] Bernard E Harcourt, *supra* note 106.

[316] West, *supra* note 53 à la p 31 En 2013, la valeur des données de consommateurs (*consumer data*) était évaluée à 156 milliards USD.

[317] Solove, *supra* note 294 à la p 763.

[318] *Ibid*.

d'intrusion où les individus peuvent s'épanouir[319]. Pour préserver cette autonomie indispensable au fonctionnement de la démocratie, d'autres droits fondamentaux, qui sont liés à la vie privée, peuvent être utilisés. C'est l'option que nous étudierons en dans la partie suivante, ainsi que celle d'un cadre juridique distinct du droit à la vie privée qui prend de plus en plus d'importance : le droit à la protection des données personnelles.

2.2. Les autres cadres juridiques applicables : potentiel et défis

Nous avons pu dans la partie précédente démontrer les forces et faiblesses du cadre juridique du droit à la vie privée lorsqu'il s'agit d'encadrer la surveillance. Plusieurs autres cadres juridiques méritent d'être mentionnés, en ce qu'ils sont aussi touchés par les effets de la surveillance et peuvent être utilisés en complément du droit à la vie privée pour y faire face. Après avoir présenté les façons dont d'autres droits fondamentaux du système international peuvent être mobilisés, et le cadre émergent de la protection des données personnelles qui vient compléter le droit à la vie privée en abordant les aspects techniques de la surveillance, nous montrerons que ces cadres juridiques partagent avec le droit à la vie privée une faille irrésolue : de reposer sur le consentement des utilisateurs d'internet, consentement qu'il est difficile de qualifier de libre et éclairé face à des technologies complexes et des opérations de surveillance gardées secrètes.

---

[319] *Ibid* à la p 762.

2.2.1. L'appui sur les autres droits de la personne

L'idée centrale qui sera exposée est que si le droit à la vie privée joue un rôle central en matière de lutte contre la surveillance abusive et est l'association la plus naturelle, la surveillance a des conséquences tentaculaires qui atteignent de nombreux droits fondamentaux. Tous les droits fondamentaux, invoqués ensemble, peuvent ainsi mieux appréhender la surveillance numérique.

Le rapport du premier rapporteur spécial de l'ONU sur la vie privée a nettement inscrit la surveillance numérique opérée par les États comme relevant du champ du droit international des droits de la personne[320]. La surveillance dans sa forme contemporaine a des implications de droits fondamentaux qui dépassent l'évidente intrusion à la vie privée. Il y a deux raisons pour lesquelles le droit à la vie privée, seul, n'est pas suffisant pour mesurer l'ampleur de la surveillance. Premièrement, parce que le droit à la vie privée étaie de nombreux autres droits fondamentaux, sans lequel ils ne peuvent être exercés[321]. Deuxièmement, la nature d'internet et la façon dont nous l'utilisons, combinées aux technologies des Big Data, créent de nouveaux risques sur l'exercice d'un ensemble de droits fondamentaux[322].

Se concentrer uniquement sur le droit à la vie privée, quand bien même la notion est large, conduit à minimiser les risques de la surveillance et par conséquent placer le standard selon lequel la surveillance est appropriée ou légitime trop bas, lorsque ses effets sur les droits fondamentaux sont mesurés au regard de la justification des

---

[320] Cannataci, *supra* note 314 au para 9; Marko Milanovic, « Human rights treaties and foreign surveillance: privacy in the digital age » (2015) 56:1 Harv Int Law J 81 à la p 85.

[321] Bernal, *supra* note 89 à la p 252.

[322] *Ibid*.

mesures de surveillance[323]. Il convient ici de mentionner les droits fondamentaux connexes à la surveillance et leur lien avec le droit à la vie privée, notamment la liberté d'expression, la liberté d'association, le droit à un procès équitable, la prohibition de la discrimination et la liberté de conscience et de religion. Pour ce faire, nous présenterons ces droits tels qu'ils apparaissent dans les instruments internationaux de droits de la personne et particulièrement le *Pacte international relatif aux droits civils et politiques* car il est le traité de droits humains protégeant le droit à la vie privée le plus ratifié, avec 173 États membres au moment de l'écriture[324].

Un des premiers effets de la surveillance numérique, qui est aussi parfois son objectif, est l'entrave à la liberté d'expression. La liberté d'expression est garantie par l'article 19 du *Pacte international relatif aux droits civils et politiques*[325]. Elle inclut la liberté de partager des informations sans interférence d'une autorité publique. Le lien entre la vie privée et la liberté d'expression, et l'exemple le plus criant en ce qui attrait à la surveillance, est la situation des journalistes[326]. Plus largement, la surveillance intensive va grandement limiter la parole des défenseurs des droits humains, des militants et de tous ceux qui critiquent le régime en place. Si les personnes savent qu'elles peuvent faire l'objet d'une surveillance intensive, elles éviteront de faire des recherches ou d'écrire sur certains thèmes qui pourraient faire d'elles des cibles de surveillance[327].

---

[323] *Ibid*.

[324] Nations Unies, « Collection des traités - Etat des traités - Pacte international relatif aux droits civils et politiques », en ligne : <https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_fr> (consulté le 26 juin 2020); Milanovic, *supra* note 320 à la p 101.

[325] PIDCP, *supra* note 28 art 19; Voir généralement Jean Morange, *La liberté d'expression*, Bruxelles, Bruylant Edition, 2009.

[326] Bernal, *supra* note 89 à la p 254.

[327] PEN America, *supra* note 184.

Cela pose également un problème pour la confidentialité des sources ; si celle-ci ne peut être garantie, cela empêche grandement les journalistes de faire leur travail[328]. Toutes les personnes qui veulent dénoncer certains abus, telles que les personnes menacées par des partenaires violents, les lanceurs d'alerte et autres, pourraient être réticents à s'exprimer s'ils savent que leur identité va être révélée[329]. La sécurité des défenseurs des droits humains est particulièrement menacée sous surveillance étatique et la crainte de représailles peut les empêcher de dénoncer les abus dont ils sont témoins[330].

Dans le même sens, la liberté d'association[331] est particulièrement touchée par une surveillance de masse et limite pour des raisons similaires le militantisme. Partout dans le monde, les réseaux sociaux sont utilisés pour organiser des manifestations et autres actions militantes, les communautés et groupes tiennent leurs réunions et assemblées en ligne ; ainsi par exemple, internet aurait joué un rôle central dans le Printemps arabe[332]. Les réunions et membres des groupes et associations peuvent facilement être identifiés, ciblés et arrêtés lorsque les activités de l'association sont organisées par internet, comme cela a pu être illustré par la surveillance de nombreux organisateurs

---

[328] Bernal, *supra* note 89 à la p 254.

[329] *Ibid*.

[330] Voir à ce sujet Karen Bennett et al, « Critical perspectives on the security and protection of human rights defenders » (2015) 19:7 Int J Hum Rights 883; Karen Bennett, « European union guidelines on human rights defenders: a review of policy and practice towards effective implementation » (2015) 19:7 Int J Hum Rights 908; Amnistie Internationale, communiqué international, « Quand les juges deviennent défenseurs des droits humains » (4 avril 2019), en ligne : <https://amnistie.ca/sinformer/communiques/international/2019/pologne/quand-juges-deviennent-defenseurs-droits-humains> (consulté le 17 avril 2019).

[331] PIDCP, *supra* note 28 art 22.

[332] Bernal, *supra* note 89 à la p 256.

de manifestations par les gouvernements[333]. Pour ce qui est des manifestations, sont également utilisées pour identifier leurs participants la géolocalisation des téléphones portables[334] et la reconnaissance faciale[335]. L'utilisation de ces moyens de surveillance permet, en plus d'identifier les participants et d'exercer une surveillance particulièrement intensive sur leur personne, de dissuader la population de manifester.

La surveillance massive a également un effet néfaste sur les droits de la défense et particulièrement concernant la présomption d'innocence[336]. Au-delà de la surveillance des communications entre les avocats et leurs clients[337], la logique des *Big Data* selon laquelle l'accumulation de données prévaut sur l'exactitude des données est problématique[338]. De plus, les données récoltées sont présentées comme des faits ce qui crée une perte de contestabilité[339]. Les données incriminantes sont difficilement réfutables, car on les pense comme une science exacte et infaillible. Cela signifie pour

---

[333] *Ibid*; Evgeny Morozov, *The net delusion: The dark side of internet freedom*, Reprint edition, New York, NY, PublicAffairs, 2012.

[334] Pour un exemple où les personnes étant à proximité d'un lieu de manifestations à Kiev avaient reçu un SMS menaçant leur indiquant qu'elles étaient à proximité de ce lieu au moment des évènements et visant clairement à les dissuader de manifester à nouveau Heather Murphy, « Ominous text message sent to protesters in Kiev sends chills around the internet », sect General (22 janvier 2014), en ligne : The Lede <https://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sent-to-protesters-in-kiev-sends-chills-around-the-internet/> (consulté le 25 juin 2020).

[335] « La reconnaissance faciale des manifestant·e·s est déjà autorisée », sect Surveillance (18 novembre 2019), en ligne : La Quadrature du Net <https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/> (consulté le 25 juin 2020).

[336] PIDCP, *supra* note 28 art 14.

[337] Bernal, *supra* note 89 aux pp 255-256.

[338] Rouvroy, *supra* note 9 à la p 14.

[339] Antoinette Rouvroy, « The end(s) of critique : data-behaviourism vs. due-process. » dans Ekatarina De Vries, dir, par Mireille Hildebrandt, *Privacy, due process and the computational turn*, Routledge, 2012.

les individus qui font l'objet de profilages une impossibilité de rendre compte des raisons de ses actes ou décisions, de les expliquer[340].

La surveillance intensive et les prédictions permises par la collecte et l'analyse de donnée viennent entraver la liberté de pensée, de conscience et de religion[341]. Si cela peut paraître étonnant au premier abord que le profilage permette de déterminer les pensées d'une personne, c'est en fait son objectif[342]. Il a même pu être argué que Google et Facebook sont en mesure de connaître une personne mieux qu'elle se connaît elle-même en raison de l'absence de « *self-deception*[343] »[344]. La liberté de choisir sa religion et de la pratiquer se trouve également limitée lorsqu'il est possible de déterminer la religion d'un utilisateur en analysant ses données et que cette connaissance pourrait être la raison de discrimination à son égard[345].

Au-delà du cadre juridique des droits de la personne prévus par la Charte des Nations Unies et les traités régionaux, un cadre juridique relativement nouveau permet de cibler la collecte et l'utilisation massive des données permises par des technologies de plus en plus perfectionnées : le droit à la protection de ses données personnelles. La

---

[340] *Ibid*; Rouvroy, *supra* note 9 à la p 15.

[341] PIDCP, *supra* note 28 art 18.

[342] Bernal, *supra* note 89 à la p 253.

[343] L'expression est difficilement traduisible mais pourrait l'être par la périphrase *l'aveuglement que l'on a à propos de soi* et rejoint la difficulté de se connaître soi-même, de se regarder avec objectivité.

