UCL Université catholique de Louvain

Faculté de droit et de criminologie (DRT)

Lois antiterroristes et surveillance de masse : boîte de Pandore aux dérives en Europe ?

Mémoire réalisé par
Marie Robert

Promoteur
Louis-Léon Christians

Année académique 2017-2018
Master en droit
Droits de l'homme

Plagiat et erreur méthodologique grave

Le plagiat entraîne l'application des articles 87 à 90 du règlement général des études et des examens de l'UCL.
Il y a lieu d'entendre par « plagiat », l'utilisation des idées et énonciations d'un tiers, fussent-elles paraphrasées et quelle qu'en soit l'ampleur, sans que leur source ne soit mentionnée explicitement et distinctement à l'endroit exact de l'utilisation.
La reproduction littérale du passage d'une œuvre, même non soumise à droit d'auteur, requiert que l'extrait soit placé entre guillemets et que la citation soit immédiatement suivie de la référence exacte à la source consultée.*

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

REMERCIEMENTS

Je tiens tout d'abord à remercier chaleureusement ma famille pour son soutien inconditionnel durant ces cinq années d'études, processus au cours duquel ils m'ont toujours épaulée, tant intellectuellement qu'humainement et financièrement. Un merci tout particulier à ma maman, Nathalie, pour sa patience et ses conseils précieux lors de la relecture de ce mémoire.

Je voudrais ensuite remercier la communauté des Kots-à-Projet de Louvain-la-Neuve, et plus particulièrement le Kot Amnesty International dont j'ai eu la chance de faire partie pendant deux ans. Cet univers aussi festif qu'enrichissant m'a accompagnée dans mon épanouissement personnel en tant que citoyenne actrice et responsable, m'a permis de rencontrer des militant(e)s des droits de l'homme inspirants et m'a fortement sensibilisée sur d'innombrables thématiques passionnantes, y compris celle de la surveillance de masse, de la sécurité et du respect de la vie privée.

Enfin, j'aimerais remercier les membres de l'Université Catholique de Louvain ayant contribué à notre formation de qualité, tant ses professeurs de premier ordre, que les personnes de l'ombre. Merci à mon promoteur, Monsieur Louis-Léon Christians, pour sa disponibilité et son intérêt durant la rédaction de ce mémoire. Merci à mon professeur, Monsieur Melchior Wathelet, de m'avoir donné le goût du droit européen et aidée lors de mes recherches. Merci à tous pour votre temps et vos enseignements inestimables.

Le sujet de mon travail est cher à mes yeux en ce qu'il concerne notre société toute entière. La rédaction de ce mémoire m'a permis de faire écho à ceux qui croient en l'avenir, à ceux qui se battent contre le fatalisme, à ceux qui nous inspirent et à ceux qui nous montrent le chemin de la transition à mettre en place.

"They who can give up
essential liberty to obtain
a little temporary safety,
deserve neither liberty nor safety."[1]

~Benjamin Franklin, 1775

[1] B. FRANKLIN, *The Works of Benjamin Franklin*, vol. VII (Letters and Misc. Writings 1775-1779), compiled and edited by John Bigelow, New York : G.P. Putnam's Sons, Knickerbocker Press, 1904, cité par MUSLIM ADVOCATES, *Losing Liberty: the state of freedom 10 years after the Patriot Act*, California, october 2011, p. 3.

Table des matières

INTRODUCTION

Dans une société démocratique, il est essentiel que tant les citoyens que leurs représentants puissent apprécier les principes de sécurité et de vie privée.[2] Les révélations du lanceur d'alerte américain Edward Snowden[3] concernant l'espionnage mondial et généralisé ont eu le mérite d'éveiller quelques esprits critiques. Néanmoins, la surveillance gouvernementale mérite plus que jamais toute notre attention. Les inquiétudes à ce sujet sont souvent accueillies par l'argument « je n'ai rien à cacher ».[4] Serait-ce là un acquiescement face à la fonte progressive de nos libertés fondamentales ? Afin que quelconque lecteur puisse se façonner une opinion quant à cet épineux sujet qu'est l'équilibre entre les mesures antiterroristes et les droits fondamentaux, nous allons, dans ce travail, tenter de dépeindre chaque étape du raisonnement. C'est en forgeant que l'on devient forgeron ; c'est en s'informant que l'on devient citoyen-acteur et que l'on peut répondre en connaissance de cause aux questions qui nous taraudent tous : vivons-nous dans une démocratie équilibrée ? Est-on prêts à se satisfaire chaque jour d'un peu moins de liberté contre un peu plus de sécurité ? Sommes-nous disproportionnellement surveillés ? Le respect des droits de l'homme est-il suffisamment assuré dans le contexte de la lutte contre le terrorisme ?

Nous vivons dans une *démocratie menacée*. Les récentes attaques nous ont procuré la preuve irréfutable que le terrorisme pouvait sérieusement fragiliser nos sociétés libérales. Personne ici ne remettra en question le but légitime poursuivi par la lutte contre le terrorisme – nouvelle priorité gouvernementale en vogue –, en ce qu'il est humainement compréhensible de vouloir prévenir et éviter toute récidive de ces atrocités.[5] Il en relèverait même de l'instinct de survie de l'homme, toujours avide de solutions, le cas échéant à l'aide des nouvelles technologies, pour assurer sa propre sécurité et, partant, prospérité. Le terrorisme instaure un climat menaçant pour les droits de l'homme, l'état de droit et la démocratie, et les Etats ont le devoir de faire tout ce qui est en leur pouvoir pour déjouer et punir efficacement ces actes odieux.[6]

---

[2] NATIONAL RESEARCH COUNCIL, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, Washington DC, The National Academies Press, 2008, p. 1.

[3] Snowden – héros pour certains, criminel pour d'autres – est un ancien employé de la *Central Intelligence Agency (CIA)* et *de la National Security Agency (NSA),* il a révélé publiquement l'existence et le fonctionnement de plusieurs programmes de surveillance de masse américains et britanniques à partir de juin 2013, voir R. KREISSL et D. WRIGHT, « European responses to the Snowden revelations », in *Surveillance in Europe,* New York, Routledge, 2015, p. 1.

[4] EUROPEAN LIBERTIES PLATFORM, *Safe and Sorry – Terrorism & Mass Surveillance*, YouTube, https://www.youtube.com/watch?v=V9_PjdU3Mpo (consulté le 22 juin 2018).

[5] NATIONAL RESEARCH COUNCIL, *op. cit.*, p. 1.

[6] N. MUIZNIEKS, *Lettre du Commissaire aux droits de l'homme du Conseil de l'Europe au Sénat français*, Strasbourg, Conseil de l'Europe, 10 juillet 2017.

Nous vivons une *période paradoxale*. Une ère où, pour défendre nos démocraties, nous employons des méthodes qui la détruisent. Bien que les droits de l'homme soient au cœur de nos démocraties libérales et fondent l'état de droit, les interventions du gouvernement s'effectuent de plus en plus au détriment de ces libertés et droits fondamentaux. Nous jouons aux « pompiers pyromanes »[7] : en voulant protéger les valeurs qui nous sont le plus cher, nous les sacrifions sur l'autel de la sécurité. Plusieurs droits fondamentaux sont concernés, au-delà du droit fondamental au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme, ci-après « CEDH ») : le droit fondamental à la protection des données personnelles (art. 8 Charte des droits fondamentaux de l'Union européenne, ci-après « la Charte »), la liberté de pensée, de conscience et de religion (article 9 CEDH), la liberté d'information et d'expression (article 10 CEDH), la liberté de réunion et d'association (article 11 CEDH), le droit à la non-discrimination (article 14 CEDH), le droit à un recours effectif (article 13 CEDH)… Il est pourtant indéniable que des législations sécuritaires adoptées dans l'urgence et autres mesures disproportionnées n'engendrent que « peur de l'autre, discriminations et stigmatisations » ; qu'un climat basé sur « l'exclusion et le rejet » ne favorisera pas la réalisation pleine et entière de nos « valeurs de démocratie, paix et justice »[8].

Nous vivons à l'*ère numérique*. Les scandales divulgués par Snowden ont fourni la preuve manifeste de l'établissement de certains programmes de grande échelle au sommet des avancées technologiques. Ceux-ci sont développés aux Etats-Unis par les services secrets, en collaboration avec certains Etats membres du Conseil de l'Europe, dans le but de récolter, conserver et disséquer nos données personnelles, telles que les données de communication, de géolocalisation, les historiques de recherche et autres données plus sensibles, notamment les croyances politiques, religieuses et orientations sexuelles.[9] A cet âge digital qui est le nôtre, il existe des techniques de pointe offrant des possibilités inimaginables en termes de surveillance. En traitant chaque citoyen comme un suspect potentiel, la surveillance de masse – en tentant de prédire nos actes – remet en question les fondations même de la présomption d'innocence.[10] Le droit au respect de notre vie privée serait-il rendu caduc par l'abus des progrès technologiques ?

---

[7] C. MACQ et S. VAN OUTRYVE, « Les droits fondamentaux à l'épreuve de la lutte contre le terrorisme », in *Etat des droits de l'homme en Belgique – Rapport 2016-2017* (sous la dir. de Ligue des droits de l'homme asbl), Bruxelles, 2017, p. 34, www.liguedh.be (consulté le 28 juin 2018).

[8] C. MACQ et S. VAN OUTRYVE, *ibidem*, pp. 34 et 35.

[9] COUNCIL OF EUROPE, *Mass surveillance – Who is watching the watchers?*, Editions du Conseil de l'Europe, Strasbourg, mars 2016, p. 5.

[10] J. ZEH, I. TROJANOW, E. MENASSE *et. al.* (Membres du collectif « Writers against mass surveillance »), *Pour une défense de la démocratie à l'ère numérique*, 2013, www.change.org (consulté le 25 juin 2018).

Nous vivons dans un monde fait *d'équilibres*. Le droit fondamental au respect de la vie privée n'est pas un droit absolu. Certaines ingérences peuvent êtres prévues, notamment au nom d'un objectif d'ordre public tel que la lutte contre le terrorisme, le maintien de la sécurité, voire même la sauvegarde du droit à la vie. Néanmoins, Nils Muiznieks – commissaire aux droits de l'homme auprès du Conseil de l'Europe – nous rappelle que la Cour européenne des droits de l'homme a déjà précisé, notamment dans son arrêt *Klass*[11], que l'objectif de lutte contre le terrorisme ne permet pas d'adopter n'importe quelle mesure jugée appropriée par les Etats.[12] En effet, les droits de l'homme et les libertés fondamentales peuvent se voir restreints au nom de cette lutte, mais doivent par ailleurs respecter plusieurs conditions cumulatives, à savoir : respect du principe de légalité, proportionnalité et existence d'un contrôle démocratique.

Nous vivons dans une société propice aux *dérives*. Nos quotidiens, bercés dans le prolongement indéfini de l'état d'urgence, sont de plus en plus habitués à être les témoins des conséquences concrètes et des abus découlant de la mise en œuvre de ces mesures antiterroristes. Entre l'explosion des perquisitions, assignations à résidence, fermetures de lieux de culte et interdictions de manifester, la route vers des ingérences légales et proportionnées est encore longue. En France, la Commission nationale consultative des droits de l'homme a d'ailleurs, dans un avis de 2016[13], insisté sur le fait que l'état d'exception devait demeurer passager au lieu d'imprégner notre droit commun de façon persistante. En outre, les carences les plus importantes en termes de droits fondamentaux au sein de ces dispositions sont souvent similaires : manque de critères précis et de définitions clairement circonscrites, esquive des garanties d'un contrôle judiciaire équitable et effectif, violation du principe de stricte nécessité – applicable à toutes les ingérences dans les droits humains – par des champs d'application trop étendus, octroi de larges pouvoirs discrétionnaires aux autorités administratives – entraînant un risque élevé d'arbitraire, etc.[14] Ces pouvoirs ne sont donc pas toujours suffisamment encadrés par la loi, ni soutenus par des garanties légales adéquates visant à éviter les abus et les dérives.[15]

---

[11] Cour EDH, 6 septembre 1978, arrêt *Klass e.a. et autres c. Allemagne*, § 49.
[12] N. MUIZNIEKS, *op. cit*.
[13] COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME*, Avis sur le suivi de l'état d'urgence,* Paris, assemblée plénière du 18 février 2016, http://www.cncdh.fr/ (consulté le 29 juin 2018).
[14] N. MUIZNIEKS, *op. cit*.
[15] Cour EDH, 12 janvier 2010, arrêt *Gillan et Quinton* c. *Royaume-Uni*.

Nous vivons dans une communauté remplie *d'espoir*. Contrairement à Julian Assange – informaticien, cybermilitant australien et créateur de WikiLeaks, ONG donnant une voix aux lanceurs d'alerte et aux fuites d'information – qui affirme que « l'enjeu de la vie privée est perdu »[16], de nombreuses organisations, personnalités et citoyens sont convaincus qu'un dialogue constructif est capable de rendre à nos valeurs fondamentales leur véritable place. Face à l'informatisation et à la surveillance de masse, nombreux sont ceux qui se battent pour nos droits et libertés. D'un point de vue juridique, les combats sont menés pour limiter les interprétations extensives de concepts tels que « menace terroriste », « suspect potentiel » ou « doutes raisonnables », inciter au respect des principes de stricte nécessité et de proportionnalité, ainsi qu'assurer le déploiement de contrôles en amont de la mise en œuvre de ces mesures et de l'appréciation de ces notions, plutôt qu'en aval.[17]

Ce travail n'a pas la prétention de couvrir tous les niveaux de cette polémique. Il se veut substantiellement sélectif et géographiquement circonscrit. Nous avons en effet sélectionné les cadres législatifs nous paraissant les plus pertinents et actuels en la matière, ainsi que les cas concrets se révélant les plus interpellants, le tout à une échelle parfois internationale, européenne voire nationale selon le sujet traité, bien qu'une dimension européenne sera préférée tout au long de cette analyse. Nous commencerons par une première partie dressant les constats – prémisse essentielle en vue de se donner tous les outils nécessaires à la formation d'un avis critique – en matière de surveillance de masse (Titre I), tant au niveau factuel (Chapitre 1) que législatif (Chapitre 2) et jurisprudentiel (Chapitre 3). Nous continuerons ensuite avec une deuxième partie analysant plus spécifiquement les dérives que peuvent engendrer ces mesures antiterroristes et dénonçant différentes formes d'abus présents aujourd'hui dans nos sociétés (Titre II, Chapitre 1). Par la suite, nous nous interrogerons sur la réelle utilité de ces dispositions en termes d'efficacité et de résultats concrets (Chapitre 2), pour enfin nous plonger dans un examen plus pragmatique des défis, solutions et terrains d'entente envisageables pour contrer les excès et injustices relevés lors de cette recherche (Chapitre 3).

[16] RT FRANCE, *Assange à RT: « l'enjeu de la vie privé est perdu, la surveillance de masse est là pour de bon »*, 10 décembre 2015, https://francais.rt.com/ (consulté le 23 juin 2018).
[17] N. MUIZNIEKS, *op. cit*.

TITRE I. Constats

CHAPITRE 1. Contexte factuel

Section 1. Attaques terroristes et état d'urgence

Depuis les attentats du 11 septembre 2001 jusqu'aux attaques les plus récentes, la lutte contre le terrorisme est devenue une priorité politique absolue.[18] Cette menace n'est cependant pas toujours aisée à gérer. Les exigences de sécurité sont en effet souvent invoquées pour réduire les libertés garanties par les instruments constitutionnels et internationaux des droits de l'homme. Ainsi, nous assistons de plus en plus aux réactions impulsives et puissantes de nos gouvernements et parlements, lorsqu'ils invoquent le bouclier de l'état d'urgence. Ces pouvoirs d'urgence suscitent la controverse : sont-ils utilisés dans la mesure du strict nécessaire, deviennent-ils un danger pour une démocratie fondée sur l'état de droit ? De nombreuses mesures et dispositifs de surveillance et d'intrusion sont prises sans que les garanties encadrant ces méthodes ne soient parallèlement renforcées.[19] Il est nécessaire de réinterroger le cadre juridique existant et de réévaluer le recours à ces mesures d'exception, au risque de voir une 'normalisation' de l'état d'urgence et de ses mesures antiterroristes effrayantes.[20]

Le début du XXIème siècle restera marqué par un retour de la violence terroriste en Occident. Rien n'excuse cette violence meurtrière ni cette haine odieuse. Mais les réponses nationales et internationales qui y sont apportées sont préoccupantes. « La taille de notre pays est inversement proportionnelle à la distance qui semble parfois séparer les gens »[21], et nous tombons dans le piège de la méfiance et de l'intolérance les uns envers les autres. Les forces militaires font désormais partie du décor, tandis que l'état d'urgence – supposé exceptionnel et temporaire – semble devenir notre quotidien.[22] Cela constitue-t-il la réponse la plus indiquée à ce défi du 21ème siècle? Nous allons le voir, il semblerait que « plus que d'un état d'urgence, c'est de l'urgence d'un état où chacun trouve sa place dont nous avons besoin »[23].

---

[18] W. SCHWIMMER, « Préface », in *Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme* (sous la dir. du COMITE DES MINISTRES), Conseil de l'Europe, 2002, p. 5.
[19] AMNESTY INTERNATIONAL, *France. La prolongation de l'état d'urgence risque de normaliser des pouvoirs d'exception*, 16 décembre 2016, www.amnesty.fr (consulté le 7 juillet 2018).
[20] AMNESTY INTERNATIONAL, *ibidem*.
[21] CENTRE INTERFEDERAL POUR L'EGALITE DES CHANCES, *Rapport annuel 2016 : pour une société inclusive, par où commencer ?*, Bruxelles, Unia, 2017.
[22] L'état d'urgence se prolonge à répétition, si bien qu'il aura, par exemple, duré plus de 20 mois en France.
[23] CENTRE INTERFEDERAL POUR L'EGALITE DES CHANCES, *op. cit*.