[344] James Carmichael, « Google knows you better than you know yourself - predictive analysis combs through calendars and search histories—and gets in the way of routine self-deception. », *The Atlantic* (19 août 2014), en ligne : The Atlantic <https://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/> (consulté le 26 juin 2020); Jon Evans, « When Facebook knows you better than you know yourself », en ligne : TechCrunch <https://social.techcrunch.com/2015/10/24/when-facebook-knows-you-better-than-you-know-yourself/> (consulté le 26 juin 2020).

[345] Bernal, *supra* note 89 à la p 253.

présentation de l'émergence et des principes de ce droit, ainsi que sa comparaison avec le droit à la vie privée, seront l'objet de la sous-partie suivante.

2.2.2. Le droit à la protection des données personnelles : un droit complémentaire au droit à la vie privée

Le droit à la protection des données est un droit relativement récent. La question n'est pas d'actualité au moment de la rédaction des instruments internationaux de droits humains. Le droit à la vie privée avait plus tard été interprété pour l'inclure[346]. Les premières conventions visant expressément la protection des données sont la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe dite Convention 108[347], modernisée en 2018 et portant désormais le nom de Convention 108+[348], et la directive européenne de 1995[349] qui a été abrogée en 2018[350] par l'entrée en vigueur du Règlement général de protection des données[351].

---

[346] Alan Calder, « Bref historique sur la protection des données » dans *RGPD UE*, coll Guide de poche, IT Governance Publishing, 2016, 11 à la p 15.

[347] *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Conseil de l'Europe, STE n°108, 28 janvier 1981 (entrée en vigueur : 1er octobre 1985).

[348] « Modernisation of Convention 108 », *Conseil de l'Europe*, en ligne : Conseil de l'Europe <https://www.coe.int/en/web/data-protection/convention108/modernised> (consulté le 26 juillet 2020).

[349] *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,* [1995] JO L 281.

[350] Calder, *supra* note 346 aux pp 15 et 18.

[351] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)* [2016] JO L 119/1 [RGPD].

Il y a une exception à cette absence de consécration d'un droit à la protection des données personnelles dans les instruments internationaux de droits de la personne : il figure en tant qu'article distinct du droit à la vie privée dans la Charte des droits fondamentaux de l'UE à l'article 8[352]. L'article prévoit en son premier point que toute personne a "droit à la protection des données à caractère personnel la concernant"[353]. L'article contient en son deuxième point plusieurs principes à suivre pour la collecte et le traitement des données : elles 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[354]. Un second droit accordé aux utilisateurs et le droit d'accès aux données collectées les concernant et le droit d'en obtenir la rectification[355].

Le règlement européen majeur qui a porté le droit de la protection des données dans l'actualité et changé le quotidien des utilisateurs d'internet est le *Règlement général de protection des données*, dit RGDP[356]. Il convient de noter que le RGPD ne s'applique pas à la surveillance étatique antiterroriste puisqu'il s'applique uniquement aux entreprises et aux institutions et organes de l'Union et qu'il est explicité que la collecte des données pour des fins de lutte contre la criminalité et pour la sécurité par les États n'est pas soumise au règlement[357]. Cependant ce règlement a eu des répercussions dans le monde entier : au-delà de son ambition de réguler tout le droit européen de la protection des données, il est prévu que son application est extraterritoriale, même si

---

[352] *Charte des droits fondamentaux de l'Union européenne, supra* note 267 art 8.

[353] *Ibid*.

[354] *Ibid*.

[355] *Ibid*.

[356] RGPD, *supra* note 351.

[357] *Ibid* art 2.

elle est difficile à mettre en pratique[358]. Il a d'ailleurs inspiré d'autres réglementations telles que le *California Consumer Privacy Act* (CCPA)[359] où l'état californien a repris un grand nombre de dispositions du RGPD[360]. Le RGPD a fondamentalement modifié les attentes qu'ont les utilisateurs par rapport au traitement de leurs données et affirme plusieurs principes fondateurs pour la collection et l'utilisation des données.

Certains principes sont repris à la Charte des droits fondamentaux de l'Union européenne, tels que la loyauté et la licéité du traitement des données, auxquelles est ajoutée la *transparence* de ce traitement[361]. On retrouve également l'exigence d'objectifs déterminés pour le traitement des données, avec l'ajout que ceux-ci doivent être explicites et légitimes[362]. Le règlement prévoit que les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités, c'est le principe de minimisation des données[363]. L'exactitude des données et la possibilité de les rectifier[364], ainsi que la limitation de la conservation des données dans le temps sont également prévues par le RGPD. Le dernier principe est l'intégrité et la confidentialité des données[365] : ceux qui collectent les données doivent leur assurer une protection

---

[358] Benjamin Greze, « The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives » (2019) 9:2 Int Data Priv Law 109.

[359] *California Civil Code, California Consumer Privacy Act,* 2018, AB-375, s 1798.100.

[360] Baik JS, « Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA) » (2020) 52 Telemat Inform; Stallings William, « Handling of personal information and deidentified, aggregated, and pseudonymized information under the California Consumer Privacy Act » (2020) 18:1 IEEE Secur Priv 61.

[361] RGPD, *supra* note 351 art 5 a.

[362] *Ibid* art 5 b.

[363] *Ibid* art 5 c.

[364] *Ibid* art 5 d.

[365] *Ibid* art 5 e.

suffisante contre d'éventuelles failles de sécurité[366]. Enfin, il revient au responsable du traitement de données de prouver que les principes précédents ont été respectés[367].

La question a pu être posée après la consécration d'un article spécifique protégeant le droit à la protection des données personnelles, distinct du droit à la vie privée, dans la Charte des droits fondamentaux de l'Union européenne, de savoir si le droit à la protection des données est un sous-ensemble du droit à la vie privée, ou s'il apporte des protections supplémentaires aux données personnelles[368]. Le droit à la vie privée ne couvre pas toute information sur des personnes identifiables, mais c'est ce que le droit à la protection des données personnelles vise à couvrir[369]. Si traditionnellement les droits humains ont été mis en place pour protéger les individus des abus de l'État, il est intéressant que le droit à la protection des données crée directement des obligations pour les entreprises[370].

Une autre différence réside dans les interférences permises. Tel que précité[371], 'article 8.2 de la Charte des droits fondamentaux de l'Union européenne prévoit que les 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. Cela signifie que si ces conditions sont remplies, il n'y a pas de violation de l'article 8, sans que le caractère privé ou non des données soient précisé[372].

---

[366] *Ibid* art 5 f.

[367] *Ibid* art 5.2.

[368] Juliane Kokott et Christoph Sobotta, « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR » (2013) 3:4 Int Data Priv Law 222 à la p 222.

[369] *Ibid* à la p 225.

[370] *Ibid* à la p 226.

[371] *Charte des droits fondamentaux de l'Union européenne, supra* note 267 art 8.2.

[372] *Ibid*.

Il peut cependant y avoir une violation de l'article 7, soit du droit à la vie privée, si certaines de ces informations, bien que traitées loyalement, à des fins déterminées et sur la base d'une loi, interfèrent avec le droit à la vie privée[373]. Une addition à la protection des données personnelles dans la Charte des droits fondamentaux est l'exigence de la révision par une autorité indépendante[374], et la CJUE a pu confirmer ce critère dans sa jurisprudence[375].

S'agissant donc du lien entre le droit à la protection des données personnelles et le droit à la vie privée, le premier ne remplace pas le second en termes de surveillance numérique, les deux sont complémentaires. Le droit à la protection des données à caractère personnel garantit à l'individu des prérogatives de contrôle sur ses données quand bien même leur traitement ne constituerait pas une atteinte à la vie privée[376]. En d'autres termes, la protection des données confère à l'individu un certain contrôle sur ses informations et sur ce qui sera exposé au monde, là où la protection de la vie privée garantit la possibilité pour l'individu de construire sa personnalité à l'abri des contraintes extérieurs excessives[377]. Le droit à la protection des données a par ailleurs une finalité spécifique et ajoutée par rapport au droit à la protection de la vie privée, qui est d'avoir parmi ses objectifs la réduction des asymétries de pouvoir et

---

[373] *Ibid*.

[374] *Ibid* art 8.3.

[375] *Commission européenne c République d'Autriche, No C-614/10* [2012] CJUE ; *Commission européenne c République fédérale d'Allemagne, No C-518/07,* [2010] CJUE.

[376] Rouvroy, *supra* note 9 à la p 21.

[377] Philip E Agre, *Technology and privacy: the new landscape*, First Printing edition, Cambridge, Mass, The MIT Press, 1998 à la p 3.

d'information entre les individus et les institutions qui collectent, conservent et traitent les données[378].

Après avoir présenté le cadre juridique de la protection des données personnelles et montré sa différence avec le droit à la vie privée, ainsi que sa complémentarité avec ce dernier, nous montrerons, en s'appuyant sur les arguments de la doctrine, qu'il est construit sur le même modèle que les autres cadres juridiques mobilisables en matière de surveillance : le consentement. Cet appui est particulièrement criant en droit de la protection des données personnelles, où l'utilisateur doit quotidiennement consentir à la collecte de ses informations. Nous montrerons que le recours au consentement d'une personne pose plusieurs difficultés à une protection adéquate des données personnelles collectées.

2.2.3. Un dilemme persistant : le paradigme du consentement

Le cadre juridique de la vie privée, celui de l'ensemble des droits humains, ainsi que celui de la protection des données, sont construit sur le modèle du consentement. Le fonctionnement est le suivant : la loi fournit aux individus un ensemble de droits qui leur permet de prendre des décisions sur la façon dont ils gèrent leurs données. La caractéristique commune entre ce droit à la protection des données et généralement le droit international des droits humains est que l'on peut volontairement renoncer à ses droits. Même si le RGPD prévoit que certaines données « sensibles » bénéficient d'une

---

[378] Voir Orla Lynskey, « Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order » (2014) 63:3 Int Comp Law Q 569.

protection particulière, la majorité des dispositions repose sur le consentement de l'intéressé, ce qui a été repris dans les transpositions au niveau national[379].

Le principe du consentement est central en droits de la personne et nécessaire dans une démocratie où il paraît essentiel de donner cette décision à l'individu, mais il va présenter certaines limites dans le contexte de la surveillance numérique. Ce dilemme du consentement, à savoir sa nécessité, mais à la fois les problèmes qu'il présente, sera l'objet de cette partie où nous présenterons, en s'appuyant principalement sur les recherches du Professeur Daniel Solove[380], les différentes lacunes du consentement comme garantie du respect des droits fondamentaux des individus face à la surveillance numérique.

Les enjeux concernant les informations personnelles deviennent de plus en plus épineux, mais l'approche législative reste inchangée : un ensemble de droits sont accordés aux individus, tels que le droit d'accès ou de notification et il leur revient de les exercer ou non[381]. Pour donner un exemple du quotidien, il revient à l'utilisateur d'aller décocher les cases autorisant certains cookies considérés comme non-nécessaires sur un site internet, mais le visiteur du site peut choisir d'accepter la transmission de ces données à l'ensemble des partenaires et pour une grande variété d'utilisation telles que le marketing ciblé pour n'en citer qu'une seule. Lorsque l'on fait du consentement la base de l'accord d'un droit, on se réfugie dans la volonté de l'individu en question, sans prendre en considération le caractère juste, dangereux ou

---

[379] A titre d'exemple : *Code pénal,* France art 226, qui précise pour chaque offense « sans le consentement ».

[380] Daniel Solove, « Introduction: privacy self-management and the consent dilemma » (2013) 126:7 Harv Law Rev 1880.

[381] *Ibid* à la p 1881.

intrusif de la collecte de certaines données[382]. Cette approche est appelée par Solove « *privacy self-management*[383] ». Les failles du repos sur le consentement peuvent être divisées en deux catégories : premièrement, les difficultés cognitives, qui concernent la façon dont les humains prennent des décisions et deuxièmement, un ensemble de problèmes structurels qui naissent de la façon dont les décisions relatives à la vie privée sont construites[384].

Parmi les problèmes cognitifs, le plus évident est celui qui a été formulé comme « l'individu non-informé[385] ». La plupart des personnes ne lisent tout simplement pas les avis de confidentialité et ne changent pas les paramètres par défaut sur les sites internet[386]. La première hypothèse pour une telle décision tient à la longueur et à la complexité des avis de confidentialité : la question de l'amélioration des avis de confidentialité a donc pu être posée. Cependant, les essais de raccourcissement et d'illustration par des graphiques des avis de confidentialité n'ont montré que peu d'amélioration sur leur fréquence de lecture par les visiteurs des sites internet[387]. Une autre option tient à faire ressentir émotionnellement les effets des décisions que les

---

[382] *Ibid*.

[383] *Ibid* à la p 1884.

[384] *Ibid* à la p 1883.

[385] *Ibid* à la p 1885.

[386] Pour les statistiques et plus de précisions au sujet des études réalisées, voir notamment Helen Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*, 1 edition, Stanford, Calif, Stanford Law Books, 2009 analysant une étude de 2006 montrant que seulement 20% des personnes lisent les avis de confidentialité (TRUSTe & TNS, Consumers have a false sense of security about online privacy : Actions inconsistent with attitudes, PR Newswire) ; Fred H Cate, « The failure of fair information practice principles » dans par Jane K Winn, *Consumer protection in the age of the information economy*, Routledge, 2006, en ligne : Consumer Protection in the Age of the Information Economy <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972#references-widget> (consulté le 26 juillet 2020); George R Milne et Mary J Culnan, « Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices » (2004) 18:3 J Interact Mark 15.

[387] Ryan Calo, « Against notice skepticism in privacy (and elsewhere) » (2012) 87:3 Notre Dame Law Rev 1027 à la p 1056.

utilisateurs doivent prendre quand ils entrent sur un site, à l'image des photographies ou phrases ayant pour but de choquer sur les paquets de cigarettes : l'idée de « *visceral privacy notice* » propose de retenir davantage l'attention des utilisateurs en faisant appel à leurs émotions[388]. La difficulté que présente la simplification ou la mise en image des avis de confidentialité, est qu'elles ne remplacent pas la réelle information des individus : la façon dont les données sont collectées, partagées et traitées est complexe[389]. Par conséquent, il y a une concession à faire entre la production d'une information exacte ou la réduction à quelque chose de court et simple mais qui risque de négliger des éléments importants[390].

Le second défi cognitif qui entache l'approche du consentement est la façon biaisée dont les humains prennent généralement des décisions[391]. Les personnes manquent de l'expertise nécessaire pour évaluer les conséquences de leur consentement à partager certaines données[392]. En réalité, la plupart des personnes renoncent de manière routinière à leurs données pour de très petits bénéfices[393]. Cela peut être illustré par les cartes de fidélité des supermarchés par exemple, qui vont permettre de lier les achats au consommateur, et ainsi la revente de ces informations à divers organismes, telles que les assurances de santé qui pourront les utiliser pour calculer leurs frais en fonction du régime alimentaire du consommateur par exemple. Ce raisonnement n'est pas uniquement visible dans les cas de protection de vie privée et rejoint une littérature plus large des sciences sociales sur certains obstacles à la prise de décisions rationnelles[394].

---

[388] *Ibid* aux pp 1034-1035.

[389] Solove, *supra* note 380 à la p 1886.

[390] *Ibid*.

[391] *Ibid*.

[392] *Ibid*.

[393] *Ibid*.

[394] *Ibid* aux pp 1886-1887.

Deux éléments peuvent être mentionnées ici : la *rationalité limitée*[395], qui fait que nous nous basons sur des modèles simplifiés pour prendre des décisions et la *disponibilité heuristique*[396] selon laquelle nous évaluons les dangers familiers comme plus risqués que ceux qui ne nous sont pas encore familiers. Un dernier élément sur l'imperfection du processus de prise de décisions est le fait que les personnes sont plus enclines à partager leurs informations personnelles quand elles se sentent en contrôle, indépendamment du fait que ce contrôle soit réel ou illusoire[397].

Pour résumer l'ensemble des problèmes cognitifs que pose l'approche de *privacy self-management*, les personnes ne lisent pas les informations concernant la collecte de leurs données. Si certaines personnes les lisent, il reste la difficulté de les comprendre. Quand bien même ces informations sont comprises, ils ne possèdent pas toutes les informations pour faire un choix réellement éclairé et après cela, certaines failles dans le processus de décision général affectent particulièrement ces choix tels que la préférence pour des bénéfices immédiats par exemple[398].

A ces défis s'ajoutent des problèmes structurels : le premier est tout simplement un problème d'échelle. C'est toute la force des Big Data, il y a trop d'entités qui collectent, utilisent et publient une quantité trop importante de données pour qu'elles puissent être appréhendées par une seule personne[399]. Les individus ne possèdent pas les ressources

---

[395] Alessandro Acquisti et Jens Grossklags, « What can behavioral economics teach us about privacy? » dans *Digital Privacy: Theory, Technologies, and Practices*, 2007, 363 à la p 369.

[396] Richard H Thaler et Cass R Sunstein, *Nudge: Improving decisions about health, wealth, and happiness*, Revised&Expanded edition, New York, Penguin Books, 2009 à la p 25.

[397] Laura Brandimarte, Alessandro Acquisti et George Loewenstein, « Misplaced confidences: Privacy and the control paradox » (2013) 4:3 Soc Psychol Personal Sci 340 à la p 3.

[398] Solove, *supra* note 380 à la p 1888.

[399] *Ibid* aux pp 1888-1889.

ou le temps pour effectivement gérer toutes leurs données auprès de toutes les institutions qui les collectent.

Le second problème structurel, toujours lié aux Big Data, est le problème de l'agrégation : il est impossible de déterminer comment nos données vont être classées et assemblées dans le futur[400]. L'effet d'agrégation va permettre à des données qui semblent anodines d'être plus révélatrices lorsqu'elles sont combinées pour faire émerger des profils, schémas, habitudes etc. De plus, le type de prédiction qui pourra être faite sur ce profilage est impossible à anticiper[401].

Le dernier problème structurel est la difficulté d'évaluer les dangers des violations du droit à la vie privée. Ce point rejoint une complexité que nous avons déjà évoquée et qui est souvent reprochée aux partisans d'une protection robuste du droit à la vie privée : où sont les preuves des dommages ? Le mécanisme de *privacy self-management* ne permet pas de prendre en compte les effets non sur le seul individu qui prend la décision sur ses données, mais sur la société dans son ensemble. Pour reprendre les thèses de la Professeure Julie Cohen sur l'importance de la protection de la vie privée des individus pour une société, la vie privée préserve une zone d'autonomie pour les individus[402]. Elle est nécessaire pour permettre l'innovation et la créativité, qui sont asséchées par une surveillance intensive[403]. Le recours au consentement des individus sur la collecte

---

[400] *Ibid* à la p 1891.

[401] *Ibid*; Voir à propos des analyses de données prédictives Eric Siegel et Thomas H Davenport, *Predictive analytics: The power to predict who will click, buy, lie, or die*, 1 edition, Hoboken, New Jersey, Wiley, 2013; Alberto Cordoba, *Understanding the predictive analytics lifecycle*, 1 edition, Wiley, 2014.

[402] Julie Cohen, *Configuring the networked self*, New Haven Conn, Yale University Press, 2012 à la p 1428.

[403] Cohen, *supra* note 197 à la p 1904.

de leurs données crée le risque qu'ils y consentent et affectent l'ensemble de la société par leurs décisions.

Les problèmes structurels de l'approche du consentement peuvent être synthétisés comme suit : l'ampleur et la finalité même des technologies des Big Data ne permettent pas à un humain seul de pouvoir mesurer et anticiper tout ce qui sera révélé sur sa personne. De plus, les effets néfastes des collectes de données vont encore au-delà du niveau individuel et le système de *privacy self-management* ne permet pas de les compenser

Pour conclure sur le consentement, il se trouve à la base de tout ce qui permet de protéger les personnes des effets de la surveillance, mais il présente de nombreuses failles. Cependant, les alternatives à un système qui repose sur le consentement sont-elles plus efficaces pour protéger l'autonomie des individus ? Comment éviter les défauts du consentement, sans priver les personnes de leur libre arbitre ?

La question est majeure et l'alternative principale est le retrait de ce consentement : la détermination, par le droit, des données qui peuvent être collectées, sans laisser le choix à l'utilisateur. Cette alternative rassemble plusieurs partisans[404] ; Solove la qualifie lui de paternaliste[405]. L'argument est que de nombreuses activités qui seraient autrement illégitimes le sont rendues par le consentement[406]. Par exemple, un grand nombre de droits constitutionnels peuvent être abandonnées par consentement. La Professeure Anita Allen argue que le droit à la vie privée est un « *foundational human good* » et

---

[404] Anita Allen, *Unpopular privacy: What must we hide?*, coll Studies in Feminist Philosophy, Oxford, Oxford University Press, 2011 à la p 13; Cohen, *supra* note 402 à la p 148.

[405] Solove, *supra* note 379 à la p 1894.

[406] *Ibid*.

doit ainsi, dans certaines situations, être imposé[407]. Dans le même sens, Cohen explique que les individus ne devraient pas pouvoir renoncer à leur vie privée dans certaines circonstances, parce que lorsque le choix de consentir est laissé, ils le font quasiment tout le temps quand bien même ce n'est pas dans leur intérêt[408].

Le défaut de cette proposition, même si elle évite en effet un certain nombre de problèmes du consentement et qu'une loi très protectrice de la vie privée permettrait une moins grande circulation de données et une limitation des effets négatifs de la surveillance, c'est que les bons choix quant au partage de données ne seraient pas toujours évidents[409]. Ceci est en lien avec le concept de société d'exposition précédemment présenté et la volonté de partage d'informations sur soi et d'opinions via les réseaux sociaux. Le partage de certaines informations et expériences peut être thérapeutique pour certaines personnes[410] alors il faudrait ainsi imaginer une règle capable de s'adapter à un grand éventail de situations.