Section 2. Révélations et scandales

En plus d'un état d'urgence devenu presque permanent, nous ne pouvons non plus rester indifférents face aux divulgations ayant éclaté au grand jour concernant la surveillance globale. Nous avons tous entendu parler des révélations de Snowden – ancien employé de la Central Intelligence Agency (CIA) et de la National Security Agency (NSA), aujourd'hui « lanceur d'alerte » – apparues à partir de 2013 à propos de la surveillance mondiale d'internet, des téléphones mobiles et autres moyens de communications par la NSA. A compter de juin 2013 – apogée où *The Guardian* a débuté à publier certaines de ses révélations[24] –, d'autres médias ont dénoncé les particularités des modes opératoires de la NSA et ses collaborateurs internationaux.[25]

Ces dernières années ont également vu grandir l'ampleur de ces scandales : les divulgations des renseignements collectés par les services secrets américains et britanniques ne peuvent qu'inquiéter. La NSA et les services d'espionnage britanniques sont ainsi capables d'allumer le microphone de votre smartphone, d'activer la caméra de votre ordinateur portable, même éteints, de recueillir vos données de localisation, d'avoir accès à vos relevés téléphoniques,[26]… pour recueillir vos données les plus intimes, et ce sans que vous ne vous rendiez compte de rien.[27] L'opération la plus intrusive des services secrets jamais révélée au grand public est sans doute le programme « PRISM » collectant nos données personnelles en ligne telles que nos courriers électroniques, appels vidéo, documents transférés, informations retenues par les réseaux sociaux – ce qui a d'ailleurs impliqué la collaboration des monstres du net tels que les neuf entreprises internet Google, Facebook, Skype, Amazon, Microsoft, Yahoo, AOL, YouTube et Apple.[28]

Par ailleurs, Wikileaks – organisation non-gouvernementale fondée par le lanceur d'alerte Julian Assange en 2006 – restera l'acteur de la plus grande publication de documents confidentiels sur la CIA. En effet, pas moins de 8761 documents issus de l'agence d'espionnage exposant le programme de piratage ont été publiés le 7 mars 2017, dévoilant ainsi l'immense opération de

[24] G. GREENWALD, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, 6 juin 2013, www.theguardian.com (consulté le 22 juin 2018).
[25] A. LEFEBURE, *L'affaire Snowden – Comment les Etats-Unis espionnent le monde*, Paris, Editions La Découverte, 2014.
[26] R. KREISSL et D. WRIGHT, *op. cit.*
[27] EUROPEAN LIBERTIES PLATFORM, *op. cit.*
[28] N. LEE, *Counterterrorism and Cybersecurity – Total Information Awareness*, 2nd ed., e-book, Springer, 2015, pp. 135-189 ; O. STONE, film *Snowden*, 2 novembre 2016, 1'51'' (regardé le 15 mai 2018).

hacking ayant pris place entre 2013 et 2016 visant citoyens et entreprises américains et étrangers.[29] Les agissements de l'agence se sont basés sur des défaillances de téléphones mobiles (Android, Windows, Linux, Apple), ordinateurs et télévisions intelligentes.[30] Mais quel serait le danger pour nous, citoyens victimes de cet espionnage massif de la population ? Si ces révélations sont bien la preuve qu'aucune technologie n'est infaillible et que la protection de documents secrets ne s'apparente pas à une forteresse imprenable, nous ne pouvons nous empêcher de craindre que ces 'armes numériques' ne soient détournées de leurs fins soi-disant légitimes.[31]

Enfin, ces divulgations ont également terni les relations diplomatiques avec plusieurs alliés européens, et entaché les relations de confiance préexistantes.[32] La Chancelière allemande Angela Merkel avait par exemple, en réaction, demandé l'élaboration d'un pacte de non espionnage entre les Etats-Unis, l'Allemagne et la France.[33] Par ailleurs, la Cour de justice de l'Union européenne, méfiante suite aux révélations de Snowden sur les excès des programmes de surveillance américains, a invalidé en octobre 2015 le régime des « Safe Harbor » – principes de la « sphère de sécurité » encadrant le transfert des données personnelles européennes sur le territoire américain.[34] Pour tenter de calmer les esprits, les Etats-Unis ont entre autres adopté en 2015 le *USA Freedom Act*[35] réformant le régime d'espionnage de la NSA, ainsi que le *Judicial Redress Act*[36] étendant les garanties du *Privacy Act* de 1974[37] aux ressortissants européens.[38]

Néanmoins, aujourd'hui, les pays européens se tournent vers le développement, à leur tour, des mêmes techniques d'intrusion dans la vie privée de la population sous le couvert de la lutte antiterroriste. Progressivement, des lois sont adoptées pour légitimer un potentiel accru de surveillance de la part des services de renseignement à l'échelle mondiale.[39] Prolongation de

[29] M. BODDAERT, *Wikileaks – Ce que l'on sait des méthodes d'espionnage de la CIA*, Libération, 8 mars 2017, http://www.liberation.fr/ (consulté le 22 juin 2018).
[30] M. BODDAERT, *ibidem*.
[31] M. BODDAERT, *ibidem*.
[32] R. KREISSL et D. WRIGHT, *op. cit.*, pp. 11-12 et pp. 30-33.
[33] R. KREISSL et D. WRIGHT, *ibidem*.
[34] CJUE, 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, affaire C-362/14 ; E. DAOUD, *Le Safe Harbor est mort, vive le droit à la vie privée et à la protection des données!*, Dalloz actualité, octobre 2015.
[35] USA Freedom Act of 2015, H.R. 2048.
[36] Judicial Redress Act of 2015, H.R. 1428, 130 Stat. 282.
[37] Privacy Act of 1974, 5 U.S.C. § 552a.
[38] S. PEYROU, « Retour du balancier après le 'tout sécuritaire' : le printemps annoncé de la protection des données à caractère personnel », in *R.A.E.*, 2015, p. 709.
[39] J. ASSANGE, *Sécurité ou surveillance : le droit à la vie privée et la sécurité anti-terroriste peuvent-ils coexister à l'âge digital ?*, Vidéoconférence depuis l'ambassade de l'Equateur à Londres, 20 décembre 2012.

l'état d'urgence et de ses extensions de pouvoir en France, augmentation de caméras de surveillance en Allemagne, adoption de lois antiterroristes alarmantes en Pologne… Si l'on en croit les analyses de Snowden, la loi antiterroriste anglaise de 2016 a permis *« the most extreme surveillance in the history of western democracy »*[40] en ce qu'elle donne l'accès à la police, durant un an, à l'historique de navigation de n'importe quel citoyen, potentiel terroriste ou non. Il est donc compréhensible de se demander si la protection de la vie privée demeure réellement garantie face au développement exponentiel de la surveillance de masse.[41]

Section 3. Origines sociohistoriques et politiques du phénomène

Certes, la surveillance de masse nous paraît être un phénomène récent adjacent à l'ère de la numérisation et du développement technologique et informatique de pointe. Néanmoins, l'on trouve déjà des manifestations de collecte globale des données de la population sous l'Ancien Régime.[42] Quelle a été l'évolution de cette forme de surveillance ? Comment expliquer la vélocité de la propagation ahurissante des techniques de profilage ? Deux acteurs seraient à la source de ce bouleversement. Premièrement, les Etats ont toujours entendu contrôler leurs individus dans le but de maintenir leur propre existence. Toutefois, ce n'est que dans ses dernières variations que la surveillance étatique, animée aujourd'hui par un souci sécuritaire acéré, mise avant tout sur une prévention terroriste et troque sa surveillance ciblée pour une surveillance massive de la population.[43] Deuxièmement, depuis plusieurs années, les entreprises influentes du secteur privé se sont adonnées, suivant un objectif économique, à un recensement massif des données personnelles des consommateurs. A tout cela s'ajoute la révolution numérique et le progrès informatique qui a facilité une « extension, systématisation et accélération du profilage »[44] en quelques années à peine.

---

[40] E. SNOWDEN, *The UK has just legalized the most extreme surveillance in the history of western democracy*, Twitter, 17 novembre 2016, cité par T. ROSSI, *L'ONU, nouvel adversaire de la surveillance de masse*, Libération, 15 mars 2017, http://www.liberation.fr/ (consulté le 3 juillet 2018).

[41] Selon Assange, « La victoire de l'informatisation et de la surveillance de masse sur l'humanité et les valeurs humaines est inexorable », cité par J. ASSANGE, *op. cit.*, 2012.

[42] V. MILLIOT, « L'oeil et la mémoire : réflexions sur les compétences et les savoirs policiers à la fin du XVIIIe siècle, d'après les "papiers" du lieutenant général Lenoir », in *Revue d'Histoire des Sciences Humaines*, n° 19, 2008, pp. 51-73.

[43] C. TILLY, *Coercion, capital, and European states,* AD 990-1990, Cambridge, Massachussets, Blackwell, 1990.

[44] L. FRANCOU et Q. VERREYCKEN, *Compte-rendu de : Armand Mattelart, André Vitalis, Le profilage des populations. Du livret ouvrier au cybercontrôle*, ENS de Lyon, 2014.

Depuis toujours, des techniques existent pour simplifier le contrôle des individus et classifier les actes et mouvements de la population : contrôles d'identité, fichage, profilage, études quantitatives biométriques…[45] Que ne ferait-on pas pour prévenir les risques ? Le premier « fichage systématique » des citoyens en Europe a vu le jour lors de l'élaboration de la sécurité sociale.[46] Après la crise économique des années septante suivie d'une « crise des démocraties occidentales », nous basculons aujourd'hui dans une crise du terrorisme et de l'immigration. Pourrait-on y voir une certaine continuité dans le rôle de l'informatique et des techniques de communication ? Une chose est sûre, ces outils apaisent la peur de l'Etat face à ces crises modernes, le transformant en « Etat surveillant » atteint d'une « fièvre sécuritaire ».[47]

Aujourd'hui, ce rôle de prévention des risques d'attentat est endossé tant par les acteurs publics que privés, qui se dédient à l'analyse de données personnelles recueillies par une surveillance tant horizontale – diffusion de données entre citoyens – que verticale –, avec à sa tête un Etat protecteur et sécuritaire.[48] La croissance du sentiment d'insécurité dans les années 1990 a fait naître un besoin pour l'Etat d'adopter un nouveau rôle : celui de la prévention du crime organisé par l'adoption de mesures politiques et la mise en place de la surveillance. Ce sentiment d'insécurité est devenu l'argument politique par excellence lors de l'adoption et la légitimation des récentes politiques de sécurité – jusqu'aux plus dangereuses pour les libertés fondamentales –, tant ce concept est davantage malléable et flou que d'autres concurrents plus tangibles, tels que les statistiques.[49] Ce choix politique n'est pas surprenant, surtout quand l'on sait que la probabilité de mourir dans un attentat est de 1 pour 116 millions, soit 250.000 fois moins élevée que celle d'être atteints du cancer, ou encore 10 fois moins élevée que nos chances de gagner au lotto. Quand pourrions-nous espérer un investissement dans la recherche contre le cancer[50] ou la prévention du danger des armes à feu aux Etats-Unis[51] équivalent à celui qui est consacré à la surveillance de masse organisée au nom de la lutte contre le terrorisme ?

---

[45] P. BAUDRY, C. SORBETS et A. VITALIS, *La vie privée à l'heure des médias*, Bordeaux, Presses universitaires de Bordeaux, 2002.
[46] L. FRANCOU et Q. VERREYCKEN, *op. cit.*
[47] L. FRANCOU et Q. VERREYCKEN, *ibidem.*
[48] L. FRANCOU et Q. VERREYCKEN, *ibidem.*
[49] H. ADEN, « L'Etat protecteur, mobilisation de nouveaux acteurs et repli sécuritaire. Les politiques de sécurité et de prévention en Allemagne dans les années 1990 », in *Déviance et Société*, 2001, pp. 465-472.
[50] Nous recensons près de 4000 milliards de dollars investis dans la guerre en Irak, en Afghanistan et dans les mesures antiterroristes du côté des Etats-Unis, soit 100 fois plus que la recherche contre le cancer durant les dix dernières années, voir A. SMITH, *On a plus de chance de gagner au loto que de mourir du terrorisme !*, www.youtube.com, 5 décembre 2015 (consulté le 8 juillet 2018).
[51] Aux Etats-Unis, l'année où 3 personnes sont mortes pendant les attentats terroristes au marathon de Boston, 5 personnes sont mortes tuées accidentellement par des enfants de moins de 5 ans qui jouaient avec une arme à feu, voir A. SMITH, *ibidem*.

CHAPITRE 2. Bilan législatif sur la scène européenne

Comment s'est façonné l'arsenal législatif européen relatif à la protection de la vie privée et des données à caractère personnel ? Depuis les essors de la technologie en 1970 – époque à partir de laquelle la traite automatique de l'information s'est développée à vitesse grand v –, de nombreux juristes et organismes publics se sont préoccupés des dangers qu'elle pouvait représenter pour les droits fondamentaux des citoyens, en particulier celui de la protection de la vie privée.[52] Nous allons retracer l'évolution du droit européen en la matière, avec quelques références pertinentes au droit international et national.

Section 1. Historique

§1. Point de vue international

Le Conseil de l'Europe – institution protectrice des droits de l'homme par excellence – a rédigé de nombreuses recommandations et résolutions sur le thème des données personnelles, toutes fondées sur l'article 8 de la Convention européenne des Droits de l'homme (CEDH), qui garantit le droit au respect de la vie privée.[53] A ce sujet, il adopta en 1981 la première Convention d'envergure « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »[54], dite « Convention n° 108 ». A cette Convention de Strasbourg sont attachés des effets contraignants, bien que ses dispositions ne soient pas auto-exécutables : un citoyen ne peut en tirer directement aucun droit.[55] Ainsi, chaque Partie signataire a dû prendre, dans son droit interne, « les mesures nécessaires pour donner effet aux principes de base pour la protection des données »[56] énoncés dans la Convention, et ainsi les rendre exécutoires. Plus particulièrement, la condition de prévoir les mesures nécessaires dans l'ordre judiciaire interne constituait une exigence préalable à la ratification de la Convention. Ainsi, puisqu'en l'absence de l'adoption d'une loi nationale, aucune concrétisation de la Convention n'était envisageable, la Belgique – ayant signé la Convention le 7 mai 1982 et étant

[52] P. DE HERT et S. GUTWIRTH, *Anthologie de la vie privée. Compilation d'articles, de législation et de jurisprudence concernant la protection de la vie privée et des données à caractère personnel pour la Belgique jusque 1998*, Bruxelles, Academic and Scientific Publishers, 2013, p. 9.
[53] P. DE HERT et S. GUTWIRTH, *ibidem*, p. 9.
[54] Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981, approuvée par la loi du 17 juin 1991, *M.B.*, 30 décembre 1993, p. 29023.
[55] P. DE HERT et S. GUTWIRTH, *op. cit.*, p. 11.
[56] Art. 4 de la Convention n° 108 précitée.

légèrement à la traîne du point de vue de son droit interne en matière de vie privée – a adopté cette norme de droit national donnant force de loi à la Convention dans son droit interne.[57]

En parallèle, l'Organisation de Coopération et de Développement économiques (OCDE) a œuvré à l'adoption de directives au niveau international au sujet de la protection des données. A l'image de la Convention n° 108, ces directives visent à inciter les droits nationaux à intégrer le « 'noyau dur' de principes et mesures de protection de la vie privée à l'égard du traitement automatisé de données à caractère personnel » repris dans celles-ci.[58] Néanmoins, bien qu'elles disposent d'une grande force morale de par l'incarnation d'un consensus sur plusieurs principes fondamentaux, les directives de l'OCDE, contrairement à la Convention n° 108, ne sont pas contraignantes.[59]

Enfin, il existe encore d'autres outils législatifs supranationaux ayant contribué à l'élaboration de cet attirail juridique, tels que les directives et résolutions des Nations Unies, les Conventions Schengen et Europol. Ces deux dernières ont par exemple, afin de stimuler le respect des impératifs internationaux et principes nouvellement affirmés, conditionné leur adhésion à la ratification de la Convention n° 108 ainsi qu'à l'adaptation du droit interne des Etats signataires.

Pour conclure, rappelons que la Déclaration universelle des droits de l'homme[60] – outil symbolique et non contraignant – fut la première à affirmer le droit au respect de la vie privée au titre de droit de l'homme en 1948, suivie en 1966 par le Pacte international relatif aux droits civils et politiques[61] – outil juridiquement contraignant. Par ailleurs, la Charte des droits fondamentaux de l'Union européenne[62] – outil initialement purement déclaratoire et symbolique, rendu obligatoire en 2007 grâce au Traité de Lisbonne – détient le rôle principal. En effet, elle fut l'actrice pionnière dans la proclamation d'un droit fondamental à la protection des données à caractère personnel distinct de celui luttant pour le respect de la vie privée – pour

[57] P. DE HERT et S. GUTWIRTH, *op. cit.*, p. 12.
[58] P. DE HERT et S. GUTWIRTH, *ibidem*, p. 11.
[59] « Pour des raisons évidentes, l'initiative substantiellement comparable du Conseil de l'Europe met davantage l'accent sur la protection de la vie privée que ce n'est le cas pour les directives de l'OCDE. En effet, en tant qu'organisation, le Conseil de l'Europe s'aligne très étroitement sur la CEDH et la problématique des droits et libertés fondamentaux de l'homme », voir P. DE HERT et S. GUTWIRTH, *ibidem*, p. 11.
[60] Déclaration universelle des droits de l'homme, adoptée par l'Assemblée Générale des Nations Unies, signée à New York le 10 décembre 1948.
[61] Pacte international relatif aux droits civils et politiques, signé à New York le 16 décembre 1966, approuvé par la loi du 15 mai 1981, *M.B.*, 6 juillet 1983, p. 8806.
[62] Charte des droits fondamentaux de l'Union européenne, *op. cit.*

le reste consacré par la Convention européenne des droits de l'homme[63]. Ainsi, la Charte est libellée comme suit :

Article 7
Respect de la vie privée et familiale
Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Article 8
Protection des données à caractère personnel
1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

§2. Point de vue européen

A l'époque de l'adoption par le Conseil de l'Europe de la Convention n° 108 précitée, la Communauté européenne a, dans un premier temps, poussé ses Etats membres à ratifier celle-ci. Ensuite, au début des années 1980, la Commission européenne s'est mise à publier des recommandations adressées aux Etats membres[64], tandis que le Parlement européen a publié une série de résolutions en la matière[65]. Par la suite, la Commission européenne diffusa une communication à propos de la protection des personnes à l'égard du traitement de données à caractère personnel, ce à quoi une proposition de directive comprenant les principes fondamentaux sur le sujet emboîta le pas en 1990.[66]

Ce premier mouvement donna naissance cinq ans plus tard à l'adoption de la directive 95/46/CE *relative à la protection des personnes physiques à l'égard du traitement des données à*

[63] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, p. 5028.
[64] Comme par exemple « la recommandation datant du 29 juillet 1981 *concernant une convention du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, recommandant aux Etats membres de signer la Convention n° 108 dans le courant de l'année 1981 et de la ratifier avant la fin de l'année 1982 » , voir P. DE HERT et S. GUTWIRTH, *op. cit.*, p. 12.
[65] Comme par exemple « la résolution du Parlement européen du 9 mars 1982 *sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique* », voir P. DE HERT et S. GUTWIRTH, *ibidem*, p. 12.
[66] P. DE HERT et S. GUTWIRTH, *ibidem*, p. 13.

caractère personnel et à la libre circulation de ces données[67]. Sa rédaction donna du fil à retordre aux Etats, faute d'accord unanime et de positions communes entre eux.[68] Par exemple, le critère relatif à l'autorisation du transfert de données personnelles en direction de pays tiers s'est vu tempéré en comparaison à celui prévu dans la Convention n° 108 ou dans les directives OCDE, en vue de faciliter une entente avec les Etats-Unis et ses entreprises. Ainsi, la directive prévoyait qu'une transmission de données fut possible à condition que le pays de destination offre non plus une protection « équivalente » mais bien une protection « appropriée ou adéquate ».[69]

L'article 1er de la directive constituait en lui-même la preuve du double objectif contradictoire poursuivi : à la fois protéger les libertés et droits fondamentaux des personnes physiques – « notamment de leur vie privée, à l'égard du traitement des données à caractère personnel » – tout en affirmant le droit économique de la libre circulation des données entre Etats membres. Enfin, la définition elle-même du concept de « données à caractère personnel » était ambivalente : sa nature juridique se partageant entre élément de la personne et bien économique.[70] Cette notion se définissait comme suit :

> « *Toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ».[71]

Bien que cette directive visait à « préciser et amplifier » les principes de la Convention n° 108, elle présentait quelques faiblesses et ne couvrait pas tous les cas de figure désormais envisageables. Par exemple, elle ne s'appliquait pas au « traitement de données effectué dans la sphère de la police, de la Justice et des services secrets ».[72] Pourtant, l'on imagine bien qu'à l'heure du numérique, de l'état d'urgence et de la surveillance gouvernementale accrue, une

---

[67] Dir. (CE) n° 95/46 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, *J.O.C.E.*, L.281/31, du 23 novembre 1995.

[68] C. CASTETS-RENARD, « Introduction – Les enjeux et l'actualité de la protection des données personnelles en Europe », in *Quelles protections des données personnelles en Europe?* (sous la dir. de I. DE LAMBERTERIE, A. STROWEL et C. CASTETS-RENARD), Bruxelles, Larcier, 2015, p. 24.

[69] Nous étudierons de nouveau cette question dans la deuxième section de ce chapitre ; P. DE HERT et S. GUTWIRTH, *op. cit.*, p. 13.

[70] C. CASTETS-RENARD, *op. cit.*, p. 24 ; J. ROCHFELD, Notes du colloque sur *« les biens numériques »* (sous la dir. de A. CHAIGNEAU et E. NETTER), Université d'Amiens, Paris, coll. CEPRISCA, 2014.

[71] Art. 2 de la Dir. 95/46/CE précitée.