La nécessité d'un changement de paradigme n'est pas parfaitement démontrée en l'absence d'alternative aussi souple que le consentement. Malgré ses nombreuses limites, la notion de consentement peut difficilement être abandonnée. Certaines recommandations peuvent tout de même être dégagées : premièrement, en prenant en compte la littérature des sciences sociales sur le processus décisionnel, la façon dont les choix sur la protection des données sont proposés pourrait être modifiée[411].

---

[407] Allen, *supra* note 404 à la p 13.

[408] Cohen, *supra* note 402 à la p 148.

[409] Solove, *supra* note 380 à la p 1895.

[410] *Ibid*.

[411] *Ibid* aux pp 1900-1901.

L'alternative au consentement et à l'interdiction de partager certaines données est le compromis entre ces deux théories : ne pas laisser la possibilité de renoncer à la protection de données qui peuvent être dangereuses. C'est ce qu'a probablement tenté de suivre le RGPD dans sa catégorisation de données considérées comme 'sensibles' à l'article 9, que sont les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, la vie sexuelle et l'orientation sexuelle, ainsi que les données génétiques et les données biométriques et concernant la santé. Si le traitement de ces données est en principe interdit, le second paragraphe de l'article liste un grand nombre de possibilités de déroger à cette interdiction, notamment en obtenant le consentement explicite de la personne concernée.

La possibilité de renoncer à certains droits n'est pas nouvelle, mais elle est portée à son paroxysme avec la mise en œuvre du droit à la protection des données personnelles, où il est nécessaire de faire un choix concernant ses données à chaque visite d'un site internet. Le problème central de ce choix est qu'il ne peut être fait en connaissance de cause. Ainsi, l'objectif du consentement qui est de donner un certain contrôle aux utilisateurs sur leurs données n'est pas réalisé et sert de façade pour prétendre à une collecte de données plus juste, car l'individu a, du moins en théorie, accepté la collecte et le partage à une liste immense de « partenaires » de ses données.

De plus, si même les personnes désirant protéger leurs données sont d'une certaine façon contraintes de consentir, tel qu'évoqué précédemment, il reste une partie importante de l'opinion publique qui estime qu'une surveillance intensive est justifiée dans le cadre de la lutte anti-terroriste et qui va donc volontairement consentir à cette surveillance, aidée par des discours des gouvernements poussant ce récit et le manque de transparence sur l'utilisation et l'utilité des informations collectées. Dans ce sous-chapitre nous avons vu qu'il était possible et nécessaire de mobiliser des cadres juridiques autres que le seul droit au respect de la vie privée afin de prendre en compte

toute la gamme des effets de la surveillance et la spécificité de la surveillance automatisée. Nous avons toutefois relevé un nombre d'insuffisances du cadre juridique actuel et souhaitons aboutir cette recherche par l'exploration des solutions proposées pour pallier ces manquements.

2.3. Les solutions possibles, juridiques et extra-juridiques, aux lacunes du cadre juridique entourant la surveillance

L'objectif de cette dernière partie est d'explorer brièvement les possibilités et le futur d'une meilleure protection des individus contre les effets de la surveillance étatique anti-terroriste numérique. Dans un premier temps, nous envisagerons les réformes et pistes proposées pour une nouvelle réglementation, ainsi que certains textes de droit souple afin d'ouvrir la discussion sur les solutions aux lacunes du cadre juridique des droits fondamentaux et de la protection des données personnelles. Pour conclure, nous présenterons certaines stratégies extra-juridiques pour une meilleure protection de la vie privée et des données personnelles, afin de comprendre et d'évaluer les alternatives aux protections juridiques qui s'offrent aux utilisateurs d'internet.

2.3.1. Les propositions de traités, recommandations et lignes directrices des organisations internationales

Jusqu'à maintenant, les États n'ont pas utilisé le droit international pour imposer des contraintes sur l'espionnage entre États[412]. Cela s'explique pour plusieurs raisons ; en premier lieu, par les sources du droit international, les traités sont négociés par les États

---

[412] Ashley Deeks, « Confronting and adapting: Intelligence agencies and international law » (2016) 102:31 Va Law Rev 599 à la p 606.

eux-mêmes. La collecte d'informations donne un avantage considérable aux États et particulièrement aux plus puissants d'entre eux : ainsi ces États n'ont pas la volonté de s'imposer des limites sur des enjeux tels que la sécurité nationale[413]. Deuxièmement, il serait difficile de détecter les violations à un tel traité. Troisièmement, l'ampleur et l'utilisation de la surveillance étaient jusqu'à récemment très secrètes, et les États ne recevaient pas vraiment de pression de la part des individus sur ces sujets[414]. Ceci a changé. Plusieurs révélations sur les accords secrets de surveillance tels que les « Five Eyes[415] » ou « Maximator[416] » ont orienté le regard de la population vers les actions des services de renseignements. Après ces remises en question et les enquêtes réalisées au sujet particulièrement de la NSA, un traité international qui pourrait formuler des principes à respecter pour la surveillance étatique s'avère nécessaire notamment pour la reconstruction d'une relation de confiance entre les États[417] - mais également entre les citoyens et leurs gouvernements, confiance grandement écorchée par les multiples révélations d'espionnage de cette dernière décennie[418]. Bien qu'il ait été argué que les traités secrets entre États ne soient pas nécessairement secrets pour déroger au droit

---

[413] *Ibid* à la p 608.

[414] *Ibid* à la p 614.

[415] Ewen Macaskill et Gabriel Dance, *supra* note 10.

[416] « A beery European spy club is revealed », *The Economist*, en ligne : The Economist <https://www.economist.com/europe/2020/05/28/a-beery-european-spy-club-is-revealed> (consulté le 26 juillet 2020); *Wikipedia*, « Maximator (intelligence alliance) », en ligne : Wikipedia <https://en.wikipedia.org/w/index.php?title=Maximator_(intelligence_alliance)&oldid=969417563> (consulté le 26 juillet 2020).

[417] *Résolution 2045 (2015) Les opérations de surveillance massive*, Conseil de l'Europe, Assemblée parlementaire, Rapporteur Pieter Omtzigt, Doc 13734, 2015, en ligne : <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21583&lang=en> (consulté le 26 juillet 2020); James Ball, « NSA monitored calls of 35 world leaders after US official handed over contacts », *The Guardian*, sect US news (25 octobre 2013), en ligne : The Guardian <https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls> (consulté le 26 juillet 2020).

[418] Watt, *supra* note 174 à la p 785.

international mais pour des raisons sécuritaires[419], la volonté grandissante de transparence et de prise de responsabilité demandée par une grande partie de la société civile de la part des gouvernements verrait en l'accord d'un traité une satisfaction au moins partielle.

Une première proposition visant à réguler l'espionnage international vient du Conseil de l'Europe, et porte le nom d'« Intelligence Codex »[420]. La motivation de cette proposition de traité est née des inquiétudes du Conseil de l'Europe face aux révélations de Snowden sur l'ampleur de la surveillance opérée par la NSA[421]. Quatre règles fondamentales sont suggérées pour régir la coopération entre les services de renseignements[422]. La première et pas des moindres est que toute forme d'espionnage mutuel politique ou économique doit être prohibée sans exception[423]. La seconde règle est que toute opération de surveillance menée sur le territoire d'un autre État doit être précédée d'un accord préalable de l'État en question, dans un cadre légal et pour la raison spécifique de lutte contre la criminalité et le terrorisme[424]. La troisième proposition concerne cette fois ci les individus et prévoit que la collecte l'analyse et le stockage de données est strictement prohibé concernant les individus 'non-suspects' d'un autre État[425]. Seules les informations à propos d'un suspect pourront être

---

[419] Ashley Deeks, « A (qualified) defense of secret agreements » (2017) 49 Ariz St LJ 713.

[420] Watt, *supra* note 174 à la p 784; Assemblée parlementaire, « Rapporteur on mass surveillance reacts to revelations of collusion between NSA and BND », sect Legal affairs and human rights (4 mai 2015), en ligne : <http://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=5592&lang=2> (consulté le 26 juillet 2020); « European rights body again rejects mass surveillance », en ligne : TechCrunch <https://social.techcrunch.com/2015/04/22/european-rights-body-again-rejects-mass-surveillance/> (consulté le 26 juillet 2020).

[421] Conseil de l'Europe, *supra* note 417.

[422] Watt, *supra* note 174 à la p 784.

[423] Conseil de l'Europe, *supra* note 417.

[424] *Ibid*.

[425] *Ibid*.

collectées, de manière exceptionnelle et après évaluation individuelle[426]. Enfin, les services de renseignements n'ont pas le droit de forcer les compagnies internet et de télécommunications à leur accorder un libre accès à leurs bases de données de masse sans décision de justice l'ayant autorisée au préalable[427].

S'agissant de la faisabilité d'un tel traité, s'il demeure difficile d'imaginer un consensus à l'échelle mondiale à cause de désaccords sur la gouvernance du cyberespace[428], il est plus réalistement envisageable que la proposition aboutisse à un accord de non-espionnage mutuel au niveau de l'Union européenne[429]. On peut aussi imaginer l'option d'un accord « volontaire » de droit souple, qui pourrait encourager les États à adhérer plus largement et serait plus facile à amender et modifier[430]. A minima, la proposition a une valeur symbolique comme étant une première tentative de dialogue international sur la question de l'espionnage international[431].

Plusieurs instruments de droits souples ont été rédigé avec la volonté d'encourager la coopération internationale en matière de protection de la vie privée. C'est par exemple le cas de la Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée[432], qui prévoit que les États

---

[426] *Ibid*.

[427] *Ibid*.

[428] Watt, *supra* note 174 à la p 785; Robert M McDowell, « The U.N. threat to internet freedom », *Wall Street Journal*, sect Opinion (21 février 2012), en ligne : Wall Street Journal <https://www.wsj.com/articles/SB10001424052970204792404577229074023195322> (consulté le 26 juillet 2020).

[429] Watt, *supra* note 174 à la p 785.

[430] *Ibid* à la p 787.

[431] *Ibid* à la p 790.

[432] OCDE, *Recommandation de l'OCDE relative à lacoopération transfrontière dans l'application des législations protégeant la vie privée*, 2007.

membres pratiquent l'assistance mutuelle lorsqu'il s'agit de créer et de faire respecter des mécanismes protégeant le droit à la vie privée et encourage la coopération des autorités régionales et nationales entre elles[433].

La nomination en 2015 d'un rapporteur spécial sur le droit à la vie privée parmi les missions spéciales du Haut-commissariat des droits de l'Homme des Nations Unies[434], en plus d'affirmer le besoin urgent de s'intéresser aux enjeux contemporains de la protection de la vie privée, a permis la formulation de plusieurs recommandations sur le respect du droit à la vie privée, que l'on peut regrouper avec une partie des recommandations des rapports de la rapporteuse spéciale sur le respect des droits humains dans le cadre de la lutte anti-terroriste[435] pour obtenir un ensemble de lignes directrices en matière de législation garantissant le droit à la vie privée et la protection des données personnelles. Ainsi, il est recommandé aux États d'adopter une législation robuste et exhaustive en matière de vie privée et de données personnelles[436]. De telles lois devraient prévoir une supervision des mesures de surveillance et des remèdes effectifs[437] lorsque la collecte ou l'utilisation de données a été abusive. D'autre part, les États doivent reconnaître les implications des nouvelles technologies de surveillance au regard du droit à la vie privée mais également de l'ensemble des droits de la personne touchés et adapter leur législation en conséquence[438]. Les États doivent également s'assurer que les systèmes de collectes de données sont uniquement

---

[433] Clarisse Girot, « L'unification réussie : la coopération des autorités nationales en matière de protection des données » (2014) N° 52:1 LEGICOM 109.

[434] Cannataci, *supra* note 313.

[435] Ni Aoláin, *supra* note 8.

[436] Cannataci, *supra* note 313 au para 61 b..

[437] *Ibid*.

[438] *Ibid* au para 61 a.

déployés lorsque les États peuvent démontrer qu'ils sont nécessaires et proportionnés à un but légitime[439].

Il est recommandé aux États de mettre en place des autorités indépendantes chargées d'évaluer les pratiques en matière de vie privée des États et des entreprises, qui auraient le pouvoir d'enquêter sur les pratiques abusives, recevoir des plaintes de la part d'individus et d'organisations[440]. Ces organes indépendants devraient également pouvoir octroyer des amendes et autres peines lorsque le traitement de données personnelles s'avère est illégal[441]. Si ces mécanismes sont déjà en place, il faut alors les renforcer et s'assurer qu'ils aient suffisamment de ressources et sont compétents pour évaluer les mesures de surveillance étatiques[442]. La mise en place d'organes indépendants chargés d'évaluer les pratiques étatiques est également une recommandation de la rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste[443]. Enfin, il est également recommandé aux États de prendre des mesures pour améliorer la transparence et leur responsabilité dans l'acquisition de nouvelles technologies de surveillance[444]. Ces recommandations n'ont pas de caractère obligatoire et les États et les entreprises ne sont donc pas tenus de les respecter. Elles peuvent cependant servir de lignes directrices à ceux désireux de mettre en œuvre de meilleures politiques de

---

[439] *Ibid* au para 61 c.

[440] *Ibid* au para 61 d.

[441] *Ibid*.

[442] *Ibid* au para 61 f.

[443] Ni Aoláin, *supra* note 8.

[444] Cannataci, *supra* note 313 au para 61 h.

protection de la vie privée et servir d'inspiration lorsqu'il sera question de créer de nouveaux instruments juridiques en la matière qui seraient, eux, contraignants.

Après avoir constaté les nombreuses insuffisances du droit en vigueur tout au long de mémoire, il convient d'examiner les potentielles solutions extra-juridiques pour une meilleure protection du droit à la vie privée.

2.3.2. En attendant le droit : les outils alternatifs pour mieux protéger ses informations personnelles

Les lacunes du droit à la vie privée et du droit à la protection des données personnelles génèrent naturellement des inquiétudes quant à la vulnérabilité des utilisateurs d'Internet. Comment se protéger lorsque toutes les données que nous produisons sont collectées ? Si nous n'avons pas ici la possibilité de faire un état des lieux exhaustif de tous les moyens techniques disponibles, nous nous contenterons de présenter deux types de stratégies différentes ; d'une part, le chiffrement et l'anonymat, d'autre part, l'obfuscation.

Le chiffrement peut être définit comme une opération qui consiste à transformer un message à transmettre, dit « message clair », en un autre message, inintelligible pour un tiers, dit « message chiffré », en vue d'assurer le secret de sa transmission[445]. Cela permet de cacher le contenu ou les données liées à une communication ou à une connexion. Pour différencier le chiffrement et l'anonymat, il faut préciser que le chiffrement protège le contenu des communications mais pas les métadonnées qui, telles l'adresse IP, permettent l'identification. Si l'utilisateur n'utilise pas d'outils

---

[445] Éditions Larousse, *sub verbo* « Définitions : chiffrement - Dictionnaire de français Larousse », en ligne : <https://www.larousse.fr/dictionnaires/francais/chiffrement/15322> (consulté le 26 juillet 2020).

protégeant son anonymat, des tiers peuvent collecter des informations importantes sur son identité en analysant des métadonnées. Ainsi, c'est l'anonymat qui permet de ne pas être identifié.[446] Il est ainsi possible d'utiliser, notamment, certains outils tels que les réseaux virtuels privés (VPN, *virtual private network*), les services de proxy, les réseaux et logiciels d'anonymisation et les réseaux entre homologues (*peer to peer*)[447]. Parmi ces technologies, on peut notamment citer la combinaison qui est recommandée par Snowden[448], PGP[449] (*pretty good privacy*) + Tor[450]. PGP est un système de cryptographie asymétrique où chaque utilisateur crée une paire de clefs (une *publique*, l'autre *privée*) et distribue la clé publique. Les signatures effectuées avec la clé privée peuvent être vérifiées en utilisant la clé publique correspondante. Tor est un réseau informatique superposé basé sur le même principe de cryptographie asymétrique, dont le principe est le « routage en oignon », dont les multiples nœuds par lesquels passent l'information permettent une meilleure protection de l'anonymat[451]. Certaines applications et extensions de navigateur proposent aussi de chiffrer ou de « bloquer » les traceurs présents sur les sites web. Ces techniques ne sont pas sans vulnérabilité, mais peuvent être utiles pour un usage quotidien et sont utilisées par les militants et défenseurs des droits humains pour mener leurs actions.

---

[446] David Kaye, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, AGNU, Conseil des droits de l'homme, A /HRC/29/32, 2015 au para 9.

[447] *Ibid*.

[448] Ewen Macaskill et Gabriel Dance, *supra* note 10.

[449] Ben Wolford, « What is PGP encryption and how does it work? », sect Security (8 août 2019), en ligne : ProtonMail Blog <https://protonmail.com/blog/what-is-pgp-encryption/> (consulté le 31 août 2020).

[450] Kaye, *supra* note 446 au para 9.

[451] *Ibid*.

Quelle est la position du droit international sur le sujet ? Le sujet du chiffrement n'a pas formellement été abordé lors de rassemblements internationaux[452], mais le rapporteur spécial sur la promotion et la protection de la liberté d'opinion et d'expression a pu exprimer des recommandations dans son rapport qui aboutit à la conclusion que le chiffrement et l'anonymat permettent aux personnes d'exercer leur droit à la liberté d'opinion et d'expression à l'ère du numérique et qu'ils méritent, à ce titre, une solide protection[453].

Pour asseoir la légitimité et les raisons d'être de ces technologies, le rapporteur spécial vient rappeler que dès le début de l'ère numérique, les autorités ont reconnu le rôle essentiel du chiffrement dans la sécurité de l'économie mondiale et en ont fait usage ou l'ont recommandé pour sécuriser les numéros d'identité générés par les administrations, les données des cartes de crédit, les informations bancaires et les documents confidentiels des entreprises. L'importance de l'accès au chiffrement et à l'anonymat a pu être résumée ainsi :

> *Le chiffrement et l'anonymat, [...] instaurent un espace de confidentialité qui sert à protéger les opinions et les convictions. Par exemple, ils rendent possibles les communications privées et sont capables de mettre les opinions à l'abri de la curiosité extérieure, ce qui est particulièrement important dans les environnements politiques, sociaux, religieux ou juridiques hostiles*[454].

---

[452] Ashley Deeks, « The international legal dynamics of encryption » [2020] Series Paper n°1609 Hoover Inst Pap - Stanf Univ, à l'exception peut-être des lignes directrices de l'OCDE rédigées en 1997 '*Recommendation of the Council concerning Guidelines for Cryptography Policy' C(97)62/FINA*L.

[453] Kaye, *supra* note 446.

[454] *Ibid* au para 12.

Ainsi, toute restriction au chiffrement doit répondre aux critères de légalité, légitimité et nécessité[455]. L'interdiction totale de l'utilisation de technologies de chiffrement à des fins personnelles est, dans tous les cas, disproportionnée car elle prive les utilisateurs du droit de disposer, en ligne, d'un espace privé où formuler leurs opinions et s'exprimer[456]. Le rapport vient également se prononcer sur le débat de l'installation obligatoire de portes dérobées, désirée par les gouvernements américains et britanniques et a conclu qu'étant donnée la vaste portée et de la nature indiscriminée des effets de ce type de failles, l'ensemble des utilisateurs de services en ligne pâtirait, de manière disproportionnée, de leur création.[457] .

La conclusion du rapporteur spécial sur le chiffrement et l'anonymat est de souligner qu'une telle sécurité peut s'avérer indispensable pour l'exercice d'autres droits, notamment les droits économiques, les droits à la vie privée, à une procédure équitable, à la liberté de réunion et d'association pacifiques et le droit à la vie et à l'intégrité physique. Compte tenu de leur importance au regard des droits à la liberté d'opinion et d'expression, les restrictions imposées au chiffrement et à l'anonymat doivent être limitées de manière stricte conformément aux principes de légalité, de nécessité, de proportionnalité et de légitimité de l'objectif poursuivi[458].

La deuxième stratégie de protection, plus teintée par la volonté de révolte contre le système de surveillance numérique, est l'obfuscation. Dans ce contexte, il s'agit d'une technique consistant à « produire délibérément des informations ambigües, désordonnées et fallacieuses et à les ajouter aux données existantes afin de perturber la

---

[455] *Ibid* aux paras 32-35.

[456] *Ibid* au para 40.

[457] *Ibid*.

[458] *Ibid* au para 56.

surveillance et la collecte des données personnelles[459] ». L'ouvrage fondateur du mouvement est *Obfuscation : la vie privée, mode d'emploi* et se veut à la fois un manifeste contre la surveillance contemporaine et un guide pratique pour protéger ses informations personnelles en ligne[460]. L'objectif de l'obfuscation est d'entourer les informations pertinentes de « bruit » rendant leur identification plus longue et difficile : l'obfuscation crée ainsi « un mélange brumeux de signaux où il est possible de se cacher[461] ». La définition mérite d'être illustrée par des exemples : on peut penser aux robots saturants des mots-dièses contestataires sur Twitter pour leur enlever toute pertinence durant les élections russes de 2011, aux logiciels masquant les requêtes effectuées sur un moteur de recherche au milieu de dizaines de recherches automatiques et factices, ou à des enregistrements de fonds sonores contenant plusieurs dizaines de voix pour rendre difficile le déchiffrage de conversations[462].

Au moment de l'écriture, il n'y a pas de mention de l'obfuscation par le droit, ni d'États ayant mis en place des interdictions de l'obfuscation, comme c'est le cas pour le chiffrement et l'anonymat par exemple[463]. Les auteurs du livre mettent toutefois en garde sur l'utilisation mesurée qui doit en être faite et militent pour une mise en balance des différents intérêts en présence, en insistant sur la prise en compte de la préservation de la vie privée des individus[464]. Les techniques d'obfuscation doivent donc, dans cette perspective, être employées de façon réfléchie et mesurée, en

---

[459] Finn Brunton et Helen Fay Nissenbaum auteur, *Obfuscation: A user's guide for privacy and protest*, First MIT Press paperback edition., The MIT Press, 2016 à la p 20.