[72] P. DE HERT et S. GUTWIRTH, *op. cit.*, p. 14.

révision de la directive de 1995 était inévitable. De plus, la définition énoncée *supra* ne rendait pas compte du fait que « la collecte et l'usage des informations se rapportant aux individus puissent être particulièrement intrusifs et intimes »[73]. La section suivante tentera d'exposer les raisons les plus évidentes qui ont poussé à la mise à jour de cette directive, et de la suite donnée à la proposition de règlement de la Commission européenne du 25 janvier 2012.[74]

Après quatre ans de négociations législatives, le nouveau règlement européen n° 2016/679 – dit règlement général sur la protection des données (RGPD) – abroge et remplace ainsi, depuis son entrée en vigueur le 25 mai dernier, la directive 95/46/CE. Celui-ci fera l'objet d'un examen détaillé dans la troisième section de ce chapitre. Enfin, précisons tout de même qu'en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel *par les institutions et organes communautaires*, il y aura lieu d'appliquer le règlement n° 45/2001/CE du Parlement européen et du Conseil datant du 18 décembre 2000 – actuellement en cours de révision – et non ce nouveau règlement. Les hypothèses concernées par cette dernière se présentent par exemple lors de l'utilisation des services en ligne proposés par les sites web des institutions européennes dans le champ « .eu ».[75]

§3. Point de vue national belge

C'est dès les années 1970 que l'on a pu voir apparaître un intérêt législatif pour la protection des personnes au niveau de l'usage automatisé de leurs données à caractère personnel. La volonté d'encadrer l'usage des banques de données et protéger les individus face aux pratiques d'écoute et d'espionnage a en effet surmonté l'absence d'une loi générale sur la protection de la vie privée.[76] C'est ainsi que diverses dispositions ont vu le jour, chacune avec un champ d'application limité à un domaine spécifique de la protection de la vie privée en relation avec le traitement des données personnelles : registre national des personnes physiques, banques centrales de données dans plusieurs secteurs spécifiques, Banque-carrefour de la sécurité sociale, cartes d'identité… En l'absence de lois spécifiques, d'autres moyens de protection étaient également mobilisés : anciens articles 10 et 22 de la Constitution (actuellement articles 15 et 29 respectivement) affirmant la protection du domicile et l'inviolabilité du secret des lettres – bien qu'ils ne constituent pas une protection pleine et entière de la vie privée, l'article 8

[73] C. CASTETS-RENARD, *op. cit.*, p. 25.
[74] C. CASTETS-RENARD, *ibidem*, p. 35.
[75] COMMISSION EUROPEENNE, *Protection de la vie privée – Protection des données à caractère personnel*, fiche informative, www.ec.europa.eu (consulté le 4 juillet 2018).
[76] P. DE HERT et S. GUTWIRTH, *op. cit.*, pp. 19 et 20.

de la CEDH comblant les éventuelles absences grâce à son effet direct –, la loi pénale – comme par exemple ses articles 460 (secret des lettres), 443 (calomnie) et 439 et suivants (violation du domicile) –, voire même d'autres branches du droit telles que le droit civil (art. 215 et 218 relatifs au domicile conjugal), le droit fiscal, le droit d'auteur, ainsi qu'enfin certaines règles spécifiques telles que la loi relative aux radiocommunications, la loi organisant la profession de détective privé, la loi sur la fonction de police, etc.[77]

Mais c'est réellement au cours des années 1990 – toujours en conséquence de l'apparition de nouvelles menaces que constituent les avancées et innovations technologiques pour la vie privée, ainsi qu'en réaction à la pression internationale et la création de la Banque-carrefour de la sécurité sociale nationale – que les négociations sont redevenues brûlantes.[78] En effet, c'est par exemple en 1991 que la Belgique a ratifié – et par là, s'est engagée à respecter et mettre en œuvre – la Convention n° 108 du Conseil de l'Europe précitée. Quant à la Convention de Schengen, sa convention d'application spécifiait qu'aucune ratification n'était envisageable sans édification préalable d'une législation nationale.[79] Dès lors, débitrice de l'obligation de promulguer et d'appliquer une législation en la matière, la Belgique a adopté – sous l'initiative parlementaire du ministre de la Justice de l'époque Melchior Wathelet, encore surnommé aujourd'hui « l'initiative Wathelet » – la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[80]. Réponse davantage tournée vers la pression internationale ou les inquiétudes nationales ? En tout état de cause, l'acte était scellé.

Mais déjà en 1995, suite à l'adoption de la directive 95/46/CE précitée appelant toutes les Parties signataires à adapter leur législation interne, et ce avec comme date limite le 25 octobre 1998[81], l'on entrevoyait la mutation législative. D'abord au moyen d'arrêtés royaux, la profonde réforme s'est finalement matérialisée dans la loi du 11 décembre 1998 transposant la directive de 1995, prenant la forme d'une modification de la loi du 8 décembre 1992 afin de satisfaire aux obligations contractées.[82]

---

[77] P. DE HERT et S. GUTWIRTH, *ibidem*, pp. 19 à 31.
[78] P. DE HERT et S. GUTWIRTH, *ibidem*, p. 36.
[79] P. DE HERT et S. GUTWIRTH, *ibidem*, p. 36.
[80] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.
[81] Date limite de transposition de la directive en droit national.
[82] P. DE HERT et S. GUTWIRTH, *op. cit.*, pp. 45 et 46.

La loi pivot du 6 janvier 2003[83] régulant les *méthodes particulières de recherche* – ci-après "MPR" – *et quelques autres méthodes d'enquête* a quant à elle attribué des pouvoirs très étendus aux services de police et de renseignement belges.[84] Cette loi est destinée à être appliquée dans les cas où les autres possibilités d'information, par essence moins préjudiciables aux droits de l'homme, ne sont plus suffisantes. Certaines de ces MPR, telles que l'observation, l'infiltration ou le recours aux indicateurs, sont réputées être très dangereuses pour le respect de la vie privée, même si elles ne sont supposées fonctionner que dans un cadre judiciaire et jamais purement exploratoire.[85] La Cour constitutionnelle n'a annulé qu'une partie infime de ces dispositions.

Enfin, en 2015, suite aux attaques perpétrées notamment en France et en Belgique, presqu'une vingtaine de mesures gouvernementales furent adoptées dans le contexte de la lutte antiterroriste. Parmi elles, nous recensons le durcissement de la circulaire *Foreign Fighters*, une multiplication des cas d'application des MPR, le déploiement du champ d'application des perquisitions, le remaniement des organisations de renseignement et de sécurité, la création du *Passenger Name Record*, la libération de fonds supplémentaires accordés à la sécurité, etc.[86] Ces dispositions ont été critiquées, dans leur grande majorité, par la Ligue des Droits de l'Homme.[87]

Section 2. Importance d'une protection législative adéquate et actualisée

§1. Contexte et enjeux

A l'époque des cyber-attaques, des révélations de Snowden, de la menace terroriste et de la collecte et le traitement illégal des données personnelles – qui vient d'ailleurs sérieusement ébranler la confiance en l'internet –, les défis législatifs sont à leur comble.[88] Certains en viennent d'ailleurs à se demander si la bataille de la protection des données vaut toujours la peine d'être menée, dès lors que le réseau internet lui-même serait trompeur. Mais à l'ère du numérique, les enjeux sont pourtant nombreux, primordiaux et variés, qu'ils soient

[83] Loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, *M.B.*, 12 mai 2003, p. 25351.
[84] Proposition de résolution n° 1624/001 précitée, développements, p. 5.
[85] COMMISSION DE LA PROTECTION DE LA VIE PRIVEE, *Avis n° 05/2015 sur le projet de loi visant à renforcer la lutte contre le terrorisme*, 25 février 2015, www.privacycommission.be (consulté le 5 juillet 2018) ; J.-L. TRULLEMANS, *Les actes de recherche de la preuve et les autres modes de preuve – Mise en oeuvre des méthodes particulières de recherche et de quelques autres méthodes d'enquête au sens de la loi du 6 janvier 2003*, Postal Mémorialis, Waterloo, Kluwer, 2004, p. 140.
[86] B. BOUCHAT, *Les mesures de lutte antiterroriste : une menace pour notre droit fondamental à au respect de la vie privée ?*, Université Catholique de Louvain, 2016-2017 (promoteur : M. VERDUSSEN), p. 24.
[87] LIGUE DES DROITS DE L'HOMME, *Rapport 2015-2016*, 2016, p. 45, www.liguedh.be (consulté le 5 juillet 2018).
[88] C. CASTETS-RENARD, *op. cit.*, p. 34.

géopolitiques[89], économiques, ou plutôt sociaux et fondamentaux.[90] Une législation efficace et pertinente de protection des données personnelles permettrait de les balancer avec génie. Pour ce faire, un « processus de modernisation, d'adaptation et d'enrichissement des dispositions nées dans un monde non encore hyper-connecté » est nécessaire.[91]

Un premier terrain d'interventions concerne l'économie numérique. Comme nous l'indique le Professeur Castets-Renard, l'Union européenne se doit de trouver « un juste équilibre entre l'émergence d'un marché des données personnelles créé par les géants de l'internet en grande majorité américain et la reconnaissance dans l'Union européenne d'un droit fondamental à la protection des données ».[92] A ce propos, le principe de la libre circulation des données personnelles en vue de renforcer le marché intérieur, consacré par la directive 95/46/CE, n'est pas remis en cause dans le nouveau règlement 2016/679. En effet, confrontés aujourd'hui à un véritable marché de données personnelles, nous ne pouvons ignorer la compétition présente dans ce secteur mondial, ni la valeur et le potentiel de ces données dématérialisées.[93] Dans le cas contraire d'une législation *trop* protectrice des données personnelles, des conséquences variables pour l'économie européenne toute entière seraient susceptibles d'apparaître. En effet, d'un côté, nous pourrions être confrontés à un *forum shopping*[94] – déplacement vers un autre pays européen, voire vers un autre continent où la protection serait moins stricte – opéré par les entreprises, toujours en quête du sol le plus hospitalier. Mais d'un autre côté, la déontologie et l'éthique de nos réglementations européennes pourraient être vendues au public comme respectueuses des libertés fondamentales des citoyens, valeurs de plus en plus au centre des préoccupations. Ainsi, l'avenir nous éclairera sur la question de savoir si l'équilibre espéré par la réforme législative européenne sera apte à défendre nos droits fondamentaux ou favorisera coûte que coûte les opportunités économiques du marché numérique.[95]

---

[89] Pour une réflexion plus globale sur les enjeux géopolitiques de l'internet, voir : D. FAYON, *Géopolitique d'internet qui gouverne le monde ?*, Paris, Economica, 2013.
[90] C. CASTETS-RENARD, *op. cit.*, p. 25.
[91] C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », in *Quelles protections des données personnelles en Europe?*, *op. cit.*, p. 81.
[92] C. CASTETS-RENARD, *op. cit.*, p. 26.
[93] F. ROCHELANDET, *Économie des données personnelles et de la vie privée*, coll. Repères, Paris, La Découverte, 2010 , cité par C. CASTETS-RENARD, *ibidem*, p. 28.
[94] C. CASTETS-RENARD, *ibidem*, p. 29.
[95] Y. BENKLER, *The wealth of Networks : how social production transforms markets and freedom*, Yale, University Press, 2006.

Un deuxième domaine nous intéresse davantage : celui de l'équilibre à réaliser entre les libertés fondamentales et la sécurité nationale. En ce sens, le Parlement européen et le Conseil ont adopté le 27 avril 2016 la directive 2016/680[96] abrogeant la précédente décision-cadre 2008/977/JAI du Conseil. Ce texte, davantage contraignant en matière pénale, marque la détermination du législateur européen à « ne pas accorder aux individus le même niveau de protection en matière pénale que dans les autres matières ».[97] Donnant un nouveau souffle à la protection des données à caractère personnel applicables à la coopération judiciaire en matière pénale et à la coopération policière et au traitement, tant transfrontière que national, des données à caractère personnel, cette disposition s'inscrit dans le contexte de l'Espace de liberté sécurité et justice (ELSJ)[98]. Les garanties accordés aux individus en matière de collecte et conservation des données personnelles y sont amoindries face à la mission de l'Etat qui est de maintenir l'ordre public et assurer la sécurité générale – « l'intérêt général primant l'intérêt individuel ».[99]

Certes les plus pessimistes diront que toutes ces normes sont finalement insignifiantes face aux fonds impénétrables du réseau internet et la complexification de l'informatique ; que la récupération et le stockage des données se feront quoi qu'il arrive et sans que la population ne s'en rende compte ; qu'il n'y a déjà plus de vie privée, comme l'a par exemple affirmé Marc Zuckerberg sur son compte Twitter – PDG du réseau social Facebook. C'est dire l'ampleur des défis factuels que doit relever le nouveau règlement général sur les données personnelles, dont il sera question à la section suivante.

§2. Vigoureuse réaction européenne : Résolution de 2014 et actualité

Le Parlement européen, soucieux de l'intérêt de ses citoyens et méfiant envers les Etats-Unis dans ce contexte d'hyper-surveillance constante, a adopté le 12 mars 2014 une Résolution[100] sur les organismes de surveillance américains élaborant toute une série de mesures renforçant le droit

---

[96] Dir. (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L.119/89, du 4 mai 2016.

[97] C. CASTETS-RENARD, *op. cit.*, p. 30.

[98] envisagé pour la première fois dans le Traité d'Amsterdam, entré en vigueur en 1999.

[99] C. CASTETS-RENARD, *op. cit.*, p. 31.

[100] PARLEMENT EUROPEEN, *Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*, Résolution 2013/2188 (INI), 12 mars 2014, www.europarl.europa.eu. (consulté le 10 juillet 2018).

fondamental à la vie privée. Dans cellle-ci, le Parlement européen avait premièrement demandé la suspension des accords UE-USA, faute de plein respect, par les Etats-Unis, des droits fondamentaux reconnus par l'Union. Citons par exemple un usage rapporté illicite de l'accord SWIFT de 2010[101] autorisant le gouvernement américain à entrer en possession des données bancaires européennes dans le but de déjouer le terrorisme, sous certaines conditions et dans le respect *supposé* du droit à la vie privée des citoyens. Deuxièmement, cette Résolution sollicitait la « suspension immédiate » des postulats de la « sphère de sécurité » - appelée notamment *Safe Harbor* – à propos des transferts transatlantiques des données personnelles européennes.[102] Cette dernière a finalement été anéantie par la Cour de justice en octobre 2015 (cf. *infra*), laissant place à un vide juridique. Troisièmement, soulignons que les négociations quant à un partenariat transatlantique de commerce et d'investissement (TTIP) ont été suspendues, entre autres grâce au Parlement européen – devant donner son feu vert, avec le Conseil, à un texte négocié par la Commission au nom de l'Union – insistant sur le fait que la lutte contre le terrorisme ne pourra jamais légitimer une surveillance de masse secrète et illégale.[103]

N'étant qu'un acte non-législatif, cette Résolution exprima néanmoins clairement la tendance suggérée par le Parlement – suivie par une très large majorité (544 voix sur 682) – en faveur d'un maintien strict, voire une protection accentuée des droits fondamentaux des citoyens.

En juin 2018, la commission des libertés au Parlement européen (Libe) a demandé la suspension pure et simple du *Privacy Shield* – entente trouvée entre la Commission européenne et les Etats-Unis visant à pallier à l'invalidation de l'accord *Safe Harbor* précédent et à permettre la poursuite de ces transferts – en ce qu'il existerait un manque de contrôle de la part de la Commission européenne vis-à-vis de cet espace peu sécurisé.[104] En effet, les exceptions reprises dans cet accord sont libellées de façon tellement large qu'elles permettraient de contourner sa propre interdiction de récolte généralisée de données.[105] Ainsi, malgré le travail qui justifie cet accord, celui-ci risquerait de ne pas rencontrer les critiques avancées par la CJUE, et de nous ramener au faible niveau de protection antérieur.[106]

---

[101] L'accord EU-US *Terrorist Finance Tracking Programme* (TFTP) autorise un programme de surveillance gouvernemental américain à accéder aux transactions financières internationales sur le réseau 'SWIFT'.

[102] C. CASTETS-RENARD, *op. cit.*, p. 32.

[103] PARLEMENT EUROPEEN, *Communication de presse – NSA : mettre fin à la surveillance massive ou faire face aux conséquences*, http://www.europarl.europa.eu, 12 mars 2014 (consulté le 10 juillet 2018).

[104] M. REES, *Au Parlement européen, la commission Libe demande la suspension du Privacy Shield*, www.nextinpact.com, 12 juin 2018.

[105] Les interdictions de cet accord permettent une interprétation étendue de concepts tels que « lutte contre le terrorisme » et, partant, de son champ d'application. M. BERNAERTS, « Les transferts de données à caractère personnel entre l'Union européenne et les États-Unis : une valse à mille temps ? », in *R.D.C.,* 2017, pp. 178-179.

[106] PARLEMENT EUROPÉEN, *EU-US 'Privacy Shield' for data transfers: further improvements needed, MEPs*

Section 3. Derniers changements législatifs

§1. Evolution internationale capitale : Protocole d'amendement à la Convention n° 108

Attentif à une protection internationale poussée des données à caractère personnel, le Conseil de l'Europe a adopté, le 18 mai dernier, un Protocole d'amendement (STCE n° 223)[107] qui actualise sa Convention relative à la protection des données, dite « Convention n° 108 » (voir *supra*).[108] Face aux défis technologiques du 21ème siècle – explosion des méthodes de géolocalisation, de vidéosurveillance, le recours en hausse aux identifiants biométriques... – , le Comité conventionnel de la Convention n° 108 a lancé en 2010 une étude[109] recensant les déficiences de la Convention, suivie d'une consultation publique[110] en 2011, afin d'élaborer les pistes d'amélioration les plus adaptées possibles.[111]

La révision parallèle de la directive 95/46 et des Lignes directrices de l'OCDE de 1980, même si celles-ci ne sont pas vouées à un développement analogue, a exercé une influence extérieure importante, en ce qu'une cohérence absolue est nécessaire, « sous peine de voir les États membres de l'UE et signataires de la Convention n° 108 tiraillés entre des engagements contradictoires ».[112]

La modernisation ayant ainsi été actée, celle-ci n'a pas mis à mal les principes clés que la Convention a maintenu pendant presque quarante ans. Ces principes d'origine[113], incarnant neutralité technologique et continuité législative, ont été réaffirmés, renforcés, voire même réadaptés à l'ère numérique.[114] Par ailleurs, de nouveaux principes ont été reconnus, tels que « les principes de transparence, de proportionnalité, de responsabilité, de limitation des données, de respect de la vie privée pris en compte dès la conception etc ».[115]

---

say, UE, Communiqué de presse*,* Bruxelles, 26 mai 2016.

[107] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signé à Elseneur (Danemark) le 18 mai 2018.

[108] CONSEIL DE L'EUROPE, *Communiqué de presse – Améliorer la protection des données au niveau mondial: le Conseil de l'Europe met à jour sa convention phare*, Elseneur (Danemark), 18 mai 2018, www.rm.coe.int/ (consulté le 12 juillet 2018).

[109] C. DE TERWANGNE et J.-Ph. MOINY, « Les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) face aux développements technologiques », in *Rapport pour le Conseil de l'Europe*, Strasbourg, novembre 2010.

[110] C. DE TERWANGNE et J.-Ph. MOINY, *Rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Conseil de l'Europe, Strasbourg, juin 2011.

[111] C. DE TERWANGNE, « La réforme de la Convention 108… », *op. cit.*, p. 82.

[112] C. DE TERWANGNE, « La réforme de la Convention 108… », *ibidem*, p. 83.

[113] Il s'agit par exemple du principe de loyauté, du principe de finalité ou encore des exigences liées à la qualité des données. Voir C. DE TERWANGNE, « La réforme de la Convention 108… », *ibidem*, pp. 92 à 95.

[114] CONSEIL DE L'EUROPE, *Rapport explicatif*, Strasbourg, 10.X.2018 ; C. DE TERWANGNE, *ibidem*, p. 84.

[115] CONSEIL DE L'EUROPE, *La Convention 108 modernisée : aperçu des nouveautés*, mai 2018, www. rm.coe.int/ (consulté le 2 juillet 2018).

§2. Evolution européenne dominante : le règlement 2016/679 (RGPD)

Le 25 mai dernier, un nouveau règlement est entré en vigueur : il s'agit du règlement général sur la protection des données personnelles (ci-après « RGPD »)[116]. La révision de la directive de 1995 qui en découle représente un enjeu politique et sécuritaire majeur pour l'Europe toute entière. Dans les paragraphes suivants, nous allons tenter d'analyser dans quelle mesure le RGPD intègre un meilleur degré d'harmonisation ainsi que l'avènement du numérique.[117]

Tout d'abord, pourquoi avoir troqué la forme d'une directive pour celle d'un règlement ? Le choix de l'instrument légal opéré par la Commission en 2012 a été félicité par François Biltgen – ministre de la Justice à l'époque – en ce qu'un règlement uniforme permettra selon lui « l'établissement d'un marché numérique unique ».[118] Notons que dans cette section, nous nous limiterons tout d'abord à étudier les changements clés vis-à-vis des citoyens, même si ce règlement comporte de nombreux changements pour les entreprises, sous-traitants et professionnels. Ensuite, nous nous concentrerons sur les évolutions les plus marquantes qui, notons-le, viennent souvent confirmer les interprétations de la directive défendues par les Commissions nationales et le Groupe 'Article 29' – organe consultatif européen indépendant sur le thème de la protection des données personnelles et de la vie privée.