[460] *Ibid*.

[461] *Ibid* à la p 97.

[462] Camille Girard-Chanudet, « Helen Nissenbaum, Finn Brunton, Obfuscation. La vie privée, mode d'emploi » [2019] Lectures à la p 4, en ligne : Lectures <http://journals.openedition.org/lectures/37113> (consulté le 26 juillet 2020).

[463] Kaye, *supra* note 446 à la p 41.

[464] Girard-Chanudet, *supra* note 462 à la p 5.

fonction des configurations et des objectifs [465] .
Il est important de préciser que le chiffrement, l'anonymat et l'obfuscation ne sont pas réellement des solutions aux atteintes aux droits fondamentaux causées par la surveillance numérique, mais des moyens temporaires de se protéger et de s'exprimer contre l'intensité de cette surveillance afin de pousser au changement législatif.

Ce chapitre a d'abord présenté une définition du droit à la vie privée en droit international, définition qualifiée de nébuleuse par la doctrine et qui dessert une protection appropriée de la vie privée lorsqu'elle est placée face à des objectifs de sécurité, spécifiquement dans le cadre de la lutte anti-terroriste. Si la définition du droit à la vie privée est large et non exhaustive, cette souplesse a toutefois permis aux tribunaux d'élargir sa définition pour l'appliquer à une surveillance contemporaine. Nous avons ensuite pu critiquer le maintien de l'argument de la nécessité d'un tel degré de surveillance par les gouvernements et une acceptation quasi générale de ces propos sans preuve. Les lacunes observées nous ont permis de conclure à l'insuffisance du droit à la vie privée pour appréhender la surveillance étatique.

Pour pallier ce manquement, nous avons étudié la possibilité de mobiliser l'ensemble des droits de la personne affectés par la surveillance de masse. Si les différents cadres juridiques mentionnés ensemble permettent de mieux saisir les effets tentaculaires de la surveillance, ils présentent dans leur mise en place une faille commune : le repos sur le consentement, qui ne peut être réellement libre et éclairé au vu de la complexité des technologies *Big Data*. Nous avons finalement pu mentionner certaines propositions, juridiques et extra-juridiques. Toutefois, nous assistons à l'émergence d'un secteur en ébullition, voué à évoluer dans les années qui suivent, au vu de sa présence dans les débats d'actualité et le développement incessant de technologies de surveillance

---

[465] *Ibid*.

intrusives en parallèle d'un contexte politique et sécuritaire marqué par la lutte anti-terroriste.

CONCLUSION

La surveillance des populations n'est pas une pratique nouvelle. La surveillance contemporaine diffère sur plusieurs points et est notamment caractérisée par l'utilisation de technologies qui permettent des dérives particulièrement dangereuses, mais dont les effets sont difficiles à évaluer. Il existe également des intérêts étatiques très forts à disposer d'un maximum d'informations, d'autant plus que cette ferveur s'est vue justifiée par les attentats du 11 septembre et les suivants. Cependant, les raisons de cette surveillance sont en réalité plus larges et rejoignent un désir de contrôle qui lui n'est pas nouveau ; simplement, les moyens techniques pour sa mise en œuvre ont fondamentalement évolué.

La tâche est imposante pour le droit : régir la collecte et l'utilisation d'informations à très grande échelle dont les méthodes sont majoritairement gardées secrètes, par une multiplicité d'acteurs, dans toutes les juridictions et virtuellement sans limites. En s'intéressant au rôle du droit international des droits de la personne, il a pu être constaté que le droit au respect de la vie privée a pu être invoqué à plusieurs reprises devant les tribunaux pour se défendre des effets de la surveillance de masse. L'Union européenne est décrite comme pionnière en la matière, aussi bien pour ses jurisprudences à issue favorable pour une protection de la vie privée, mais également pour son rôle dans la croissance d'un cadre juridique relativement nouveau : le droit à la protection des données personnelles. L'approche y est différente en ce qu'elle est axée sur le processus de collecte, construite autour du consentement de l'utilisateur et ne prend que légèrement en compte le caractère plus ou moins privé de certaines données par rapport

aux autres. Ainsi, il ne remplace pas le cadre juridique du droit à la vie privée mais vient le compléter. Cependant, les cadres juridiques autres que le droit à la vie privée partage ses failles et leur champ d'action restent limités.

Cela dit, l'intérêt pour la protection des informations face à une surveillance intensive ne faiblit pas et les propositions et solutions juridiques pour une meilleure protection du droit à la vie privée n'en sont qu'à leurs débuts. Le contexte actuel de pandémie mondiale (*Covid-19*) a par ailleurs pu révéler la dangerosité de certaines technologies de surveillance et le débat les concernant montre à quel point le sujet est extrêmement pertinent et prioritaire. En effet, les effets de la surveillance intensive sur les droits de la personne tendent à être moins examinés en temps de crise, en ce que l'attention est détournée par l'objet de la crise. Si ce mémoire souligne les spécificités de la lutte anti-terroriste, il nous semble intéressant d'ouvrir la discussion sur le contexte actuel de crise sanitaire en évoquant certains parallèles entre ces deux motifs de surveillance.

Les potentiels effets des mesures de lutte contre la propagation du coronavirus sur l'exercice des droits humains ont fait l'objet de plusieurs déclarations de la part des organisations internationales, notamment de l'Organisation mondiale de la santé[466] et du Conseil de l'Europe[467]. Ce dernier a ainsi émis des lignes directrices pour le respect des droits de la personne par les gouvernements dans leur gestion de l'épidémie[468]. Ces

---

[466] Organisation mondiale de la santé, *Addressing human rights as key to the COVID-19: response*, WHO/2019-nCoV/SRH/Rights/20201, 2020, en ligne : <https://www.who.int/publications/i/item/addressing-human-rights-as-key-to-the-covid-19-response> (consulté le 26 août 2020).

[467] Conseil de l'Europe, « Coronavirus: guidance to governments on respecting human rights, democracy and the rule of law », sect News 2020 (8 avril 2020), en ligne : <https://go.coe.int/c7W6G> (consulté le 26 août 2020).

[468] Conseil de l'Europe, *Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis A toolkit for member states*, Information Document, SG/Inf(2020)11, 2020, en ligne : <https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40> (consulté le 26 août 2020).

recommandations rappellent les conditions de dérogations aux droits garantis par la Convention européenne des droits de l'Homme, telles que les principes de légalité et de nécessité. Le document liste également l'ensemble des droits de la personne qui sont menacés par les mesures prises par les États. S'agissant du droit à la vie privée et de la protection des données personnelles, si le potentiel de l'accès et de l'utilisation des données de santé pour remédier à la crise sont reconnus, le potentiel intrusif de ces technologies doit être mesuré proportionnellement[469].

Une des mesures spécifiques à cette épidémie est la mise en place d'applications de traçage pour « contrôler » l'épidémie en identifiant les personnes ayant été testées positifs au virus, présentant des symptômes, ou bien ayant été en contact avec une personne testée positive, ou encore se trouvant à proximité d'un foyer de contamination à l'aide de la géolocalisation. Ces applications sont librement téléchargées par les individus, mais leur utilisation est fortement recommandée par les gouvernements et prônée dans les médias. Plusieurs gouvernements ont proposé ce type d'application, c'est notamment le cas de la France où l'application « Stop Covid » a suscité l'indignation, en partie pour son manque de transparence par rapport aux données collectées. Il a par exemple été découvert par des chercheurs en cryptographie que l'application ne recueille pas seulement les identifiants des personnes contacts se situant à moins d'un mètre pendant quinze minutes, tel que ce qui avait été promis par le gouvernement, mais également ceux de toutes les personnes croisées ayant installé l'application pendant les quatorze derniers jours[470].

---

[469] *Ibid* à la p 7.

[470] Géraldine Delacroix, « StopCovid, l'appli qui en savait trop », *Médiapart*, sect Santé (15 juin 2020), en ligne : Médiapart <https://www.mediapart.fr/journal/france/150620/stopcovid-l-appli-qui-en-savait-trop> (consulté le 15 août 2020).

Au Québec, l'utilisation d'une telle application de traçage continue d'être discutée au moment de l'écriture, même si elle est critiquée par la société civile. La Commission des institutions de l'Assemblée nationale du Québec a tenu des « consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19 [471]». La Ligue des Droits et Libertés a notamment présenté un mémoire lors des consultations, soulignant en plus des préoccupations liées à la vie privée que l'efficacité de tels outils n'a pas été démontrée[472].

L'historien contemporain Yuval Noah Haari prévient par ailleurs de la nécessité de penser à « l'après-crise » lorsque l'on cautionne certaines mesures, qui pourraient devenir pérennes[473]. Ce risque rappelle fortement les lois d'état d'urgences établies précipitamment juste après les attentats terroristes et dont les mesures dépassent ladite urgence, jusqu'à devenir pérennes[474]. La surveillance intensive, dans le cadre de la crise sécuritaire du terrorisme, mais plus largement, en temps de crise, est particulièrement problématique en ce qu'elle n'est justement pas limitée à la crise mais que les mesures liberticides perdurent. Il a ainsi pu être observé que les droits limités pendant les crises

---

[471] « Consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts dans le cadre de la lutte contre la COVID-19 - Assemblée nationale du Québec », en ligne : Assemblée nationale du Québec <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci/mandats/Mandat-43205/index.html> (consulté le 26 août 2020).

[472] Ligue des droits et libertés (LDL), *Mémoire de la Ligue des droits et libertés-Consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19*, 2020, en ligne : <https://liguedesdroits.ca/memoire-outils-tracage-numerique-covid19/> (consulté le 15 août 2020).

[473] Yuval Noah Harari, « Yuval Noah Harari: the world after coronavirus », *Financial Times* (20 mars 2020), en ligne : Financial Times <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75> (consulté le 22 mars 2020).

[474] Voir Ni Aoláin, *supra* note 8.

ne sont généralement pas rétablis à leur degré initial après la crise. Ainsi, il est nécessaire de maintenir une vigilance quant aux mesures de surveillance et leurs effets sur l'exercice des droits humains et encore plus particulièrement dans les contextes de crises qui sont propices aux abus.

BIBLIOGRAPHIE

INSTRUMENTS INTERNATIONAUX

Traités

Pacte international relatif aux droits civils et politiques, 16 décembre 1966, 999 RTNU 171 (entrée en vigueur : 23 mars 1976).

Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques, Assemblée générale résolution 2200 A (XXI), 16 décembre 1966, 999 RTNU 302 (entrée en vigueur : 23 mars 1976).

Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs, 14 septembre 1963, 704 RTNU 10106 (entrée en vigueur 4 décembre 1969).

Convention pour la répression de la capture illicite d'aéronefs, 16 décembre 1970, 860 RTNU 12325 (entrée en vigueur : 14 octobre 1971).

Convention pour la répression des actes illicites dirigés contre la sécurité de l'aviation civile, 23 septembre 1971, 974 RTNU 14118 (entrée en vigueur : 26 janvier 1973).

Convention sur la prévention et la répression des infractions contre les personnes jouissant d'une protection internationale, y compris les agents diplomatiques, 14 décembre 1973, Résolution de l'Assemblée générale 3166 (XXVIII) (entrée en vigueur : 20 février 1977).

Convention internationale contre la prise d'otages, 17 décembre 1979, 1316 RTNU 21931 (entrée en vigueur : 3 juin 1983).

Convention sur la protection physique des matières nucléaires, 26 octobre 1979, 1456 RTNU 24631 (entrée en vigueur : 8 février 1987).

Protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale, 24 février 1988, 1589 RTNU 14118 (entrée en vigueur : 6 août 1989).

Convention pour la répression d'actes illicites menés contre la sécurité de la navigation maritime, 10 mars 1988, 1678 RTNU 29004 (entrée en vigueur : 1er mars 1992).

Protocole à la Convention du 10 mars 1988 pour la répression des actes illicites contre la sécurité des plateformes fixes situées sur le plateau continental, 10 mars 1988, 1678 RTNU 29004 (entrée en vigueur : 26 juin 1992).

Convention sur le marquage des explosifs plastiques et en feuilles aux fins de détection, 1er mars 1991, S/22393, (entrée en vigueur : 21 juin 1998).

Convention internationale pour la répression des attentats terroristes à l'explosif, 15 décembre 1997, 2149 RTNU 37517, (entrée en vigueur : 23 mai 2001).

Convention internationale pour la répression du financement du terrorisme, 9 décembre 1999, 2178 RTNU 38349 (entrée en vigueur : 10 avril 2002).

Convention internationale de 2005 pour la répression des actes de terrorisme nucléaire, 13 avril 2005, 2220 RTNU 39481 (entrée en vigueur : 7 juillet 2007).

Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale, 10 septembre 2010, (entrée en vigueur : 1er juillet 2018).

Protocole complémentaire à la Convention pour la répression de la capture illicite d'aéronefs, 10 septembre 2010, (entrée en vigueur : 1er juillet 2018).

Protocole portant amendement de la Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs, 4 avril 2014, (entrée en vigueur : 1er janvier 2020).

Autres sources internationales

Comité des droits de l'Homme, *Observation générale n°16 : Article 17, droit au respect de la vie privée*, Doc NU HRI\GEN\1\Rev.1 (1988).

———, *Observation générale n°29 : États d'urgences (article 4)*, Doc NU CCPR/C/21/Rev1/Add11 (2001).

Conseil de sécurité, *Résolution 1373 sur la menace à la paix et à la sécurité internationales résultant d'actes terroristes*, Doc NU S/RES/1373 (2001).

Commission des droits de l'homme, *Résolution 2005/80 sur la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU E/CN4/RES/2005/80 (2005).

Conseil des droits de l'Homme, *Résolution 15/15 sur la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste: mandat du Rapporteur spécial sur des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU A/HRC/RES/15/15 (2010).

———, *Résolution 22/8 sur la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste: mandat du Rapporteur spécial sur des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU A/HRC/22/L15 (2013).

———, *Résolution 31/3 sur la Protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste : mandat du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc NU A/HRC/RES/31/3 (2016).

Déclaration universelle des droits de l'Homme, Résolution AGNU 217 (III) A, Doc NU A/810, 10 décembre 1948.

INSTRUMENTS REGIONAUX

Union européenne

Conventions

Convention européenne des droits de l'Homme et des libertés fondamentales, Conseil de l'Europe, STCE n°005, 4 novembre 1950 (entrée en vigueur : 3 septembre 1953).

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe STE n°108, 28 janvier 1981 (entrée en vigueur : 1er octobre 1985).

Législation

Charte des droits fondamentaux de l'Union européenne, [2000], JO, 2012/C 326/02.

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, [1995] JO L 281.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) [2016] JO L 119/1.

Jurisprudence

10 Human rights organizations c Royaume-Uni, No 960/15, [2016-en cours] CEDH.

Berrehab c Pays-Bas, No 10730/84 [1988] CEDH.

Big Brother Watch et autres c Royaume-Uni, No 58170/13, 62322/14 et 24960/15, [2018] CEDH.

Catt c Royaume-Uni, No 43514/15, [2019] CEDH.

Commission européenne c République d'Autriche, No C-614/10 [2012] CJUE.

Commission européenne c République fédérale d'Allemagne, No C-518/07, [2010] CJUE.

Digital Rights Ireland c Minister for Communications et autres, Affaires jointes C-293/12 et C-594/12, [2014] CJUE.

Pretty c Royaume-Uni, No 2346/02, [2002], CEDH.

Privacy International c Royaume-Uni (UK 5EY FOIA), No 606646/14, [2015-en cours] CEDH.

SAS c France, No 43835/11 [2014] CEDH.

Szabo et Vissy c Hongrie, No 37138/14, [2016] CEDH.

Tele2 Sverige AB c Post-och telestyrelsen and Secretary of State for the Home Department c Tom Watson et autres, Affaires jointes C-203/15 et C-698/15, [2016] CJUE.

Zakharov c Russie, No 47143/06, [2015] CEDH.

Autres sources européennes

Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, (2013/2188(INI)), Strasbourg, Parlement européen, 2014, en ligne : <https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//FR> (consulté le 23 juin 2020)

Organisation des États américains

Convention américaine relative aux droits de l'Homme, Pacte de San José, Organisation des États américains, 22 novembre 1969 (entrée en vigueur 18 juillet 1978).

INSTRUMENTS NATIONAUX

Législation

British Terrorism Act, Royaume-Uni, Section 2, 2000.

California Civil Code, California Consumer Privacy Act, Etats-Unis, 2018, AB-375, s 1798.100.

Code Criminel, Canada, LRC 1985, c. C-46.

Code pénal, France.

Loi antiterroriste, Canada S.C. 2001, c. 41.

Jurisprudence

Klayman v Obama, Etats-Unis, 2013 United States District Court, District of Columbia.

MONOGRAPHIES

Agre, Philip E. *Technology and privacy: The new landscape*, First printing edition, Cambridge, Mass, The MIT Press, 1998.

Allen, Anita. *Unpopular privacy: What must we hide?*, coll Studies in Feminist Philosophy, Oxford, Oxford University Press, 2011.

Ashworth, Andrew et Lucia Zedner. *Preventive justice*, OUP Oxford, 2014.

Ball, Kirstie, Kevin D. Haggerty et David Lyon. *Routledge handbook of surveillance studies*, coll Routledge international handbooks, Routledge, 2014.

Bauman, Zygmunt et David Lyon. *Liquid surveillance: a conversation*, coll Polity conversations series, Cambridge, UK ; Malden, MA, Polity Press, 2013.

Bentham, Jeremy et Miran Božovič. *The panopticon writings*, 2e éd, coll Radical Thinkers, Verso Books, 2011.

Bianchi, Andrea, dir. *Enforcing international law norms against terrorism*, 1st edition, Oxford, Hart Publishing, 2005.

Browne, Simone. « Race and surveillance » dans *Routledge handbook of surveillance studies*, Routledge, 2012.

Brunton, Finn et Helen Fay Nissenbaum *Obfuscation: a user's guide for privacy and protest*, First MIT Press paperback edition., The MIT Press, 2016.

Calder, Alan. « Bref historique sur la protection des données » dans *RGPD UE*, coll Guide de poche, IT Governance Publishing, 2016, 11.

Cate, Fred H. « The failure of fair information practice principles » dans par Jane K Winn, *Consumer protection in the age of the information economy*, Routledge, 2006.

Champeil-Desplats, Véronique. *Méthodologies du droit et des sciences du droit*, 2e édition, coll Méthodes du droit, Dalloz, 2016.

Cohen, Julie. *Configuring the networked self*, New Haven Conn, Yale University Press, 2012.

Conte, Alex. « Counter-terrorism law in New Zealand » dans Alex Conte, dir, *Human rights in the prevention and punishment of terrorism: Commonwealth approaches: The United Kingdom, Canada, Australia and New Zealand*, Berlin, Heidelberg, Springer, 2010, 185.

Cordoba, Alberto. *Understanding the predictive analytics lifecycle*, 1 edition, Wiley, 2014.

Foucault, Michel. *Surveiller et punir Naissance de la prison*, Gallimard, coll Tel, 1975.

Garland, David. *The culture of control : crime and social order in contemporary society*, OUP 2002

Greenwald, Glenn. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*, Hamish Hamilton, 2014.

Harcourt, Bernard E. *Exposed: desire and disobedience in the digital age*, Harvard University Press, 2015

Klabbers, Jan. *International law*, 2nd edition, Cambridge UK ; New York, Cambridge University Press, 2017.

Koudé, Roger. *La déclaration universelle des droits de l'homme a-t-elle encore un sens ?*, Revue d'études francophones sur l'Etat de droit et la Démocratie, coll Hors-série, Archives contemporaines, 2008.

Laurent, Sébastien-Yves. *Le secret de l'État. Surveiller, protéger, informer XVIIe-XXe siècle*, Nouveau Monde, 2015.

Leman-Langlois, Stéphane. *Sphères de surveillance*, coll Régulation sociale, Montréal, Les Presses de l'Université de Montréal, 2011.

Lyon, David. *Surveillance after September 11*, coll Themes for the 21st century, Malden, Mass, Polity Press in association with Blackwell Pub Inc, 2003.

———. *Surveillance after Snowden*, Polity Press, 2015

———. *Surveillance studies An overview*, Polity Press, 2007.

———. *Theorizing surveillance: the panopticon and beyond*, Cullompton, Willan Publishing, 2006.

Michael, James. *Privacy and human rights: an international and comparative study, with special reference to developments in information technology*, Paris, France; Aldershot, Hampshire, England, UNESCO ; Dartmouth Pub Co, 1994.

Morange, Jean. *La liberté d'expression*, Bruxelles, Bruylant Edition, 2009.

Morozov, Evgeny. *The net delusion: The dark side of internet freedom*, Reprint edition, New York, NY, PublicAffairs, 2012.

Nissenbaum, Helen. *Privacy in context: Technology, policy, and the integrity of social life*, 1 edition, Stanford, Calif, Stanford Law Books, 2009.

Oràà, Jaime. *Human rights in states of emergency in international law*, Oxford, Clarendon Press, 1992.

Roach, Kent. *September 11: Consequences for Canada*, McGill-Queen's Press - MQUP, 2003.

Rosen, Jeffrey. *The naked crowd: Reclaiming security and freedom in an anxious age*, 1 edition, Random House, 2004.

Rouvroy, Antoinette. « The end(s) of critique : data-behaviourism vs. due-process. » dans Ekatarina De Vries, dir, par Mireille Hildebrandt, *Privacy, due process and the computational turn*, Routledge, 2012.