Premièrement, l'art. 5 du règlement concernant les principes relatifs au traitement des données à caractère personnel s'est enrichi comparé à son prédécesseur (art. 6 dir. 95/46). Tout d'abord, il ajoute, dans les conditions cumulatives nécessaires au traitement des données personnelles, un principe de transparence aux principes de licéité et loyauté. Ceci permettra, théoriquement, un meilleur contrôle pour les citoyens.[119] Deuxièmement, le principe de responsabilité est renforcé[120] en ce qu'il fait peser la charge de la preuve sur le collecteur de données du respect

[116] 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 Dir. 95/46/CE, *J.O.U.E.*, L. 119/1, du 4 mai 2016.

[117] C. CASTETS-RENARD, *op. cit.*, p. 24.

[118] EUROPAFORUM LUXEMBOURG, *Conseil JAI - Le ministre François Biltgen a salué la proposition de la Commission de procéder par voie de règlement uniforme en matière de protection des données*, 26 octobre 2012, http://www.europaforum.public.lu/ (consulté le 5 juillet 2018).

[119] Règlement 2016/679, art. 5, §1, a) ; « La transparence implique que toute information adressée au public ou à la personne concernée doit être aisément accessible et facile à comprendre, et être formulée en termes simples et clairs, particulièrement en ce qui concerne les informations relatives à l'identité du responsable et aux finalités du traitement » (voir le considérant 39.). Les obligations d'information à charge du responsable du traitement résultant du principe de transparence sont détaillées aux articles 12 et s. du Règlement.

[120] Règlement 2016/679, art. 5, §2 ; « Son respect implique que le responsable mette en place des mécanismes et des systèmes de contrôle (mesures d'audit, politique interne…) au sein de son entité pour garantir la conformité du traitement pendant toute sa durée et pour en conserver la preuve. Cette obligation de rendre compte est davantage

des principes de base et, ensemble avec le principe de transparence, pourraient impliquer « une révision des processus de traitement actuel dans l'organisation du responsable du traitement ».[121] Enfin, ce règlement introduit le principe de minimisation des données[122], véritable « invitation explicite à la modération ».[123] Au sujet de l'importance de la *qualité* des données, la directive avait déjà établi une limitation à la collecte étant « adéquation et pertinence », mais cet ajout constitue en vérité une application du principe de proportionnalité.

Ensuite, le règlement renforce l'obligation d'information *lorsque les données n'ont pas été collectées auprès de la personne concernée*[124] – ce qui peut par exemple être le cas lors d'une collecte automatisée des données telle que le profilage. Un devoir d'information inconditionné concernera ainsi le fondement juridique du traitement, ses finalités ou intérêts légitimes sur lesquels se repose le collecteur des données, la logique sous-jacente et les conséquences pour la personne.[125] De plus, l'intention de transférer les données vers un pays étranger ou une organisation internationale devra faire l'objet d'une information expresse et obligatoire.[126] Mais de l'autre côté, le législateur multiplie les exceptions à cette obligation d'information.[127] La plus marquante concerne la levée du devoir d'information, dans le cas où :

« *La fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* (…) *ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. »*[128]

Néanmoins, le législateur a tenté de nous apaiser en insérant la finale suivante :

« En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles. »[129]

---

explicitée par l'article 24 du Règlement. », selon CABINET ULYS, *GDPR – Article 5 : Principes relatifs au traitement des données à caractère personnel*, www.gdpr-expert.eu (consulté le 2 juillet 2018).

[121] CABINET ULYS, *ibidem*.

[122] Principe relatif au traitement des données à caractère personnel selon lequel celles-ci doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées », voir Règlement 2016/679, art. 5, §1, c).

[123] C. DE TERWANGNE, « La réforme de la Convention 108… », *op. cit.*, p. 94.

[124] Règlement 2016/679, art. 14.

[125] CABINET ULYS, *GDPR – Article 14 : Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée*, *op. cit.*

[126] CABINET ULYS, *ibidem.*

[127] Règlement 2016/679, art. 14, §5.

[128] Règlement 2016/679, art. 14, §5, b).

[129] Règlement 2016/679, art. 14, §5, b), *in fine*.

Il est tout de même raisonnable de se demander si un tel élargissement des exceptions générales à ce devoir d'information est respectable, en ce qu'une interprétation large de ces concepts flous et imprécis pourrait mener à une opacité contre-productive face aux aspirations réaffirmées de transparence et de protection renforcée des droits et libertés.

En outre, dans le but de surmonter l'improductivité administrative et financière découlant de l'ancienne obligation de notification préalable prévue par la directive, le règlement a préféré la remplacer par un double mécanisme : la création d'un registre des activités de traitement (art. 30) et la nouvelle obligation de mener une analyse d'impact relative à la protection des données (art. 35). Ces deux dispositifs incarnent le passage d'obligations *générales* à des obligations *ciblées* directement sur les traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées et ainsi espérer stimuler l'efficacité de ces mécanismes de protection.[130] Concernant le registre, il est désormais obligatoire pour les responsables du traitement et les sous-traitants de garder une trace documentaire des pratiques de traitement qui leur sont imputables.[131] Au sujet de l'analyse d'impact, celle-ci est obligatoire lorsqu'un traitement présente de sérieux dangers pour les droits et libertés des individus.[132] L'étude portera surtout sur « l'origine, la nature, la portée, le contexte, la particularité et la gravité de ce risque ».[133] Malgré le fait que la version finale du règlement ait supprimé l'énumération non exhaustive des risques justifiant une analyse d'impact, le considérant n° 91 nous rassure en indiquant qu'une telle analyse est applicable :

« en particulier aux opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, par exemple, en raison de leur caractère sensible, lorsque, en conformité avec l'état des connaissances technologiques, une nouvelle technique est appliquée à grande échelle, ainsi qu'à d'autres opérations de traitement qui engendrent un risque élevé pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces personnes d'exercer leurs droits (...) ».[134]

Ce cas de figure est en effet tout à fait assimilable au phénomène de la surveillance de masse, et nous raccroche aisément aux grands déploiements de *Big Data* réalisés via les réseaux sociaux.
Par ailleurs, l'on est septique face à l'expansion des dérogations à l'interdiction de transfert vers un pays tiers ou une organisation internationale dans les cas où il n'existe pas de décision

[130] CABINET ULYS, *GDPR – Article 30 et Article 35*, *op. cit*.
[131] Règlement 2016/679, art. 30, §1.
[132] Règlement 2016/679, art. 35, §1.
[133] CABINET ULYS, *GDPR – Article 35 : Analyse d'impact relative à la protection des données, op. cit.*
[134] Règlement 2016/679, considérant n° 91.

d'adéquation[135] ou de garantie appropriée[136]. En effet, reprenant les exceptions classiques, le règlement offre une dernière possibilité, certes limitée, pour faciliter l'admission de transferts exceptionnels ne présentant pas le niveau de protection adéquat :

« *Lorsque aucune des dérogations pour des situations particulières prévues aux points a) à g) du présent paragraphe n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel* ».[137]

Il s'agira d'être attentifs aux utilisations et interprétations faites au cas par cas du concept « intérêts légitimes impérieux », qui ne fait l'objet d'aucune liste, qu'elle soit exemplative ou exhaustive.

Enfin, une critique vive plus générale s'adresse à une lacune par rapport à la *supposée* unification des règles nationales au niveau européen – vertu présumée du règlement. En effet, malgré le fait que les Etats désirent conserver une part de leur souveraineté, le fait que le règlement leur laisse la possibilité d' « adapter les règles applicables aux traitements imposés par une loi nationale »[138] et ainsi le pouvoir de toujours rajouter diverses sortes de traitements sur une base spécifique et nationale pourrait s'avérer incontrôlable à l'avenir. Dans le même sens, la liberté laissée aux Etats d'introduire des limitations à l'interdiction du traitement des données sensibles concernant les données génétiques, biométriques ou celles concernant la santé, crée un risque majeur qui viendrait ruiner l'harmonisation des différentes finalités ou types de données, et la protection des données personnelles en général.[139]

---

[135] C'est-à-dire lorsque nous ne sommes pas dans le cas de figure où « la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection *adéquat* », voir art. 45, §§1 et 3 dudit règlement.

[136] C'est-à-dire lorsque nous ne sommes pas dans le cas de figure où « en l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives », voir art. 46 dudit règlement.

[137] Règlement 2016/679, art. 49, §1, al. 2.

[138] CABINET ULYS, *GDPR – Article 6 : Licéité du traitement*, *op. cit.*

[139] CABINET ULYS, *GDPR – Article 9 : Traitement portant sur des catégories particulières de données à caractère personnel*, *ibidem.*

§3. Evolutions nationales : aperçu comparé des législations nationales en Europe

Avant de clôturer ce chapitre, nous aimerions souligner que les Etats-Unis n'ont pas le monopole de cette tendance au durcissement des lois antiterroristes. En effet, toutes ces dispositions ont pour dénominateur commun de restreindre l'exercice des droits et libertés fondamentaux et, partant, les garanties essentielles à la protection des citoyens contre les dérives, les discriminations et l'arbitraire.[140]

En droit belge, depuis 2016, nous avons vu l'adoption de dispositions inquiétantes autorisant par exemple les perquisitions de nuit en cas de soupçon de terrorisme[141], l'ouverture de banques de données personnelles[142], la légitimation de la multiplication des arrestations et des contrôles de sécurité, la conservation de toutes les métadonnées électroniques par les opérateurs de télécommunication pour un potentiel usage policier ou judiciaire postérieur[143], et « l'intensification de ces mesures coïncidant parfois avec une augmentation de pratiques policières abusives ».[144]

En France, une loi légalisant la surveillance de masse, notamment en dehors de ses propres frontières, a été adoptée en 2015 – qui plus est en limitant au maximum les réactions et le débat citoyen.[145] Le Conseil constitutionnel français a d'ailleurs avalisé la majorité de ses dispositions, malgré les critiques vives[146] de la CNIL[147], des députés et autres ONGs et organisations. En 2016, le pays adopta deux lois[148] présentant plusieurs vices : accentuation des pouvoirs des

[140] C. MACQ et S. VAN OUTRYVE, *op. cit.*, p. 32.

[141] Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme, *M.B.*, 9 mai 2016, p. 30567.

[142] Loi du 27 avril 2016, *ibidem*.

[143] Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016, p. 44717.

[144] C. MACQ et S. VAN OUTRYVE, *op. cit.*, p. 32.

[145] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *J.O.R.F.*, 26 juillet 2015, n° 0171.

[146] La loi développant des moyens techniques faramineux de collectes massives de données des agences de renseignement et sur la mise en circuit de « boîtes noires » chez les fournisseurs d'accès à Internet pour déceler automatiquement des activités « typiques » des terroristes par un traitement des métadonnées de toutes les communications de l'entièreté de la population, voir AMNESTY INTERNATIONAL, « France. Des vies bouleversées. L'impact disproportionné de l'état d'urgence en France », in *Rapport 2016*, Londres, 4 février 2016, pp. 33 et 34 et M. TUAL, « L'essentiel de la loi sur le renseignement jugé conforme à la Constitution », in *Le Monde,* 23 juillet 2015, http://www.lemonde.fr/ (consulté le 3 juillet 2018).

[147] Commission Nationale Informatique et Libertés

[148] Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, *J.O.R.F.*, 4 juin 2016, n° 0129 et Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste, *J.O.R.F.*, 22 juillet 2016, n° 0169.

forces de police en les autorisant à conduire des fouilles et contrôles d'identité, concession aux services de renseignement du pouvoir de conduire, sans aval judiciaire préalable, des analyses instantanées concernant les données personnelles de tout individu « susceptible d'être en lien avec une personne susceptible de constituer une menace »[149], tolérance vis-à-vis des perquisitions de nuit et possibilité de saisie de données personnelles lors de celles-ci, etc.

Cela se répète également au Royaume-Uni, où la consécration du *Investigatory Powers Act* de 2016 pourrait bien voir apparaître le mécanisme de surveillance le plus drastique et intrusif de l'Union européenne. Selon Joseph Cannataci – rapporteur spécial aux Nations Unies pour la défense de la vie privée et Professeur de droit maltais –, cette loi serait pire que ce que Georges Orwell avait imaginé dans *1984*.[150] En effet, il permet un accès exorbitant aux données personnelles, sans nécessiter aucune trace de risque terroriste quelconque en contrepartie, et sans autorité indépendante de contrôle le supervisant.[151]

L'Allemagne, « démocratie libérale stable et progressiste »[152] par excellence, a quant à elle adopté une loi en 2016 qui accroît disproportionnellement les pouvoirs de surveillance de l'Office fédéral de renseignements.[153]

L'on comprend mieux à présent pourquoi la Résolution de 2014 précitée du Parlement européen a demandé à 14 Etats membres – dont le Royaume-Uni, la France, l'Allemagne, la Suède, les Pays-Bas et la Pologne – de revoir leur législation.[154] Il faut croire que la demande de clarification sur les dérives d'une surveillance de masse n'ait pas encore permis de rencontrer un équilibre raisonnable entre le droit fondamental de vivre en sécurité et le respect de l'ensemble des droits et libertés fondamentaux.[155]

---

[149] AMNESTY INTERNATIONAL, « France. Des vies bouleversées (…) », *op. cit.*

[150] A. DOLHEIN, *Le premier rapporteur pour la défense de la vie privée de l'ONU, Joseph Cannataci, juge la surveillance au Royaume-Uni "pire" que dans "1984"*, 26 août 2015, http://reinformation.tv/ (consulté le 12 juillet 2018).

[151] A. TRAVIS, « Investogatory powers bill: the key points », in *The Guardian,* 4 novembre 2015, https://www.theguardian.com/ (22 juillet 2017).

[152] AMNESTY INTERNATIONAL, « Des mesures disproportionnées – L'ampleur grandissante des politiques sécuritaires dans les pays de l'UE est dangereuse », in *Rapport 2017*, Londres, 2017, p. 34.

[153] AMNESTY INTERNATIONAL, *ibidem*.

[154] Résolution (UE) du Parlement européen du 12 mars 2014, *op. cit.* ; C. CASTETS-RENARD, *op. cit.*, p. 33.

[155] C. MACQ et S. VAN OUTRYVE, *op. cit.*, p. 32.

CHAPITRE 3. Avancées jurisprudentielles

L'actualité juridique de la protection des données personnelles en Europe se caractérise certes par la succession de ses réformes législatives, mais aussi au travers de son activité judiciaire importante : différents arrêts de principe et revirements de jurisprudence, tant de la Cour de justice de l'Union européenne que de la Cour européenne des droits de l'homme, exercent une importante influence morale et méritent toute notre attention.

Section 1. Cour de justice de l'Union européenne

La question de la récolte et de l'utilisation des données personnelles est au centre de l'attention, surtout pour la Cour de justice de l'Union européenne qui a rendu plusieurs arrêts majeurs en la matière.[156] Ces arrêts montrent l'intérêt de la Cour pour le respect des droits fondamentaux, en invalidant notamment la directive 2006/24/CE sur la conservation des données dans son intégralité[157], les principes du « *Safe Harbor* »[158] et toute conservation *non ciblée* de données personnelles[159]. Les affaires emblématiques sélectionnées ci-dessous font acte et amplifient ce combat pour une meilleure protection du droit fondamental au respect de la vie privée.

§1. L'affaire Digital Rights Ireland (arrêt du 8 avril 2014)

Deux arrêts rendus en 2014[160], l'un concernant la Hongrie et l'autre l'Irlande, ont clairement prohibé la surveillance de masse en se basant sur une violation des dispositions de la Charte des Droits Fondamentaux de l'Union européenne – Charte à laquelle il est ainsi reconnu toute sa puissance et sa portée. L'un des arrêts, à savoir *Digital Rights Ireland*, prohibe radicalement toute surveillance de masse en invalidant intégralement la directive 2006/24/CE sur la conservation des données à caractère personnel, bâtie sous impulsion anglaise dans le contexte émotionnel des attentas de Londres de juillet 2005.[161]

---

156 C. CASTETS-RENARD, *op. cit.*, pp. 23 et 24.

157 CJUE, Grande Chambre, 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, affaires jointes C-293/12 et C-594/12 ; Dir. (CE) n° 2006/24 du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de service de communications électroniques accessibles au public ou de réseaux publics de communication et modifiant la dir. (CE) n° 2002/58, *J.O.C.E.*, L.105/54, du 13 avril 2006 (invalidée).

158 CJUE, *Maximilian Schrems c. Data Protection Commissioner, op. cit.*

159 CJUE, 21 décembre 2016, *Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a*, affaire C-203/15.

160 CJUE, 8 avril 2014, *Commission/Hongrie*, affaire C-288/12, §47. V. et CJUE, *Digital Rights Ireland*, *op. cit.*

161 M.-L. BASILIEN-GAINCHE, « Une prohibition européenne claire de la surveillance électronique de masse », in *La Revue des droits de l'homme*, Actualités Droits-Libertés, 14 mai 2014, pp. 1 à 4 ; F. BENOIT-ROHMER, « Protection des données personnelles », note sous CJUE, arrêt Digital Rights Ireland, in *RTDE*, 2015, p.168.

La question préjudicielle a été posée à la CJUE par la High Court irlandaise à la suite du recours introduit par la société *Digital Rights Ireland Ltd* questionnant la légalité de mesures législatives et administratives nationales transposant la directive 2006/24 relative à la conservation de données relatives aux communications électroniques face à la Charte.[162]

L'arrêt est déterminant pour trois raisons principales. Premièrement, en désaccord avec son arrêt datant du 10 février 2009[163], la Cour semble enfin « prendre ses responsabilités »[164] en rendant une décision sur le sujet sensible de la conservation des données de communications électroniques allant dans le sens de la protection des droits fondamentaux.[165] Par cette invalidation, la Cour s'inscrit d'ailleurs dans une continuité établie au centre des dispositifs – affirmant l'inconstitutionnalité des mesures nationales de transposition de la directive 2006/24/CE – rendus par les cours suprêmes nationales des Etats membres de l'UE.[166] Deuxièmement, la Cour prononce sans embarras la violation des articles 7 et 8 de la Charte :

> « *L'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère [...] d'une vaste ampleur [...]* et *doit être considérée comme particulièrement grave* » ; « *la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante* ».[167]

Ainsi, elle renforce respectivement la protection de la vie privée – « *affectée de manière directe et spécifique* »[168] en ce que « *l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental* »[169] – et la protection des données à caractère personnel – qui « *revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci* »[170]. De plus, concernant la discussion portant sur

---

[162] M.-L. BASILIEN-GAINCHE, *ibidem*, p. 3.

[163] CJUE, 10 février 2009, *Irlande contre Parlement européen et Conseil de l'Union européenne*, affaire C-301/06.

[164] LABAYLE (H.), « La Cour de justice et la protection des données : quand le juge européen des droits fondamentaux prend ses responsabilités », note sous CJUE, arrêt Digital Rights Ireland, in *RTDE*, 2015, cité par M.-L. BASILIEN-GAINCHE, *op. cit.*, pp. 2 et 3.

[165] « Le juge de Luxembourg mène en effet un examen tranchant et donne une conclusion cinglante : « *cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* ». » (point 65), cité par M.-L. BASILIEN-GAINCHE, *ibidem*, pp. 3 et 4. L'on y retrouve d'ailleurs le principe de minimisation des données.

[166] A ce sujet, voir C. JONES et B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, Secile, 2014, cité par M.-L. BASILIEN-GAINCHE, *ibidem*, p. 5.

[167] CJUE, *Digital Rights Ireland*, *op. cit.*, §37.

[168] CJUE, *Digital Rights Ireland*, *ibidem*, §29.

[169] CJUE, *Digital Rights Ireland*, *ibidem*, §35.

[170] CJUE, *Digital Rights Ireland*, *ibidem*, §53 ; Même si, selon des auteurs tels que Steve Peers, « la CJUE semble ne avoir oser s'aventurer sur le terrain difficile de la *différenciation* entre respect de la vie privée et protection des

l'objectif d'intérêt général poursuivi, la Cour reconnaît l'importance de la lutte contre le terrorisme et la garantie de la sécurité publique, tout en rappelant aux institutions européennes et Etats membres « *les limites posées à leur pouvoir de légiférer* » et les mettant en garde contre des « *atteintes inutiles et inadéquates, inappropriées et injustifiées aux droits fondamentaux des citoyens européens* »[171]. Enfin, bien que le juge n'approfondisse pas la prétendue utilité – et donc la nécessité – de l'outil que constitue la conservation des données[172], il est intransigeant concernant le critère de la proportionnalité des mesures adoptées face à l'objectif poursuivi. En effet, sur ce dernier point, la Cour reproche au texte de la directive d'autoriser une ingérence démesurée – en ce qu'elle touche « *de manière globale l'ensemble des personnes faisant usage de services de communications électroniques* », soit « *la quasi-totalité de la population européenne* »[173] –, sans établir aucune limitation à l'accès aux données conservées ni aucun contrôle préalable, tout en ne prévoyant aucun cadre pour la conservation de ces données.[174] Troisièmement, la Cour fournit une aide précieuse aux institutions européennes au moyen de nombreuses indications détaillées et explicites, comme par exemple la transition vers une conservation des données *ciblée* et plus *globale*, « *des conditions matérielles et procédurales d'accès des autorités aux données* »[175], ou encore des exigences pour « *une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données* »[176]. Pour conclure, notons que le rôle de la Cour n'est pas seulement d'épauler la rédaction d'une nouvelle directive, mais aussi d'assister la (re)construction d'une « approche globale du traitement informatisé des données à caractère personnel à l'échelle de l'Union »[177] ; mission que nous développerons davantage dans notre Titre II[178].

---

données personnelles que certains auteurs de doctrine estiment pourtant fondamentale », voir S. PEERS, « Data retention: a landmark court of justice's ruling. Will this saga continue and how ? », note sous CJUE, arrêt Digital Rights Ireland, X, 2014., cité par M.-L. BASILIEN-GAINCHE, *op. cit.*, p. 7.

171 « *Un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la Dir. 2006/24 soit considérée comme nécessaire aux fins de ladite lutte* », CJUE, *Digital Rights Ireland*, *ibidem*, §51, cité par M.-L. BASILIEN-GAINCHE, *ibidem*, p. 8.

172 CJUE, *Digital Rights Ireland*, *ibidem*, §49 et s.

173 CJUE, *Digital Rights Ireland*, *ibidem*, §§ 56 à 58.

174 M.-L. BASILIEN-GAINCHE, *op. cit.*, pp. 9 et 10.

175 CJUE, *Digital Rights Ireland*, *op. cit.*, § 61.

176 CJUE, *Digital Rights Ireland*, *ibidem*, §66.

177 M.-L. BASILIEN-GAINCHE, *op. cit.*, p. 13.

178 En effet, « la référence faite par le juge de Luxembourg à la conservation des données de communications électroniques en dehors du territoire de l'Union (§ 68) est une allusion à peine dissimulée à la problématique pour le moins sensible des transferts de données entre l'UE et les USA », voir S. CLAVET, « Les conséquences de l'accord Passenger Name Record sur la protection des droits fondamentaux en Europe », in *Droits Fondamentaux*, n°8, janvier 2010 et S. PEYROU, « De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », in *R.A.E.*, 2013, cités par M.-L. BASILIEN-GAINCHE, *ibidem*, p. 14.

§2. L'affaire Schrems (arrêt du 6 octobre 2015)

Un an et demi après l'arrêt *Digital Rights Ireland*, la Cour renforce ses positions[179] d'une manière cohérente dans l'affaire *Maximillian Schrems c. Data Protection Commissioner*[180] en s'attaquant cette fois à la question de la légalité du transfert vers les Etats-Unis – suite à la reconnaissance par la décision de la Commission européenne d'un « niveau adéquat de protection »[181] – des données européennes issues du réseau social Facebook.

Dans cet arrêt, la Cour a renouvelé son dispositif et s'est de nouveau prononcée dans le sens d'une « atteinte au contenu essentiel du droit fondamental au respect de la vie privée »[182] dans le cas d'un « accès généralisé par les autorités publiques au contenu des communications électroniques »[183]. Dans son analyse, la Cour a conclu au manque de « garanties suffisantes contre les abus », pourtant nécessaires et d'autant plus cruciales lorsque ces « données sont soumises à un traitement automatique »[184] et qu'est prévue la conservation « généralisée [...] de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées »[185]. Par conséquent, l'on peut en conclure que la décision 2000/520/CE – précédent fondement aux transferts de données à caractère personnel vers les Etats-Unis validant les principes dits de la « Sphère de sécurité » ou *Safe Harbor*[186], elle-même prise sur le fondement de la directive 95/46/CE – constitue une violation grave du droit à la vie privée et du droit à la protection des données personnelles (respectivement inscrits aux articles 7 et 8 de la Charte), « même dans l'objectif de la protection de la sécurité nationale ».[187]

---

[179] « *S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire.* », voir CJUE, *Digital Rights Ireland*, *op. cit.*, §§ 48 et 52.

[180] CJUE, *Maximilian Schrems c. Data Protection Commissioner, op. cit.*

[181] Art. 25, §1 de la Dir. 95/46/CE pose le principe suivant : le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement ne peut avoir lieu que si ce pays assure un niveau de protection « adéquat » à de telles données, pouvant être constaté par une décision de la Commission. Inversement, le considérant 57 de la même directive prévoit l'interdiction d'un transfert de ces données vers un pays-tiers lorsque celui-ci n'offre pas ledit niveau de protection., cité par J.-P. FOEGLE, « Chronique du droit "Post-Snowden" : La CJUE et la CEDH sonnent le glas de la surveillance de masse », in *La revue des droits de l'homme*, Actualités Droits-Libertés, 30 mars 2016, p. 1.

[182] CJUE, *Maximilian Schrems c. Data Protection Commissioner, op. cit.,* §94.

[183] CJUE, *Maximilian Schrems c. Data Protection Commissioner, ibidem,* §94.

[184] CJUE, *Maximilian Schrems c. Data Protection Commissioner, ibidem,* §91.

[185] CJUE, *Maximilian Schrems c. Data Protection Commissioner, ibidem,* §93.

[186] J.-P. FOEGLE, *op. cit.*, p. 1.

[187] F. DUBUISSON, « La Cour européenne des droits de l'homme et la surveillance de masse », in *Rev. trim. dr. h.*, n° 108/2016, Bruxelles, Anthemis, 2016, p. 872 ; BOT (Y.), Concl. de l'avocat général, note sous CJUE, arrêt Schrems c. Data Protection Commissioner, in *RTDE*, 2015, §207.

§3. L'affaire Tele2 (arrêt du 21 décembre 2016)

Fin 2016, la Cour a affirmé une nouvelle fois sa détermination à garantir les droits fondamentaux des citoyens à l'ère numérique en clarifiant l'interprétation de la directive 2002/58/CE sur la vie privée et les communications électroniques[188], lue à la lumière de la Charte. Face aux législations nationales anglaise et suédoise prévoyant une obligation générale, pour les fournisseurs de services de communications électroniques, de conservation « *systématique, continue, généralisée et indifférenciée de données relatives au trafic et des données de localisation, sans aucune exception* »[189], la Cour a réitéré une analyse analogue à celle de l'arrêt *Digital Rights*, en affirmant être en présence d'une *« ingérence particulièrement grave »*[190].

De plus, ces régimes nationaux permettaient aux autorités nationales compétentes d'avoir un accès illimité aux données conservées – c'est-à-dire sans qu'une lutte contre la criminalité grave ne doive justifier cet accès intrusif dans la vie privée des individus –, qui plus est sans prévoir de contrôle préalable d'une juridiction ou autorité administrative indépendante.[191] La Cour a également condamné le fait que ces législations nationales n'exigeaient pas que les données en cause soient « *conservées sur le territoire de l'Union* »[192] ni qu'elles soient « *irrémédiablement détruites au terme de leur durée de conservation* »[193] – ce qui pourrait rappeler l'éternelle méfiance de l'Europe envers les Etats-Unis, à son apogée dans l'arrêt *Schrems* analysé précédemment. Ainsi, la Cour a conclu que ces régimes dérogatoires au droit fondamental au respect de la vie privée ne s'opéraient pas dans les limites du strict nécessaire[194] – principe désormais bien ancré dans la jurisprudence de la Cour.

Enfin, notons que la Cour ne s'est pas opposée en bloc à toute conservation de données à titre préventif, pour autant que celle-ci soit ciblée, qu'elle vise uniquement à lutter contre la criminalité grave, que les catégories de données conservées soit limitées au strict nécessaire, que l'accès des autorités nationales soit soumis à conditions, dont un contrôle préalable, etc.[195]

---

[188] Dir. (CE) n° 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E,* L.201/37, du 31 juillet 2002.

[189] CJUE, *Tele2*, *op. cit.*, §§ 46, 50, 62, 97, 103, 105, 112 et 134.

[190] CJUE, *Tele2*, *ibidem*, §§100, 125 et 134 ; CJUE, *Digital Rights*, *op. cit.*, §37.

[191] CJUE, 21 décembre 2016, *Tele2*, Communiqué de presse n° 145/16, Luxembourg.

[192] CJUE, *Tele2*, *op. cit.*, §§ 114, 122 et 125.

[193] CJUE, *Tele2*, *ibidem*, §122.

[194] Voir le considérant n° 30 de la Dir. 2002/58 : « *les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires*. » ; CJUE, *Tele2*, *ibidem*, §§ 103, 107 à 110, 118 et 119.

[195] A.-L. VILLEDIEU, *Données personnelles : la défense du droit à la vie privée face à la volonté des Etats membres d'imposer une surveillance généralisée*, mai 2017, www.lexplicite.fr (consulté le 14 juillet 2018).

Section 2. Cour européenne des Droits de l'Homme

Dans un contexte aussi sensible que celui du respect des droits fondamentaux tels que la protection de la vie privée ou les données à caractère personnel, il est important de souligner que la Cour de Strasbourg s'est, elle aussi, attelée à radicalement condamner la surveillance de masse, d'abord dans son arrêt Zakharov en 2015[196], suivi de son arrêt Szabo en 2016[197]. Ces arrêts de principe seront les premiers à influencer les nouvelles législations nationales en matière de recueil des données personnelles à travers l'Europe.[198]

§1. L'affaire Zakharov (arrêt du 4 décembre 2015)

La Cour, saisie d'une affaire mettant en cause le système d'interception secrète et généralisée des communications de téléphonie mobile en Russie, a conclu à la violation de l'article 8 de la Convention, en « *l'absence de garanties adéquates et effectives contre l'arbitraire et le risque d'abus* »[199]. En effet, ce risque est d'autant plus important en Russie, en ce que les systèmes de surveillance et les policiers sont autorisés à accéder directement à l'ensemble des communications privées des citoyens.[200] De plus, de nombreuses défaillances juridiques furent pointées par la Cour : absence de durée limite de conservation des données, de contrôle des interceptions, d'autorisation préalable, de délimitation des circonstances visées, etc.[201] Enfin, l'effectivité des recours (art. 13) posait également problème, en ce qu'une plainte était uniquement possible lorsque les individus étaient à même de prouver l'interception des données par les autorités.[202]

§2. L'affaire Szabo (arrêt du 12 janvier 2016)

Dans cette affaire, la Cour a opté pour un autre raisonnement : celui du test de la « stricte nécessité »[203] introduit par la CJUE dans son arrêt *Digital Rights* et utilisé par le rapporteur spécial de l'ONU. Par ailleurs, elle a renouvelé sa conclusion concernant le droit fondamental au respect de la vie privée face à une surveillance de masse secrète et en l'absence de contrôle juridictionnel et de garanties suffisamment précises, effectives et complètes.[204] En effet, bien

---

196 Cour EDH, Gr. Ch., 4 décembre 2015, *Roman Zakharov c. Russie*, Req. n°47143/06.

197 Cour EDH, 5e sect., 12 janvier 2016, *Szabo et Vissy c. Hongrie*, Req.n°37138/14.

198 J.-P. FOEGLE, *op. cit.*, pp. 1 et 2.

199 Cour EDH (Unité de presse), *Fiche thématique – Protection des données personnelles*, juin 2018, www.rm.coe.int (consulté le 17 juillet 2018).

200 Cour EDH (Unité de presse), *ibidem*.

201 Cour EDH (Unité de presse), *ibidem.*

202 Ce qui est en réalité techniquement impossible, en l'absence de système de notification ou de possibilité d'accès aux informations sur les interceptions, voir Cour EDH (Unité de presse), *ibidem.*

203 Cour EDH, *Szabo*, *op. cit.*, §§ 67 à 70 et 73.

204 Et fait ainsi référence à sa jurisprudence classique, à savoir Cour EDH, *Klass, op. cit.* et Cour EDH, *Zakharov*, *op. cit.*

que la Cour reconnaisse que le contexte actuel mène naturellement à un recours aux techniques de surveillance par les gouvernements, elle ne valide pas les mesures injustifiées et exagérément intrusives qui peuvent frapper abusivement tous les citoyens. De plus, vu qu'aucun texte international ne permet de « déclarer illégal en son principe » le mécanisme de surveillance massive, la Cour se replie sur un contrôle très exigeant de proportionnalité axé sur son « encadrement effectif ».[205] Pour conclure, l'arrêt de la Chambre constitue un certain pivot dans la jurisprudence de la Cour, en ce qu'un dispositif de surveillance devra répondre de l'épreuve de stricte nécessité dans tous les cas de figure, qu'il soit ciblé ou non.[206] Il reste à voir si la Grande Chambre confirmera ce changement de paradigme dans un positionnement ultérieur.

Section 3. Contribution des juges européens dans l'évolution de la protection des données

Finalement, cet exposé permet de percevoir les points communs entre deux juridictions concurrentes. En effet, plongés dans un « dialogue des juges » à l'ère numérique, « dans un contexte européen où les populismes progressent et les libertés régressent à proportion »[207], ces juges siégeant au sein de différentes institutions (Cour EDH, CJUE…) parviennent à unir leurs forces pour enclencher la « procédure d'alerte » – d'ailleurs créée suite aux affaires hongroises mentionnées à la Section 1 –, pour interpréter le droit de façon cohérente, en ne cédant pas face aux pressions gouvernementales, le tout dans le but ultime d'ériger progressivement une figure stable et équilibrée de la protection des droits fondamentaux. Au cœur des mesures sécuritaires inquiétantes et des progrès informatiques, ces juges prennent leurs responsabilités et censurent les dérives auxquelles l'on a donné trop de liberté. Pleinement conscients des enjeux actuels, ils condamnent les abus et sauvegardent les bases démocratiques de notre société. Le Juge Paul Pinto de Albuquerque, siégeant à la Cour EDH dans l'affaire *Szabo*, résume d'ailleurs parfaitement ce combat comme suit :

> « ***a system of secret surveillance designed to protect national security entails a risk of undermining or even destroying democracy on the ground of defending it*** »[208].

***

[205] F. DUBUISSON, *op. cit.*, p. 884.
[206] F. DUBUISSON, *ibidem*, p. 883.
[207] S. PEYROU, « Surveillance de masse : un coup d'arrêt aux dérives de la lutte antiterroriste », note sous CEDH, arrêt *Szabo et Vissy c. Hongrie*, janvier 2016, www.gdr-elsj.eu (consulté le 17 juillet 2018).
[208] Voir Cour EDH, Grande Chambre, 5 mai 2000, arrêt *Rotaru v. Romania*, § 59, paraphrasant lui-même en réalité Cour EDH, *Klass, op. cit.*, § 49: « ***The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*** », cité par Cour EDH, *Szabo*, *op. cit.*, §34 de l'opinion concordante du Juge P. DE ALBUQUERQUE.

TITRE II. Analyses dérives et défis

Les méthodes de lutte contre le terrorisme sont aujourd'hui de plus en plus étendues et de moins en moins encadrées. Face au renforcement des pouvoirs de la police, à l'assouplissement d'un certain nombre de procédures, à la mise entre parenthèses de certaines garanties élémentaires, à la multiplication des formes de profilage ethnique, racial et religieux par la police et nos gouvernements,… ne sommes-nous pas à la dérive vers un Etat policier ? Existe-t-il encore une balance entre le pouvoir judiciaire et le pouvoir de plus en plus étendu de l'exécutif (Chapitre 1) ? La mise en œuvre de ces mesures est-elle réellement nécessaire et efficace ? Valent-elles la peine de sacrifier, fut-ce temporairement, nos droits fondamentaux ? Cet état d'urgence, cette dérogation au droit conventionnel nous apporte-elle réellement plus de sécurité (Chapitre 2) ? Est-il possible de rétablir un équilibre entre la sauvegarde des droits et libertés des citoyens et la garantie de la protection de la sécurité (Chapitre 3) ? Quelle est la gravité du risque actuel pour l'Etat de droit et la forme démocratique de notre société ?[209]

CHAPITRE 1. Dérives et vulnérabilités en Europe

Section 1. Multiplication des formes de surveillance généralisée

§1. Passenger Name Record (PNR)

« *Une Europe qui protège est une Europe qui se défend, à l'intérieur comme à l'extérieur de son territoire* »[210], a affirmé le Président de la Commission européenne Jean-Claude Juncker, insistant sur la priorité européenne de la sécurité, la lutte antiterroriste et la défense. Les dirigeants européens se soucient en effet de maintenir l'ordre sur le territoire européen et développent ainsi des actions proactives et préventives, en amont de potentielles attaques. C'est dans ce dessein que s'inscrit l'invention du PNR – récolte massive et généralisée des données personnelles fournies aux transporteurs aériens par les voyageurs, dans le but d'établir des « schémas de déplacement et de comportement », pour ensuite cibler les itinéraires suspects.[211]

[209] Interview de P. LAVENU (secrétaire national de la section Île-de-France du syndicat de police Alliance), V. DUVAL (Présidente de l'Union syndicale des magistrats (USM)), J.-M. SCHLOSSER (sociologue, ancien inspecteur de police, auteur d'une thèse sur les techniques de formation des policiers) et M. TROUVE (avocate pénaliste, membre du Syndicat national des avocats de France (SAF)), 12 janvier 2016, https://www.franceculture.fr/ (consulté le 18 juillet 2018).

[210] J.-C. JUNCKER, « Discours sur l'état de l'Union 2016 : Vers une Europe meilleure – Une Europe qui protège, donne les moyens d'agir et défend », Discours autorisé, Strasbourg, le 14 septembre 2016, https://ec.europa.eu/ (consulté le 18 juillet 2018).

[211] E. DELHAISE et C. FIEVET, « Frontières intelligentes et nouvelles incriminations pénales: l'UE face à la problématique des "Foreign terrorist fighters" », in *Journal des tribunaux*, n° 6676, 11 février 2017, p. 116.

Union européenne

A l'échelle européenne, le renforcement des mesures sécuritaires a été marqué par la directive 2016/681[212] relative à l'utilisation des données des dossiers passagers (PNR) adoptée en avril 2016. Sont ainsi récoltés quotidiennement, lors de chaque réservation ou enregistrement de vol entrant ou sortant de l'UE[213], des centaines de milliers de noms, prénoms, adresses, itinéraires, informations sur les bagages, sur les agences de voyages, adresses mail et adresses IP, numéros de téléphone et de carte de crédit, préférences alimentaires etc.[214] Celle-ci complète de ce fait la directive *Advance Passenger Information* (API)[215] de 2014, en ce qu'elle contraint aujourd'hui les compagnies aériennes à transmettre les données des passagers aux pays de l'UE dans le but de respecter la mission énoncée aux considérants n° 5 et 6, à savoir :

(5) *Les objectifs de la présente directive sont, entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes.*

(6) *L'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, et donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels.*

Ces objectifs sont-ils néanmoins suffisamment clairs, précis et encadrés pour autoriser la récolte massive et non ciblée, l'utilisation et la conservation de nombreuses données privées de l'entièreté des voyageurs ? Comme le souligne brillamment l'eurodéputé Georges Bach, « *malgré toute l'importance de la lutte contre le terrorisme, il ne faut pas perdre de vue les libertés individuelles et le droit à la protection des données* » et encore moins « *tomber dans la suspicion générale* »[216]. Malgré de nombreuses tergiversations, cette directive a fini par être votée à 32 voix contre 27 en avril 2016, en ce qu'elle a le mérite d'effacer les divergences entre les Etats membres et d'établir une protection harmonisée et cohérente des données PNR.[217]

[212] Dir. (UE) n° 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers des passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *J.O.U.E.,* L.119/132, du 4 mai 2016.