Siegel, Eric et Thomas H. Davenport. *Predictive analytics: The power to predict who will click, buy, lie, or die*, 1 edition, Hoboken, New Jersey, Wiley, 2013.

Sudre, Frédéric. *Les grands arrêts de la Cour européenne des droits de l'homme*, 8e éd, Paris, PUF, 2017.

Thaler, Richard H. et Cass R. Sunstein. *nudge: improving decisions about health, wealth, and happiness*, Revised&Expanded edition, New York, Penguin Books, 2009.

Wittgenstein, Ludwig. *Philosophical investigations*, 3rd edition, trad par G E M Anscombe, Englewood Cliffs, NJ, Pearson, 1973.

Zedner, Lucia. *Security*, Routledge, 2009.

Zuboff, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, First edition, PublicAffairs, 2019.

ARTICLES DE REVUES SCIENTIFIQUES

Amble, John Curtis. « Combating terrorism in the new media environment » (2012) 35:5 Stud Confl Terror 339.

Awan, Imran. « The erosion of civil liberties: Pre-charge detention and counter-terror laws » (2011) 84 Police J 272.

Baik J.S. « Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA) » (2020) 52 Telemat Inform.

Bennett, Karen. « European union guidelines on human rights defenders: a review of policy and practice towards effective implementation » (2015) 19:7 Int J Hum Rights 908.

Bennett, Karen, Danna Ingleton, Alice M. Nah et James Savage. « Critical perspectives on the security and protection of human rights defenders » (2015) 19:7 Int J Hum Rights 883.

Berghel, Hal. « Malice domestic: The Cambridge Analytica dystopia » (2018) 51:5 Computer 84.

Bernal, Paul. « Data gathering, surveillance and human rights: recasting the debate » (2016) 1:2 J Cyber Policy 243.

Brandimarte, Laura, Alessandro Acquisti et George Loewenstein. « Misplaced confidences: Privacy and the control paradox » (2013) 4:3 Soc Psychol Personal Sci 340.

Bruton, Elizabeth et Paul Coleman. « Listening in the dark: audio surveillance, communication technologies, and the submarine threat during the First World War » (2016) 32:3 Hist Technol 245.

Calo, Ryan. « Against notice skepticism in privacy (and elsewhere) » (2012) 87:3 Notre Dame Law Rev 1027.

Castagnino, Florent. « Critique des surveillances studies. Éléments pour une sociologie de la surveillance » (2018) Vol. 42:1 Déviance Société 9.

Cohen, Julie. « What privacy is for » (2013) 126:7 Harv Law Rev 1904.

Conway, Maura. « Terrorism and the internet: New media—new threat? » (2006) 59:2 Parliam Aff 283.

Deeks, Ashley. « Confronting and adapting: Intelligence agencies and International Law » (2016) 102:31 Va Law Rev 599.

———. « A (qualified) defense of secret Agreements » (2017) 49 Ariz St LJ 713.

———. « The international legal dynamics of encryption » [2020] Series Paper n°1609 Hoover Inst Pap - Stanf Univ.

Dijck, Jose van. « Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology » (2014) 12:2 Surveill Soc 197.

Ferejohn, John et Pasquale Pasquino. « The law of the exception: A typology of emergency powers » (2004) 2:2 Int J Const Law 210.

Foegle, Jean-Philippe. « Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse. » [2016] La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux.

———. « La Cour Européenne des Droits de l'Homme procède à une condamnation en demi-teinte de la surveillance "de masse". » [2018] : La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux.

Forgang, Jonathan. « "The right of the people": The NSA, the FISA Amendments Act of 2008, and foreign intelligence surveillance of Americans overseas » (2009) 78:1 Fordham Law Rev 217.

Girard-Chanudet, Camille. « Helen Nissenbaum, Finn Brunton, Obfuscation. La vie privée, mode d'emploi » [2019] Lectures, en ligne : Lectures <http://journals.openedition.org/lectures/37113> (consulté le 26 juillet 2020).

Girot, Clarisse. « L'unification réussie : la coopération des autorités nationales en matière de protection des données » (2014) N° 52:1 LEGICOM 109.

Greze, Benjamin. « The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives » (2019) 9:2 Int Data Priv Law 109.

Haggerty, Kevin D. et Richard V. Ericson. « The surveillant assemblage » (2000) 51:4 Br J Sociol 605.

Head, Michael. « Counter-terrorism laws: A threat to political freedom, civil liberties and constitutional rights Critique and comment » (2002) 26 Melb Univ Law Rev 666.

Isaak, Jim et Mina J. Hanna. « User data privacy: Facebook, Cambridge Analytica, and privacy protection » (2018) 51:8 Computer 56.

Jacobs, Bart. « Maximator: European signals intelligence cooperation, from a Dutch perspective » (2020) 0:0 Intell Natl Secur 1.

Jaluzot, Béatrice. « Méthodologie du droit comparé : bilan et prospective » (2005) 57:1 Rev Int Droit Comparé 29.

Kiss, Alexandre. « Permissible limitations on rights » dans *The International Bill of Rights: the Covenant on Civil and Political Rights*, Louis Henkin, New York, Columbia University Press, 1981.

Kokott, Juliane et Christoph Sobotta. « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR » (2013) 3:4 Int Data Priv Law 222.

Kubler, Kyle. « State of urgency: Surveillance, power, and algorithms in France's state of emergency » (2017) 4:2 Big Data Soc 1.

Lascoumes, Pierre. « La gouvernementalité : de la critique de l'État aux technologies du pouvoir » [2004] 13-14 Portique Rev Philos Sci Hum.

Lynskey, Orla. « Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order » (2014) 63:3 Int Comp Law Q 569.

Marx, Gary T. « Surveillance studies » dans James D Wright, dir, *International encyclopedia of the social & behavioral sciences (Second edition)*, Oxford, Elsevier, 2015, 733.

Mavi, Viktor. « Limitations of and derogations from human rights in international human rights instruments » (1997) 38 Acta Juridica Hung 107.

McCahill, Michael et Rachel Finn. « The social impact of surveillance in three UK schools : “angels”, “devils” and “teen mums” » (2010) 7:3/4 Surveill Soc.

Michel Foucault. « Le panoptisme » dans *Surveiller et punir*, coll Tel, Gallimard, 1975, 229.

Milanovic, Marko. « Human rights treaties and foreign surveillance: privacy in the digital age » (2015) 56:1 Harv Int Law J 81.

Milne, George R. et Mary J. Culnan. « Strategies for reducing online privacy risks: Why consumers read (or don’t read) online privacy notices » (2004) 18:3 J Interact Mark 15.

Münzner, Daniel. « The surveillance of friends: MI5 and friendly aliens during the Second World War » (2014) 13:2 J Intell Hist 131-143.

Murray, Daragh et Pete Fussey. « Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data » (2019) 52:1 Isr Law Rev 31.

Nellis, Ashley Marie et Joanne Savage. « Does watching the news affect fear of terrorism? The omportance of media exposure on terrorism fear » (2012) 58:5 Crime Delinquency 748.

Ofek, Eli et Matthew Richardson. « Dotcom mania: The rise and fall of internet stock prices » (2003) 58:3 J Finance 1113.

Paye, Jean-Claude. « A permanent state of emergency » (2006) 58:6 Mon Rev 29.

Pfaff, Steven. « The limits of coercive surveillance: Social and penal control in the German Democratic Republic » (2001) 3:3 Punishm Soc 381.

Rouvroy, Antoinette. « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives. » [2016] Bur Com Consult Conv Pour Prot Pers À Légard Trait Autom Données À Caractère Pers STE N°18 1.

Rouvroy, Antoinette et Thomas Berns. « Gouvernementalité algorithmique et perspectives d'émancipation » (2013) n° 177:1 Réseaux 163.

Sa'di, Ahmad H. « Colonialism and surveillance » dans *Routledge handbook of surveillance studies*, Routledge, 2012.

Smith, M. J., P. Carayon, K. J. Sanders, S-Y. Lim et D. LeGrande. « Employee stress and health complaints in jobs with and without electronic performance monitoring » (1992) 23:1 Appl Ergon 17-27.

Solove, Daniel. « "I've got nothing to hide" and other misunderstandings of privacy » (2007) 44 San Diego Law Rev 745.

———. « Introduction: privacy self-management and the consent dilemma » (2013) 126:7 Harv Law Rev 1880.

———. « A taxonomy of privacy » (2005) 154:3 U Pa Rev 477.

Stallings William. « Handling of personal information and deidentified, aggregated, and pseudonymized information under the California Consumer Privacy Act » (2020) 18:1 IEEE Secur Priv 61.

Taylor, Nick. « To find the needle do you need the whole haystack? Global surveillance and principled regulation » (2014) 18:1 Int J Hum Rights 45.

Thomas, Timothy L. « Al Qaeda and the internet: The danger of "cyberplanning" » (2003) 33:1 Parameters 112.

Watt, Eliza. « 'The right to privacy and the future of mass surveillance' » (2017) 21:7 Int J Hum Rights 773.

Weimann, Gabriel. « www.terror.net : How modern terrorism uses the internet » Special Report 116 U S Inst Peace 1.

West, Sarah Myers. « Data capitalism: Redefining the logics of surveillance and privacy » (2019) 58:1 Bus Soc 20.

Zuboff, Shoshana et Jonathan Chalier. « Le capitalisme de la surveillance : Un nouveau clergé » [2019] 5 Esprit 63.

AUTRES SOURCES

Belloc, Alexis. *Les postes françaises : recherches historiques sur leur origine, leur développement, leur législation*, Paris, 1886, en ligne : <https://gallica.bnf.fr/ark:/12148/bpt6k94475s> (consulté le 14 février 2020).

Foucault, Michel. *« La gouvernementalité » ; cours du Collège de France, année 1977-1978 : « Sécurité, territoire et population », 4e leçon, 1er février 1978, septembre-décembre 1978*.

Larousse, Pierre. *Grand dictionnaire universel du XIXe siècle*, Tome 3, 1867, en ligne : Grand dictionnaire universel du XIXe siècle <https://gallica.bnf.fr/ark:/12148/bpt6k507258> (consulté le 11 février 2020).

Nadeau, Alain-Robert. *Vie privée et droits fondamentaux : étude de la protection de la vie privée en droit constitutionnel canadien et américain et en droit international.*, Thesis, University of Ottawa (Canada), 2000.

Oudraat De Jonge, Chantal. « Les Nations Unies et la lutte contre le terrorisme » [2004] GE.04-00125 Forum du désarmement, en ligne : <http://digitallibrary.un.org/record/517048> (consulté le 2 août 2020).

Pflaum, Hans-Georg. « Essai sur le cursus publicus dans le Haut-Empire » (1940) 14:1 Mémoires Présentés Par Divers Savants Étrangers À L'Académie 189.

Smith, William et William Wayte. *A dictionary of Greek and Roman antiquities*, John Murray, London, 1890, en ligne : A dictionary of Greek and Roman antiquities <http://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.04.0063:entry=cursus-publicus-cn> (consulté le 11 février 2020).