[213] Timothy Kirkhope, eurodéputé britannique jusqu'en 2016, avait d'ailleurs proposé d'élargir le champ d'application territorial de la directive PNR aux vols intra-européennes, ce qui n'a pas été approuvé par la commission de la justice et des libertés civiles, selon C. STUPP, *Le fichage des passagers aériens franchit une étape au Parlement européen*, juillet 2015, https://www.euractiv.fr/ (consulté le 18 juillet 2018).

[214] Il y aurait 60 catégories de données PNR collectées, selon C. STUPP, *ibidem*.

[215] Dir. (CE) n° 2004/82 du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *J.O.U.E.,* L.261/24, du 6 août 2004.

[216] G. BACH, *Passagéierdaten : Schutz oder Gefor?*, 26 janvier 2015, https://csv.lu/ (consulté le 18 juillet 2018), cité par EUROPAFORUM LUXEMBOURG, *Dossier PNR*, janvier 2015, http://www.europaforum.public.lu/ (consulté le 18 juillet 2018).

[217] 16 pays européens ayant, à l'époque, développé leur propre système PNR, et l'Europe ayant conclu des accords bilatéraux avec l'Australie, le Canada, les Etats-Unis , et potentiellement le Mexique, voir C. STUPP, *op. cit*.

Accord PNR UE-USA du 19 avril 2012

Les Etats-Unis, ayant adopté une législation nationale PNR au lendemain des attentats du 11 septembre, ont depuis lors toujours sollicité des négociations avec la Commission européenne afin de légaliser le transfert des données PNR au ministère de la sécurité intérieure (US Department of Homeland Security : DHS).[218] Afin de se trouver en conformité avec la directive européenne sur la protection des données, le transfert de ces données devait jouir d'une « protection adéquate ». Le premier accord transatlantique, conclu en 2006, fut aussitôt condamné par la Cour de justice, sur requête du Parlement.[219] Depuis 2007, un nouvel accord était alors administré provisoirement. Le Parlement européen ayant refusé de signer cet accord en 2010, la Commission a relancé des négociations en 2011, ce qui a mené à l'accord finalement signé par le Conseil, ainsi que par une vaste majorité du Parlement le 19 avril 2012.[220]

Qu'est-ce qui a amené à la signature de cet accord, pourtant largement critiqué[221] concernant les garanties relatives à la protection des données et autres droits fondamentaux ? En effet, de sérieuses inquiétudes se sont faites entendre au sujet du champ d'utilisation de données potentiellement sensibles, de la durée de leur conservation – potentiellement illimitée –, le tout en l'absence de garanties contre les abus, menaçant ainsi le principe de proportionnalité.[222] Le fait est que, si cet accord n'avait pas été conclu, il aurait laissé un vide juridique et, partant, la voie libre à des accords bilatéraux, négociés individuellement avec les Etats-Unis et potentiellement bien plus liberticides.

Selon de nombreux auteurs, « l'Europe a ainsi manqué une occasion d'imposer sa voix dans cette difficile relation transatlantique », se laissant porter par des « considérations diplomatiques et pragmatiques ayant pris le dessus. »[223] Si l'on en croit l'eurodéputé Jan Philip Albrecht, cette décision « constitue encore un pas vers un Etat policier »[224].

---

[218] E. WERY, *La Cour de justice va-t-elle interdire le transfert aux autorités US des données des passagers se rendant aux USA? L'avocat général le suggère*, 27 novembre 2005, www.droit-technologie.org (consulté le 9 juillet 2018).

[219] CJCE, 30 mai 2006, aff. jointes *Parlement européen c. Conseil de l'Union européenne* et *Commission des Communautés européennes*, C-317/04 et C-318/04.

[220] S. PEYROU, *Diplomatie ou droits fondamentaux? Questions sur la conclusion de l'accord PNR entre les Etats-Unis et l'Union*, 3 mai 2012, www.gdr-elsj.eu (consulté le 12 juillet 2018).

[221] notamment par le contrôleur européen des données Peter Hustinx et l'eurodéputé Guy Verhofstadt.

[222] COPPELIA, *Accord PNR (Passenger Name Record) avec les Etats- Unis : feu vert du Parlement européen*, avril 2012, https://europe-liberte-securite-justice.org (consulté le 13 juillet 2018).

[223] S. PEYROU, *Diplomatie (...)*, *op. cit.* et S. PEYROU, *L'accord PNR entre l'Union et le Canada ne respecte pas, en l'état, la Charte des droits fondamentaux de l'UE, réflexions faisant suite aux conclusions de l'avocat général Mengozzi dans la demande d'avis 1/15*, 20 septembre 2016, http://www.gdr-elsj.eu (consulté le 19 juillet 2018).

[224] « Pour la première fois depuis dix ans, le Parlement européen avait l'opportunité d'arrêter le profilage et la

Accord UE-Canada et avis 1/15 de la CJUE du 26 juillet 2017

En 2014, le Canada et l'Union européenne signaient un projet d'accord relatif au traitement et au transfert des données des dossiers passagers (PNR). Pour la première fois, le Parlement européen a saisi, avant son approbation, la Cour de justice pour s'assurer de la conformité du projet aux droits fondamentaux exprimés dans la Charte (respect de la vie privée et protection des données à caractère personnel, art. 7 et 8).[225] Ainsi, c'est dans un avis du 26 juillet 2017[226] que la Cour a mis fin à cette polémique tournant autour des accords PNR et de la dir. 2016/681 détaillée *supra* : décision « équilibrée » et symbolisant la voie du juste milieu pour certains[227], inconsistante et incarnant un déracinement décevant pour d'autres. Cet avis se détache substantiellement de la jurisprudence antérieure de la Cour tout en réutilisant ses grilles d'analyse. En effet, même si l'arrêt de principe *Digital Rights* – condamnant toute *« conservation systématique, continue, généralisée et indifférenciée de données » (cf. supra)* – et ceux qui ont réitéré ces affirmations – à savoir les arrêts *Schrems* et *Tele2* – auraient pu laisser entrevoir une invalidation du système PNR et ainsi une continuité et une cohérence dans la jurisprudence de la Cour, cet avis nous livre une acceptation implicite du système PNR, même s'il suggère quelques aménagements substantiels du texte.[228]

Comment expliquer ce glissement significatif opéré par la Cour ? Est-ce le résultat d'une pression européenne – sachant qu'une invalidation du système PNR risquait de mettre la directive 2016/681 récemment adoptée dans l'embarras ? S'agit-il d'une pression internationale – en ce que cela remettrait en question la validité des accords conclus avec les Etats-Unis ou l'Australie ? L'explique-t-on par le contexte européen plus marqué que jamais par le terrorisme, couplé à « *l'évolution de la société, du progrès social et des développements scientifiques et technologiques* »[229] ? C'est sans doute collectivement que ces éléments ont contribué au retournement de situation exprimé dans les conclusions de l'avocat général : « *cet objectif d'intérêt général de l'UE est susceptible de justifier des ingérences, même graves, dans les droits fondamentaux* ».[230] Nous attendrons le prochain arrêt de la Cour quant à ce revirement.

---

rétention à long terme et sans fondement des données de tous les voyageurs allant aux Etats-Unis, mais une majorité a choisi de passer à côté », voir COPPELIA, *op. cit*.

[225] V. TECHENE, *L'accord UE/Canada sur le transfert de données de passagers aériens incompatible avec la Charte des droits fondamentaux de l'Union*, 31 juillet 2017, www.actualitesdudroit.fr (consulté le 3 juillet 2018).

[226] CJUE, Grande Chambre, avis 1/15 du 26 juillet 2017, ECLI:EU:C:2017:592.

[227] S. PEYROU, *Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir !*, 28 juillet 2017, http://www.gdr-elsj.eu (consulté le 10 juillet 2018).

[228] S. PEYROU*, L'accord PNR entre l'Union et le Canada ne respecte pas (…), op. cit.*

[229] CJUE, avis 1/15, *op. cit.*, § 135.

[230] CJUE, avis 1/15, *op. cit.*, §§ 148 à 151 des conclusions de l'avocat général Mengozzi.

Point de vue national belge

Parmi les Etats membres, qui disposaient d'un délai de 2 ans pour transposer la directive 2016/681 dans leur droit national, nous étudierons brièvement le cas de la Belgique – deuxième Etat de l'Union, après la Hongrie, à transposer cette directive PNR du 27 avril 2016.[231] Notons que Julian King, commissaire à la sécurité au sein de l'exécutif européen, a récemment urgé les Etats membres à adopter les dispositions législatives, règlementaires et administratives nécessaires à la bonne application de la directive PNR et la collaboration entre les nations européennes.[232]

En Belgique, la loi du 25 décembre 2016 relative au traitement des données des passagers[233], dite la « loi PNR », transpose donc en droit belge la « directive PNR ». Cette loi fait partie de l'ensemble des mesures prioritaires (dix-huit au total) prises par le gouvernement fédéral pour renforcer les outils juridiques belges de lutte contre le terrorisme et la criminalité grave.[234] Sa plus grande spécificité est sans doute son champ d'application élargi. En effet, elle définit le concept de « transporteur » et d'« opérateur de voyage », sur qui pèse l'obligation de transfert des données, comme « *toute personne physique ou morale qui assure, à titre professionnel, le transport de personnes par voie aérienne, maritime, ferroviaire ou terrestre* »[235], alors que la directive ne régit que les cas de transport aérien.

Ainsi, le constat peut être dressé comme suit : la loi belge va plus loin que les exigences minimales européennes, et intègre toutes les « possibilités de renforcement du domaine d'application » prévues par cette directive.[236] Quels sont les risques, potentiellement accrus, pour les droits fondamentaux au respect de la vie privée et à la protection des données personnelles ? Ceux-ci sont nombreux et se retrouvent tant au stade de la prévention du terrorisme qu'à l'étape des poursuites ou de la répression. Par exemple, ces nouvelles infractions – notamment la nouvelle incrimination des « voyages à visée terroriste » insérée dans le Code pénal[237] – seront compliquées à prouver, et la frontière entre la collecte des données « nécessaires à la lutte contre le terrorisme » et « à caractère sensible » reste ténue.

---

[231] L. PONCIAU, *Déjà deux millions de passagers sont passés par le PNR*, 16 avril 2018, http://plus.lesoir.be/ (consulté le 20 juillet 2018).
[232] E. DELHAISE et C. FIEVET, *op. cit.*, p. 116.
[233] Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017, p. 12905.
[234] IBZ CRISISCENTRUM, *Sécurité publique – PNR,* 2017, https://crisiscentrum.be/ (consulté le 20 juillet 2018).
[235] Art. 4, 1° et 2°, 5 à 7 et art. 45 de la loi du 25 décembre 2016, *op. cit.*
[236] E. DELHAISE et C. FIEVET, *op. cit.*, pp. 116 et 117.
[237] Loi du 20 juillet 2015 visant à renforcer la lutte contre le terrorisme, *M.B.*, 5 août 2015, p. 49326.

§2. Banques de données

Données biométriques : les empreintes digitales

Le recours à la biométrie est de plus en plus répandu dans nos registres et systèmes informatiques, et touche aujourd'hui l'immense majorité des citoyens. Le Contrôleur européen de la protection des données affirme d'ailleurs qu' « en rendant possible la mesure des caractéristiques du corps humain par des machines et en permettant l'utilisation ultérieure de ces caractéristiques, la biométrie modifie définitivement la relation entre corps et identité ».[238] Celui-ci nous met également en garde par rapport au fait que leur lecture et utilisation est éventuellement praticable « pour toujours et où que puisse se rendre la personne concernée »[239], ce qui rend cet instrument hautement intrusif et potentiellement hasardeux.

Le règlement n° 2252/2004[240] impose, en son article 1er, §2, l'obligation suivante :

« *Les passeports et les documents de voyage comportent un support de stockage de haute sécurité qui contient une photo faciale. Les États membres ajoutent deux empreintes digitales relevées à plat, enregistrées dans des formats interopérables. Les données sont sécurisées et le support de stockage est doté d'une capacité suffisante et de l'aptitude à garantir l'intégrité, l'authenticité et la confidentialité des données*. »

Dans l'affaire *Schwarz*[241], la Cour a déclaré que la condition, préalable à la délivrance d'un passeport, d'être soumis au relevé obligatoire de deux empreintes digitales ne violait pas le droit fondamental à la protection des données à caractère personnel consacré à l'article 8 de la Charte, en ce que l'atteinte devait être jugée proportionnée. Plusieurs éléments ont également amené l'avocat général à conclure à l'absence d'ingérence disproportionnée. Citons par exemple les éléments suivants : limitation du prélèvement et du stockage à deux empreintes digitales, limitation du champ d'application de cette obligation aux seuls citoyens voyageant en dehors des frontières de l'Union, limitation de l'utilisation de ces données[242], détention de ces données

[238] Avis du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, JO C 181, p. 13, cité par M. PAOLO MENGOZZI (M.), concl. générales CJUE présentées le 13 juin 2013, arrêt Michael Schwarz contre Stadt Bochum du 17 octobre 2013, X, 2013.

[239] Avis du 23 mars 2005, *ibidem*.

[240] Règlement (CE) n° 2252/2004 du Conseil, du 13 décembre 2004, *établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres*, JO L 385, p. 1, tel que modifié par le règlement (CE) no 444/2009 du Parlement européen et du Conseil, du 28 mai 2009, JO L 142, p. 1.

[241] CJUE, 13 juin 2013, *Michael Schwarz c. Stadt Bochum*, affaire C-291/12.

[242] Selon l'article 4, §3 du règlement no 2252/2004, l'utilisation de ces données doit être faite à des fins strictement déterminées: le règlement n° 2252/2004 tel que modifié prévoit ainsi que les données ne sont utilisées « que pour vérifier » l'authenticité du passeport et l'identité du titulaire, cité par M. PAOLO MENGOZZI, *op. cit.*

dans l'unique support de stockage sécurisé inséré dans le passeport – ce qui rend le citoyen européen « seul détenteur de l'image de ses empreintes »[243] –, limitation de la durée de stockage des empreintes dès lors alignée à la durée de validité du passeport et interdiction faite aux Etats de constituer, sur base dudit règlement, une base de données stockant ces informations.[244] Ce dernier élément étant particulièrement essentiel, nous nous intéresserons, dans le point suivant, à la banque de données « *Foreign Fighters Terrorism* » qui a pourtant été mise sur pied.

Néanmoins, dans l'affaire *Willems*[245] de 2015, la Cour semble « marquer le 'glas' de la démarche constructive des juges de Luxembourg en matière de protection des données personnelles »[246]. En effet, la Cour s'est ici opposée à garantir une limitation de l'utilisation des données digitales recueillies sur le fondement du règlement susmentionné. Ce faisant, la Cour ne condamne pas les potentielles utilisations de ces données qui seraient ultérieures à la délivrance du passeport – ce qui, implicitement, n'exclut pas la possibilité d'une création d'une banque de données, écartant ainsi les données biométriques concernées du champ d'application de la Charte des droits fondamentaux ainsi que de la directive 95/46[247] sur les données personnelles. En interprétant si restrictivement l'arrêt *Schwarz* de 2013, la Cour s'oriente finalement vers une lecture restrictive de la Charte elle-même, en ce qu'elle « vide tragiquement la portée du droit à la protection des données personnelles dans un domaine où celui-ci est [pourtant] vital »[248].

« Foreign Fighters Terrorism » (FFT)

C'est ainsi qu'en 2016, le législateur belge a permis aux ministres de l'Intérieur et de la Justice de créer conjointement des banques de données communes[249], notamment dans le but de « renforcer la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme »[250]. Cette banque de données commune est ainsi supposée favoriser l'échange de renseignements dans le but d'améliorer le rendement de la lutte antiterroriste.[251] Pas moins de

[243] M. PAOLO MENGOZZI, *ibidem*.
[244] M. PAOLO MENGOZZI, *ibidem*.
[245] CJUE, 16 avril 2015, *W.P. Willems c. Burgemeester Van Nuth*, affaires jointes C-446/12 et C-449/12, §1.
[246] J.-P. FOEGLE, « Sans doigt, ni loi : la CJUE donne son 'feu vert' à la biosurveillance », in *La Revue des droits de l'homme*, Actualités Droits-Libertés, juillet 2015, p. 2.
[247] Dir. 95/46/CE précitée.
[248] J.-P. FOEGLE, *op. cit*.
[249] Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme, *M.B.,* 9 mai 2016, p. 30567, art. 44/11/3*bis*.
[250] Loi du 27 avril 2016, *ibidem*, art. 44/11/3*quater*, complétant le mécanisme des banques de données initialement mis en place par la loi du 5 août 1992 sur la fonction de police, *M.B.,* 22 décembre 1992, p. 27124, art. 44/2.
[251] Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme, Avis de la Commission belge de la Protection de la Vie Privée, pp. 67 et s.

trois mois plus tard, un arrêté royal fut adopté dans le but de façonner la banque de données commune « *Foreign Terrorist Fighters* » (F.T.F.) – ou « *Returnees* », terme européen désignant ces « combattants formés dans une zone de combat djihadiste à l'étranger aux techniques de combat et susceptibles de mener des actions terroristes en Europe lors de leur retour »[252]. Celle-ci permet principalement à l'OCAM[253], à nos services de renseignement et de sécurité, à la police et à la justice[254] de « partager des connaissances afin de protéger nos citoyens de la violence aveugle de certaines personnes ou groupements et d'essayer d'anticiper et de contrer ces actions violentes » ainsi que de dresser une « fiche de renseignements » sur ces personnes dans le but « non seulement de pouvoir évaluer la menace potentielle que représentent ces personnes, mais surtout d'en assurer un suivi afin d'anticiper et d'empêcher de possibles actes terroristes de leur part »[255].

Cette banque de données – reprenant près de 600 personnes en Belgique (dont 38 sont actuellement suivies sur base d'« indices concrets de passage éventuel à un acte violent »), par contraste aux quelques 20.000 'Fichiers S' français[256] – a provoqué de vives réactions de la part de plusieurs associations. Parmi elles, l'ONG Amnesty International dénonce l'impossibilité pour les citoyens de s'assurer de l'absence de leurs données sur la liste noire de l'OCAM, ainsi que de l'absence de procédure d'accès aux informations concernant ces mêmes citoyens.[257]

Reconnaissance faciale

Avant de clore le sujet des banques de données, nous aimerions aborder le sujet délicat des systèmes de reconnaissance faciale. Cette technique, permettant, « à partir des traits de visage », d'authentifier une personne – c'est à dire « de vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès, par exemple) » – ou d'identifier une personne – c'est-à-dire « de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une

[252] EUROPOL, *EU Terrorism Situation and Trend Report (TE-SAT)*, 2016, www.europol.europa.eu/ (consulté le 27 juillet 2018), cité par E. DELHAISE et C. FIEVET, *op. cit.*, p. 113.
[253] L'Organe de coordination pour l'analyse de la menace est un service officiel belge chargé de l'analyse de la menace en matière de terrorisme et d'extrémisme, sur base des informations fournies par les services publics fédéraux.
[254] L. LEMMENS et K. MEES, *Un AR précise le fonctionnement de la banque de données 'Foreign Terrorist Fighters'*, Wolters Kluwer, 2016, https://legalworld.wolterskluwer.be (consulté le 27 juillet 2018).
[255] A.R. du 21 juillet 2016 relatif à la banque de données commune *Foreign Terrorist Fighters* et portant exécution de certaines dispositions de la section 1er *bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police, *M.B.,* 22 septembre 2016, p. 63970.
[256] N. BEN, *38 terroristes potentiels sont sous surveillance en Belgique*, mars 2018, www.lalibre.be (consulté le 26 juillet 2018).
[257] AMNESTY INTERNATIONAL, *Des mesures disproportionnées*, *op. cit.*

image ou une base de données »[258], est extrêmement inquiétant. En effet, les données biométriques uniques de notre visage sont scannées par le biais d'intermédiaires variés – tels que Facebook ou le nouvel IPhone X – et stockées, sans faire l'objet d'aucune législation. Néanmoins, cette intrusion dans la vie privée peut aller très loin, et ne doit à aucun prix être banalisée. La société Panasonic a, par exemple, développé une technologie permettant à des caméras d'identifier le nombre de passants à un lieu donné, leur nom, leur âge et leur sexe.[259] Cela pourrait conduire à égaler la situation américaine, où 117 millions d'adultes seraient fichés, à leur insu, dans des banques de données tenues par les services de sécurité.[260] Bien que cette avancée technologique puisse être très utile en termes de maintien de l'ordre et de lutte antiterroriste, nous ne devons pas sous-estimer ses dérives sous-jacentes en termes d'atteinte disproportionnée à la protection des données personnelle et de la vie privée. De plus, que dire des dégâts envisageables en cas de détournement de ces données de leur objectif initial…

§3. Perquisitions

Enfin, notons que la période légale de la mesure d'enquête particulièrement intrusive consistant en la pénétration physique d'un lieu privilégié de la sphère de la vie privée dans le but de rechercher les éléments de preuve d'une infraction, a été étendue. En effet, le principe constitutionnel de l'inviolabilité du domicile – protégeant les individus contre l'intrusion intempestive des autorités dans sa sphère intime[261] – a de nouveau été atteint, depuis que la loi du 27 avril 2016 précitée autorise les perquisitions de nuit en cas d' « indices sérieux » de menace terroriste[262] dans le chef de suspects, celles-ci n'étant antérieurement prévues par la loi qu'entre 5h du matin et 21h. Certains juges[263], la section de législation du Conseil d'Etat[264] et d'autres organisations défenderesses des droits de l'homme[265] dénoncent cette mesure Michel, qu'ils estiment particulièrement attentatoire aux libertés, voire disproportionnellement intrusive dans la vie privée des citoyens.

---

[258] CNIL, *Reconnaissance faciale*, https://www.cnil.fr/ (consulté le 17 juillet 2018).
[259] A. TIELENS, *Les dérives de la reconnaissance faciale (opinion)*, avril 2018, www.lalibre.be (consulté le 27 juillet 2018).
[260] A. TIELENS, *ibidem*.
[261] Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme, Avis du Conseil d'Etat, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 1727/001, p. 110.
[262] Loi du 27 avril 2016, *op. cit.*, art. 3, modifiant la loi du 7 juin 1969 fixant le temps pendant lequel il ne peut être procédé à des perquisitions, visites domiciliaires ou arrestations, *M.B.,* 28 juin 1969, p. 6470, art. 1er, al. 2, 6°.
[263] RTBF INFO, *Luc Hennart : "C'est une mauvaise idée de permettre les perquisitions de jour et de nuit",* décembre 2015, https://www.rtbf.be (consulté le 26 juillet 2018).
[264] Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme, *op. cit.*, p. 104.
[265] A. DESWAEF, « Conclusions », in *Etat des droits de l'homme en Belgique, op. cit.*, pp. 40 et s.

Section 2. Discrimination ethnique, raciale ou religieuse

En théorie, le droit à l'égalité et à la non-discrimination est garanti par les art. 10 et 11 de la Constitution, et l'interdiction d'associer une religion, ethnie, nationalité ou civilisation au terrorisme est affirmé par plusieurs résolutions du Conseil de Sécurité[266]. Bien que ceci soit soutenu par plusieurs auteurs et juridictions[267], la pratique semble néanmoins s'en écarter.

§1. Discrimination « probabiliste »

Au-delà de la surveillance généralisée à l'ensemble de la population, certains outils de lutte antiterroriste « de masse » sont déviés et visent, directement ou indirectement, des minorités ethniques, raciales ou religieuses de façon discriminatoire. Dans le contexte actuel, la tentation du profilage racial, ethno-religieux est forte. Avant de nous pencher sur plusieurs illustrations concrètes de ce phénomène, nous aimerions décrire le mécanisme du profilage ethno-racial ou ethno-religieux en lui-même. Plusieurs auteurs se sont penchés sur la question de savoir si les comportements discriminatoires – tels que la discrimination dite « statistique » ou « probabiliste » – revêtaient nécessairement un caractère irrationnel ?[268] Peut-on réduire cet instrument statistique à une généralisation abusive pure et simple ? Autrement dit, le syllogisme qui associerait une religion – telle que l'Islam –, une couleur de peau ou l'appartenance à une communauté ethnique – telle que la population musulmane – à la probabilité accentuée de suspections criminelles et terroristes, est-il pleinement irrationnel, inefficace et immoral ?[269] Selon certains auteurs, tels que Frederick Schauer[270] ou Randall Kennedy[271], les « gains ponctuels » obtenus par ces formes de catégorisations devraient inciter à leur utilisation. Selon un autre point de vue, majoritairement défendu par Bernard Harcourt[272], ces gains sont « illusoires ou évanescents » en matière policière et pénale, et appellent au rejet de ces pratiques qui s'avèreraient « inefficaces et contre-productives au regard de leur objectif initial »[273].

---

[266] Résolution 2354, S/RES/2354, 24 mai 2017 et Résolution 2370, S/RES/2370, 2 août 2017 du Conseil de Sécurité de l'ONU.

[267] C.C. fédérale allemande, arrêt n° 1 BvR 518/02, 4 avril 2006 ; O. DE SCHUTTER, *International Human Rights Law,* 2ème éd., Cambridge, Cambridge University Press, 2014, pp. 595 et s.

[268] B. HARCOURT, *Against Prediction : Profiling, Policing, and Punishing in an Actuarial Age*, Chicago, University of Chicago Press, Chicago, 2007.

[269] M. PARODI, « De la discrimination statistique à la discrimination positive », in *Revue de l'OFCE, Centre de recherche en économie de Sciences PO*, OFCE, Presses de Science Po, éd. 2010/1 n° 112, 2010, pp. 63 à 85.

[270] Professeur de droit constitutionnel américain à l'Université de Virginie et à l'Université de Harvard, auteur de F. SCHAUER, *Profiles, Probabilities, and Stereotypes*, Harvard University Press, Cambridge (Mass.), 2003.

[271] Professeur de droit et auteur à l'Université de Harvard sur l'intersection du conflit racial et des institutions, auteur de R. KENNEDY, *Race, Crime, and the Law*, Pantheon, New York, 1997.

[272] Professeur et directeur du *Center for the Study of Criminal Justice* à l'Université de Chicago, auteur de B. HARCOURT, *Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally*, University of Chicago Law Review, Chicago, 2004.

[273] D. SABBAGH, *Lecture critique de* B. HARCOURT, *Against Prediction (...)*, *op. cit.*, www.journals.openedition.org/

Il nous semble que cette surveillance ciblée et discriminatoire pose de sérieuses questions quant à sa légalité, sa transparence, sa morale, sa rationalité et sa mise en œuvre. En effet, cette pratique prend, selon Harcourt, la forme d'une « prophétie autoréalisatrice », en ce que ces injustices incitent à entretenir les discriminations existantes et risquent de s'accompagner d'inévitables effets pervers, tels que la « validation apparente du stéréotype raciste associant identité ('étrangère', 'musulmane', 'noire'…) et propensions criminelles », stigmatisations et formes de haine et rejet de l'autre.[274] Ainsi, ne serait-il pas possible d'observer le principe fondamental de non-discrimination, en assumant que « la probabilité d'être appréhendé et sanctionné devrait être identique pour tous les auteurs d'infractions pénales, quelle que soit leur race, ethnicité, sexe, classe ou origine nationale »[275] ?

§2. Le profilage racial, ethnique ou religieux : définition

Il n'existe pas de définition universelle du profilage, si bien que les adjectifs « racial », « ethnique » et « religieux » s'utilisent parfois comme des synonymes, tandis qu'ils peuvent dans d'autres cas illustrer une réalité totalement distincte.[276] Bien que le contexte concret et les acteurs concernés influenceront la définition de ce concept au cas par cas, nous avons décidé de nous référer à la définition donnée par *Open Society Justice Initiative*, organisation à but non lucratif internationale oeuvrant à la protection des libertés, de la justice et des droits de l'homme : nous entendrons par profilage ethnique « l'utilisation de *stéréotypes* raciaux, ethniques ou religieux pour prendre des décisions répressives d'arrestation, d'interpellation, de fouille, de contrôle de documents d'identification, d'extraction de bases de données, de collecte de renseignements et d'autres techniques »[277]. Nous verrons ci-dessous que de nombreuses activités de contrôle, surveillance et investigation peuvent s'avérer injustes, discriminatoires ou dépourvues de nécessité, accordant davantage d'importance à l'origine, l'appartenance ethnique, la religion ou l'apparence, plutôt qu'au comportement individuel ou suspect de l'individu.[278]

(consulté le 17 juillet 2018).

[274] D. SABBAGH, *ibidem*.

[275] B. HARCOURT, *Against Prediction (…), op. cit.*, p. 214.

[276] Par exemple, le Groupe « Terrorisme » de l'UE, dans une recommandation de 2002 sur l'utilisation du « profilage terroriste », a défini celui-ci comme utilisant « *un ensemble de variables physiques, psychologiques ou comportementales, qui ont été identifiées comme typiques chez les personnes impliquées dans des activités terroristes et qui peuvent avoir une certaine valeur prédictive à cet égard* ». (voir B. HAYES, *A Failure to regulate: Data protection and Ethnic Profiling in the Police Sector in Europe*, Justice Initiatives, Open Society Justice Initiative, juin 2005, p. 37) Par ailleurs, le Réseau d'experts indépendants en matière de droits fondamentaux de l'UE définit le profilage ethnique, dans leur Avis 2006/4, comme la « *pratique de classification, sur une base systématique, des individus selon leur 'race' ou origine ethnique, leur religion ou leur origine nationale, que ce soit par des moyens automatiques ou non, et de traitement de ces individus sur la base de cette classification* ». La Commission européenne, quant à elle, la a donné la définition suivante dans sa lettre du 7 juillet 2006: le profilage racial ou ethnique « *couvre tout comportement ou toute pratique discriminatoire par les agents des services répressifs et d'autres acteurs publics pertinents, à l'encontre de personnes sur la base de leur race, de leur origine ethnique, de leur religion ou de leur origine nationale, par opposition à leur comportement individuel ou au fait qu'ils correspondent à une description de 'suspect' particulière'* », cité par A. PAP, « Le profilage sur la base de l'appartenance ethnique et de la race dans la lutte contre le terrorisme, la répression et le contrôle aux frontières », in *Libertés civiles, justice et affaires intérieures*, Parlement européen, Bruxelles, novembre 2008, pp. 5 et 6.

[277] OPEN SOCIETY JUSTICE INITIATIVE, *Ethnic Profiling and Counter-Terrorism : Trends, Dangers and Alternatives*, juin 2006, cité par A. PAP, *ibidem*.

[278] A. PAP, *ibidem* ; OPEN SOCIETY JUSTICE INITIATIVE, *Police et minorités visibles : les contrôles d'identité à Paris*, Open Society Institute, New York, 2009.

§3. Contrôles d'identité au faciès

L'on entend souvent des citoyens d'origine immigrée, la plupart du temps d'ascendance nord-africaine et subsaharienne, se plaindre de contrôles d'identité à répétition se basant davantage sur leur apparence que sur leur conduite. Bien que le constat fut difficile à dresser, plusieurs études de grande envergure ont néanmoins été menées en Europe et aux Etats-Unis par plusieurs ONGs, s'intéressant, dans le chef des victimes, à la fréquence de ces contrôles, le jugement que celles-ci portaient sur les agissements de la police et la réaction émotionnelle engendrée.[279] L'issue de l'enquête dresse un bilan sévère : les citoyens relevant de minorités visibles tels que ceux perçus comme 'Noirs' (d'origine subsaharienne ou antillaise) ou 'Arabes' (originaires du Maghreb ou du Machrek) et spécialement les personnes vêtues d'une tenue vestimentaire 'jeune', ont été contrôlés par la police ou la douane de manière disproportionnée (jusqu'à 15 fois plus de risques) par rapport aux individus perçus comme 'Blancs', sur base de critères d'apparences plutôt que sur des comportements ou autres preuves objectives.[280]

Comment analyser cette pratique de contrôle au faciès – équivalent de « profilage racial » sur le plan européen – d'un point de vue juridique ? Cette conduite est tout d'abord contraire à de nombreuses lois antidiscriminatoires et Codes de déontologie nationaux. Néanmoins, notons que les normes juridiques régissant la mise en œuvre des contrôles d'identité ne sont pas irréprochables. En effet, celles-ci laissent trop souvent un pouvoir discrétionnaire généreux aux services de police dans l'appréciation d'un comportement 'suspect' ou 'inaccoutumé' d'un individu lambda. A cela s'ajoute un défaut d'archivage des contrôles, ce qui donne pratiquement carte blanche aux agents de police dans l'exercice de ces intrusions dans la vie privée – non vides de conséquences en termes de dommage moral, surtout si leur fréquence devient élevée, voire systématique. De plus, l'inexistence d'une supervision contrôlant les potentielles dérives vis-à-vis des minorités permet à ces ingérences de se perpétrer sans évaluation ni visée d'amélioration. Ainsi, ces éléments sous-jacents favorisent une utilisation « disproportionnée et discriminatoire » de ces pouvoirs, trop souvent guidés par les stéréotypes sociétaux ou le bon-vouloir de l'agent habilité.[281] A noter que cette réalité n'est pas en accord avec les normes européennes de défense des droits de l'Homme, qui prohibent notamment les distinctions fondées sur l'apparence si elles ne sont pas accompagnées de « justification objective et raisonnable ».[282]

---

[279] OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, ibidem,* p. 10.

[280] OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, ibidem,* p. 10.

[281] La formation des agents de police est, à notre sens, une autre problématique que nous n'aurons malheureusement pas l'opportunité de traiter dans ce travail, mais qui mérite tout de même toute l'attention de nos gouvernements. OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, ibidem,* pp. 41 et 42.

[282] « Les éléments recueillis dans des études émanant d'Europe et des États-Unis suggèrent que les pratiques de

§4. New York Police Department (NYPD) : Hassan v. City of New York

Aux Etats-Unis, un groupe de divers[283] plaignants musulmans américains a intenté un procès pour mettre fin au programme d'espionnage envahissant et discriminatoire du département de police le plus puissant du pays : le *New York Police Department*. En effet, en 2012, l'*Associated Press*[284] dénonçait la conduite de surveillances illégales de musulmans américains innocents menés par le NYPD sur le simple fondement de leur croyance religieuse. Ces citoyens ont été ciblés à New York, ainsi que dans les villes, les mosquées, les entreprises et les campus universitaires du nord-est du pays.[285] L'affaire *Hassan* a été portée devant la Cour fédérale du New Jersey dans la même année. Elle représente la première action en justice introduite au nom de musulmans américains surveillés illégalement sous le couvert d'enquêtes policières intrusives newyorkaises.

Le 13 octobre 2015, la Cour d'appel fédérale du troisième circuit rendait une décision unanime et théâtrale dans l'affaire *Hassan c. City of New York*. Lors de celle-ci, la Cour a reconnu l'existence d'agissements discriminatoires sur base de la religion à l'encontre des musulmans du New Jersey soumis au programme de surveillance établi par le NYPD, et ce malgré l'absence de toute suspicion à leur égard.[286] Ce faisant, la décision a infirmé une décision antérieure du tribunal de district contestant l'existence d'une telle discrimination.[287] Après près de six ans de

---

contrôle au faciès ne remplissent pas ce double critère, car leurs effets négatifs l'emportent largement sur leurs avantages », cité par OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, ibidem,* p. 11.

[283] Le panel des plaignants est en effet très diversifié, parmi lesquels l'on retrouve : un réserviste décoré de l'armée américaine, un propriétaire de petite entreprise qui est également un vétéran du Vietnam, des étudiants et des imams, voir A. GOLDMAN et M. APUZZO (The ASSOCIATED PRESS), *With cameras, informants, NYPD eyed mosques*, février 2012, https://www.ap.org/ (consulté le 23 juillet 2018).

[284] Agence de presse mondiale et généraliste dont le siège se trouve aux Etats-Unis, cette coopérative a révélé, en février 2012, l'existence du programme de surveillance de la vie quotidienne de milliers de musulmans américains ainsi que de leurs lieux de culte mené par le département de police de la ville de New York, voir A. GOLDMAN et M. APUZZO, *ibidem.*

[285] Les dossiers montrent que le NYPD a entrepris des enquêtes entreprenantes et profondément intrusives et détaillées concernant la vie quotidienne des musulmans américains, dans pas moins de 20 mosquées, 14 restaurants, 11 magasins de détail, 2 écoles primaires et 2 associations étudiantes musulmanes dans le New Jersey, voir CENTER FOR CONSTITUTIONAL RIGHTS, *Settlement reached in NYPD Muslim Surveillance Lawsuit*, New York, avril 2018, https://ccrjustice.org (consulté le 24 juillet 2018).

[286] La Cour du district du New Jersey rappelant, dans son dispositif, plusieurs principes généraux, tel que : « *In its effort to anticipate or prevent unlawful activity, including terrorist acts, the NYPD must, at times, initiate investigations in advance of unlawful conduct. It is important that such investigations not be based solely on activities protected by the First Amendment. It is also important that investigations not intrude upon rights of expression or association in a manner that discriminates on the basis of race, religion or ethnicity, where such discrimination is a substantial or motivating factor for the investigation* (…) », voir US DISTRICT COURT (New Jersey), *Hassan v. City of New York – stipulation of settlement*, 4th May 2018, Case 12-CV-3401 (WJM)(MF), p. 14, https://ccrjustice.org/ (consulté le 24 juillet 2018).

[287] « *On October 13, 2015, the Third Circuit reversed and remanded the district court's dismissal for lack of standing and failure to state a claim for further proceedings, finding, inter alia, that "discrimination itself is [a] legally cognizable injury", and that Plaintiffs plausibly pled that the NYPD conducted a "surveillance program*

procès, les demandeurs *Hassan* ont finalement conclu un accord historique (*landmark settlement*) avec le NYPD en mai dernier. Cet accord indique clairement que le simple fait d'être musulman ne constitue pas un motif de suspicion ou une base légitime à la surveillance. De plus, celui-ci marque une victoire monumentale pour les communautés musulmanes américaines qui revendiquent un traitement juste et équitable dans le chef des forces de l'ordre. Ainsi, les demandeurs *Hassan* ont, par ce fait, défendu leurs droits et les droits de tous les Américains à ne pas subir de surveillance ciblée sur la seule base de sa race, ethnie ou religion. A l'image de pionniers des droits civiques tels que Rosa Parks, Linda Brown et d'autres avant eux, les plaignants *Hassan* ont combattu la discrimination systémique – avec succès.[288]

§5. Le 'Plan canal' de Jan Jambon en Belgique

Dans le même domaine, le plan d'action du gouvernement « contre la radicalisation, l'extrémisme et le terrorisme », surnommé le « plan canal » ou le « plan Jambon » – à l'initiative du ministre de l'Intérieur Jan Jambon (N-VA) – soulève de nombreuses inquiétudes dans notre pays.[289] En effet, quand certains décident de mieux cibler et concentrer leurs recherches sur « une dizaine de personnes à haut risque », en appréhendant les individus réellement dangereux et éventuellement leurs réseaux[290], le ministre Jambon, lui, élargit la surveillance à des dizaines de milliers de citoyens, directement et via la surveillance de leurs lieux de culte, de leurs associations, maisons, entourage, famille, amis, voisins…[291] De plus, outre les analyses de la consommation en eau et électricité des domiciles dans les zones 'propices à la radicalisation'[292] et les renforts policiers dans les rues de sept communes bruxelloises bordant le canal, les forces de police et le parquet verront ajouté à leurs missions le contrôle des subdivisions illégales des logements.[293] Cette généralisation de la surveillance est-elle réellement la solution adaptée aux priorités antiterroristes, ou est-elle trop dispersée ? N'est-on pas allés trop loin ?

---

with a facially discriminatory classification" and that "intentional discrimination based on religious affiliation must survive heightened equal-protection review" », voir US DISTRICT COURT (New Jersey), *ibidem*., p. 2.

[288] MUSLIM ADVOCATES, *Hassan v. City of New* York, https://www.muslimadvocates.org/ (consulté le 22 juillet 2018).

[289] L. VANDERKELEN, *Le "Plan Canal" de Jan Jambon inquiète les associations*, février 2016, www.lalibre.be (consulté le 23 juillet 2018).

[290] Tel que le bourgmestre de Vilvorde, accompagné de nombreux experts antiterroristes et policiers.

[291] Ce qui dépasse largement les listes de l'Ocam des « foreign fighters »…, voir D. DE BLOCK, *Plan antiterroriste de Jambon : tous suspects ?*, Bruxelles, février 2016, www.solidaire.org (consulté le 22 juillet 2018).

[292] LA REDACTION, *Plan Canal : Jan Jambon veut analyser la consommation des domiciles dans les zones radicalisées*, février 2016, www.lalibre.be (consulté le 23 juillet 2018).

[293] 'Tous les propriétaires qui ont acheté une maison monofamiliale à l'époque et l'ont subdivisée en appartements pour amortir le prêt hypothécaire sans l'avoir signalé sont ainsi dans le collimateur', voir D. DE BLOCK, *op. cit.*

Ensuite, notons que l'exercice d'un contrôle démocratique et judiciaire n'est pas garanti. De fait, bien que le plan Jambon prévoit un renforcement du personnel juridique, la majorité de ces renforts ne concerne que le parquet fédéral et le ministère public, consolidant ainsi la domination du pouvoir exécutif sur le pouvoir judiciaire. Bien que crucial, « le rôle des juges d'instruction est absent et complétement sous-estimé », mettant ainsi en péril la transparence et le contrôle de la légalité des méthodes d'enquête.[294]

Par ailleurs, les effets néfastes de cette politique pourraient également nous laisser perplexe, en ce que des stigmatisations répétées sur la communauté musulmane et les habitants des zones concernées sont susceptibles de provoquer des tensions, voire un déséquilibre supplémentaire dans l'amélioration des relations humaines dans notre pays. La conséquence de ce plan risque grandement d'étiqueter l'ensemble des mosquées et éventuellement la totalité de la communauté musulmane. Ceci ne soutiendrait pas les efforts d'intégration mais, au contraire, nourrirait de nouveau la plaidoirie des enrôleurs prêchant un message d'opposition « eux contre nous ».[295] Enfin se pose la question légitime de l'efficacité réelle du plan – élément tant capital que délicat que nous aborderons dans le chapitre suivant. Bien que certaines enquêtes se soient terminées fin 2016 suite à un « manque de résultats », l'information au sujet des opérations des services de renseignement reste laborieuse à obtenir.

§6. La fermeture des lieux de culte et l'expulsion des imams radicaux en France

En France, le préfet – autorité administrative – s'est vu accorder le pouvoir de prononcer « la fermeture des lieux de culte »[296], et ce sans mandat judiciaire. Cette réalité pourrait amener à des situations de violation de la Convention européenne des Droits de l'Homme – en particulier vis-à-vis de la liberté de religion (inscrit à l'article 9 de la Convention), comme par exemple en cas d'adoption de mesures disproportionnées. En effet, « la fermeture de lieux de culte à cause des actes de *certaines* personnes aurait des résultats punitifs et stigmatisant pour les communautés religieuses *entières* concernées »[297]. Bien que la Cour EDH ait à plusieurs reprises

[294] D. DE BLOCK, *ibidem.*
[295] D. DE BLOCK, *ibidem*.
[296] Fermeture prise sur le fondement de l'article 8 de la loi d'urgence : « autorisation de fermer les lieux de culte dans lesquels sont tenus des propos relevant d'une provocation à la haine, à la violence, ou faisant la promotion d'actes de terrorisme », voir J. MICKIEWICZ, *Fermeture de quatre mosquées aux prêches radicaux en Ile-de-France*, novembre 2016, www.lefigaro.fr (consulté le 25 juillet 2018).
[297] N. MUIZNIEKS, *op. cit*.

reconnu à toute personne le droit d'exercer paisiblement son culte, ces possibilités nouvellement libellées dans la loi[298] restent préoccupantes.

§7. Le cas du Japon

Pour terminer cette section axée sur la surveillance discriminatoire ciblée en fonction de la race, ethnie ou religion, nous aimerions exposer la situation du Japon. Dans cet archipel où à peine 1 à 5% de la population serait musulmane, une opération de surveillance systématique de grande envergure a été menée par l'Etat dans les mosquées, restaurants halal et autres associations islamiques de Tokyo.[299] En effet, une fuite de dossiers d'enquête a été publiée par le journaliste Ian Munroe en été 2016, et laisse entrevoir un constat effrayant, à l'apogée du profilage religieux : de véritables CV reprenant des « renseignements personnels, une description physique, les relations personnelles, la mosquée fréquentée, ainsi qu'une section intitulée 'soupçons' » ont été dressés par les services de renseignement japonais et révélés sur le net.[300] Dix-sept musulmans ont alors uni leurs forces et ont attaqué l'Etat pour « violation de leurs droits et libertés fondamentales », action rejetée à tous les stades de la procédure judiciaire. La Cour suprême a d'ailleurs affirmé que cette pratique de surveillance basée sur la religion était « nécessaire et inévitable » pour contrer la menace terroriste.[301] En conclusion, ce phénomène de fichage ethnoreligieux n'a pas sa place dans nos sociétés, et ce qu'il soit le résultat de l'influence des stéréotypes sur la communauté musulmane au Japon, ou qu'il s'explique par le manque d'indépendance de la justice japonaise vis-à-vis de l'Etat.[302]

Dans le chapitre suivant, nous examinerons de plus près la question de l'efficacité de ces mesures de surveillance, qu'elles soient ciblées ou généralisées. Nous étudierons les objectifs poursuivis par les autorités au travers de ces pratiques, ainsi que leurs effets pervers. Se posera alors la question de savoir si les avantages de ces politiques l'emportent sur leurs points faibles.

---

[298] Après l'article 6-1 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence, il est inséré un article 6-2 ainsi rédigé : « *Art. 6-2. – Le ministre de l'intérieur, pour l'ensemble du territoire où est institué l'état d'urgence, et le préfet, dans le département, peuvent ordonner la fermeture de tout lieu de culte lorsqu'il existe des raisons sérieuses de penser que ce lieu de culte constitue une menace pour l'ordre public, ainsi que la dissolution de l'association ou du groupement de fait responsable de ce lieu de culte* », voir Loi n° 2016-987, *op. cit.*

[299] G. MIHAELY, *Japon : des musulmans sous surveillance*, juillet 2016, www.causeur.fr (consulté le 24 juillet 2018).

[300] I. MUNROE, *Top court green-lights surveillance of Japan's Muslims*, juin 2016, www.aljazeera.com (consulté le 23 juillet 2018).

[301] C. LE BRECH, *Au Japon, des musulmans surveillés sous couvert de lutte contre le terrorisme*, juillet 2016, http://geopolis.francetvinfo.fr (consulté le 24 juillet 2018).

[302] I. MUNROE, *op. cit.*

CHAPITRE 2. Questionnement sur l'efficacité des mesures de surveillance

Qu'il s'agisse d'une forme de surveillance généralisée ou de profilage ethnique, racial ou religieux, ces pratiques sont largement répandues en l'Europe, voire dans le monde entier. A travers ces méthodes, les citoyens, ciblés ou non, font souvent l'objet d'une attention disproportionnée de la part de la police, des services de renseignement ou du gouvernement. Malgré la hausse de leur utilisation, il n'existe pourtant aucune preuve du réel fonctionnement de ces pratiques en termes de lutte antiterroriste.[303] L'efficacité d'une technologie, d'un système ou d'un programme se définit en fonction de « la mesure dans laquelle elle favorise directement l'objectif recherché ».[304] Il existe certes une difficulté à la mesure du progrès de cette « guerre globale du terrorisme ».[305] Néanmoins, plusieurs auteurs, tels que le professionnel en sécurité informatique et écrivain américain Bruce Schneier, attestent ouvertement que la surveillance n'est pas à même de stopper les attaques terroristes.[306] Joseph Cannataci, rapporteur spécial de l'ONU présenté *supra*, est également très critique face à ces ingérences importantes dans les droits et libertés fondamentales, avant tout « fondées sur la psychologie de la peur » plutôt que sur leur efficacité.[307] Dans ce chapitre, nous allons étudier les différentes conséquences des intrusions décrites au chapitre précédent.

Premièrement, selon de nombreuses sources, les mesures de lutte antiterroriste s'avèrent être tout simplement inefficaces. Lorsque les gouvernements ou services de renseignement européens ou américains sont interrogés au sujet de l'utilité concrète des vastes programmes de surveillance, ceux-ci rencontrent des difficultés à justifier de façon précise sa plus-value et se satisfont de scénarios vagues et timides pour en exposer les bienfaits.[308] M. Cannataci, dans un rapport datant de mars 2017[309], dénonce l'adoption de nombreuses lois liberticides et inefficaces à travers l'Europe et la qualifie de « *gesticulation politique* » : « *politiques qui souhaitent être vus en train*

---

[303] R. NEILD, R. DELSOL et I. GORIS, *La question du profilage ethnique en Europe*, Open Society Justice Initiative, 2015.

[304] En effet, les autorités doivent juger si « *a given level of effectiveness is sufficient to proceed with the use or deployment of a given technology, system, or program* », cité par NATIONAL RESEARCH COUNCIL, *op. cit.*, point 1.8.2.

[305] D. COLE, « Are we safer? », in *The New York Review of Books*, vol. 53, n° 4, Georgetown University Law Center, mars 2006.

[306] B. SCHNEIER, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, mars 2015.

[307] C. AUFFRAY et Z. WHITTAKER, *La surveillance de masse fonctionne-t-elle? Rien ou presque ne le prouve*, mars 2017, http://www.zdnet.fr (consulté le 31 juillet 2018).

[308] F. MACHEREZ, *La surveillance de masse ne peut pas stopper les attaques terroristes*, juin 2015, https://www.vice.com (consulté le 31 juillet 2018).

[309] J. CANNATACI, *Report of the Special Rapporteur on the right to privacy*, Human Rights Council, 34th session, A/HRC/34/60, mars 2017.

de faire quelque chose, même si les lois ne fonctionnent pas vraiment dans la pratique ».[310] Selon lui, en effet, les preuves concernant l'efficacité ou la proportionnalité de certaines mesures européennes extrêmement intrusives se font rares. De nombreux faits renforcent ce constat. Notons entre autres l'attentat terroriste au camion-bélier à Nice qui a eu lieu malgré la prolongation de l'état d'urgence, les innombrables perquisitions[311] et interpellations effectuées suite aux attentats de 2015 dont l'issue et la rentabilité se sont « rapidement amenuisés »[312], ou encore l'inefficacité des « fichiers S » – pratique française consistant à suivre des personnes surveillées judiciairement – en ce que de nombreux djihadistes affiliées à EI faisant l'objet d'une telle surveillance n'ont malgré tout pas été empêchés d'agir[313], etc. Par ailleurs, des erreurs d'interprétation peuvent se produire, et engendrer des conséquences morales désastreuses : pensons à Fayçal Cheffou, confondu avec l' « homme au chapeau » des attentats de Zaventem au travers des caméras de surveillance placées dans le quartier Maelbeek.[314] En outre, la technique du profilage, en tentant de dresser des « profils-type à risque » au moyen de multiples données personnelles telles que les antécédents socio-économiques, la classe sociale, l'origine ethnique, l'âge, le sexe, l'éducation etc, s'est révélée totalement improductive. En effet, les experts conduisant ce genre de recherches en sont venus à la même conclusion : le profilage est un outil peu fiable pour repérer les terroristes potentiels.[315] Qui aurait pu par exemple prédire la radicalisation et le passage à l'acte de Muriel Degauque, femme blanche catholique de 38 ans aux cheveux blonds, ou de Nizar Trabelsi, ancienne star de football européenne ?[316] Les caractères démographiques des profils terroristes sont si divers que de nombreux chercheurs ont renoncé à prédire les suspects de cette menace. Ainsi, ils suggèrent de se concentrer davantage sur les comportements suspects et non sur le profilage. Pour conclure, il est dès lors légitime de se demander si les réponses, parfois disproportionnées, apportées à la menace terroriste sont les plus adéquates.

---

[310] J. LAUSSON, *L'ONU appelle la France à arrêter de jouer la "carte de la peur"*, mars 2017, http://www.numerama.com (consulté le 31 juillet 2018).

[311] Plus de 3500 perquisitions dans les six mois qui ont suivi les trois attentats coordonnés du 13 novembre 2015 à Paris.

[312] F. VIGNAL, *Prolongation de l'état d'urgence : réponse à la menace terroriste ou « effet de communication » ?*, juillet 2016, https://www.publicsenat.fr (consulté le 31 juillet 2018).

[313] D. DE BLOCK, *op. cit.*

[314] HUMAN RIGHTS WATCH, *Sources d'inquiétude : les réponses antiterroristes de la Belgique aux attaques de Paris et de Bruxelles*, Rapport, New York, 3 novembre 2016, pp. 45-47.

[315] Edwin Bakker, chercheur à l'Institut Clingendael de La Haye et auteur d'une étude récente, a tenté d'examiner près de 20 variables concernant les antécédents sociaux et économiques des suspects. En général, il a déterminé qu'aucun profil fiable n'existait. Dans une interview, Bakker a déclaré que de nombreux services de police locaux ont été lents à abandonner le profilage, mais que la plupart des agences de renseignement européennes ont conclu qu'il s'agissait d'un outil peu fiable pour repérer les terroristes potentiels, cité par C. WHITLOCK, *Terrorist proving harder to profile*, Washington Post Foreign Service, mars 2007, http://www.washingtonpost.com (consulté le 30 juillet 2018).

[316] C. WHITLOCK, *ibidem.*

Deuxièmement, les techniques de surveillance et de renseignement peuvent être, selon le cas, trop ou trop peu englobantes.[317] D'un côté, au cœur de ce nouveau « paradigme de la prévention »[318], le succès de ces pratiques est extrêmement difficile à atteindre en ce que les informations recherchées par les autorités se doivent d'être filtrées parmi l'énorme quantité de données disponibles.[319] Lorsque l'on cherche une aiguille dans une botte de foin, ajouter plus de foin à la botte ne va pas simplifier la recherche de l'aiguille[320]. Au contraire, en suspectant un groupe entier d'individus, nous dispersons de manière inefficace les faibles ressources attribuées au maintien de l'ordre et noyons l'information.[321] Ainsi, aux Etats-Unis comme en Europe, de multiples stratégies agressives d'arrestation et de poursuite se sont déjà introduites dans la vie privée d'un nombre incalculable de personnes : empreintes digitales [322], audiences, interpellations, assignations à résidence, perquisitions[323], détention préventive, "*national security letters*" adressées aux entreprises[324]… sans aboutir à quelconque résultat concret. D'un autre côté, ces techniques ne sont pas suffisamment inclusives, et peuvent dès lors laisser échapper des cas qui, sans correspondre au « profil-type » dressé, mériteraient néanmoins d'être étudiés.[325] Ainsi, le fait d'observer une masse d'innocents en fonction de leur apparence ou religion, détourne l'attention des forces de l'ordre concernant des personnes réellement dangereuses. De plus, de nombreux chercheurs rappellent que les groupes terroristes sont constamment à la recherche de tactiques inédites dans le but de prendre les forces de l'ordre au dépourvu : *« One guiding principle for terrorist groups is to always maintain the psychological edge and the upper hand by doing things that are surprising to the enemy* ».[326] C'est ainsi qu'ils affirment par exemple avoir décelé une augmentation du recrutement de femmes et

---

317 OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, op. cit.,* p. 21.

318 L. BERGMAN, E. LICHTBLAU, S. SHANE et D. VAN NATTA Jr., « Spy Agency Data after Sept. 11 Led FBI to Dead Ends », in *The New York Times*, janvier 2006, cité par D. COLE, *op. cit.*

319 NATIONAL RESEARCH COUNCIL, *Protecting Individual Privacy in the Struggle Against Terrorists : A Framework for Program Assessment*, Washington DC, The National Academies Press, 2008, Executive Summary.

320 EUROPEAN LIBERTIES PLATFORM, *Safe and Sorry*, *op. cit.*

321 R. NEILD, R. DELSOL et I. GORIS, *op. cit.*.

322 Within the US, Attorney General John Ashcroft repeatedly promoted what he labeled a *new* "paradigm of prevention" in law enforcement. (…) The US must act preemptively to prevent the next attack from occurring. On this theory, the administration subjected 80,000 Arab and Muslim immigrants to fingerprinting and registration, sought out 8,000 Arab and Muslim men for FBI interviews, and imprisoned over 5,000 foreign nationals in antiterrorism preventive detention initiatives, cité par D. COLE, *op. cit.*

323 En France, en deux mois, plus de 3200 perquisitions ont été conduites, 400 personnes interpellées et 400 assignées à résidence, mais une seule personne a été mise en examen pour terrorisme, cité par AMNESTY INTERNATIONAL, « Des vies bouleversées (…) », *op. cit.*, pp. 10 et s.

324 « These letters, issued without judicial review, require Internet and telecommunications companies and financial institutions to disclose information about their customers. The letters prohibit the recipients from telling anyone about the FBI's request », cité par D. COLE, *op. cit.*

325 OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, op. cit.,* p. 21.

326 a déclaré John Horgan, senior research fellow at the Center for the Study of Terrorism and Political Violence at the University of St. Andrews in Scotland, cité par C. WHITLOCK, *op. cit.*

d'enfants dans les deux dernières années.[327] Les menaces viennent d'horizons divers et sont conscientes des profils-types dressés et ont appris à les contourner. Pensons par exemple à la méthode PNR (détaillée *supra*) : certaines données sensibles, telles que la préférence alimentaire, sont récoltées dans le but d'identifier la conviction religieuse du passager. Pourtant, il est raisonnablement rationnel de penser qu'une personne mal intentionnée se garderait de révéler ce genre d'information. *In fine*, à défaut d'exclure les informations sensibles de cette récolte massive de données, ne seraient touchés que des individus innocents, sur base de leur unique croyance religieuse, utilisant ces services sans manigance aucune.[328]

Troisièmement, plusieurs éléments portent à croire que ces mesures de sécurité et de surveillance – plus particulièrement le profilage ethnique ou religieux – seraient même contre-productives, suscitant plus d'effets pervers que de résultats positifs.[329] En effet, la perpétuation, par les forces de l'ordre et services de lutte antiterroriste, de stéréotypes sociaux et raciaux en lieu et place de leur rejet encourage la banalisation et, partant, la consolidation de ces stéréotypes négatifs sur les minorités à travers nos sociétés.[330] En violant le principe fondamental de non-discrimination, cette approche crée et renforce la stigmatisation de minorités entières – telles que la communauté musulmane – et les assimile à des criminels ou terroristes potentiels, immigrés clandestins ou menaces pour la société. En donnant ainsi une « aura de légitimité »[331] à ces violations, ces attitudes engendrent, selon nous, trois problèmes majeurs. Tout d'abord, il est possible de voir apparaître des révoltes, émeutes et autres violences suite à ces formes de discriminations illégitimes.[332] Ce niveau accru d'agressivité et d'hostilité entre les communautés visées et les forces de l'ordre mène à une escalade de conflits[333], ce qui met en danger la sécurité de la population toute entière – bravant ainsi contradictoirement l'objectif initial de ces mesures.[334] Ensuite, ces dispositions difficilement justifiables et ce manque de résultats criant risquent, sur le long terme, d'ébranler la confiance

---

[327] C. WHITLOCK, *ibidem*.

[328] S. PEYROU, *L'accord PNR entre l'Union et le Canada (…)*, *op. cit.*

[329] OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, op. cit.,* p. 20.

[330] OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, ibidem,* pp. 11 et 20.

[331] R. NEILD, R. DELSOL et I. GORIS, *op. cit.*

[332] Pour différents exemples, voir D. WADDINGTON, F. JOBARD et M. KING, *Rioting in the UK and France – 2001–2008 : A comparative analysis,* Cullompton, Willan, 2009, p. 242 ; H. LAGRANGE, « Après Villiers-le-Bel : quand on veut expliquer l'inexplicable », in *Esprit*, Janvier 2008, p. 155–156, cités par OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, op. cit.,* p. 21.

[333] ONTARIO HUMAN RIGHTS COMMISSION, *Paying the Price: The Human Cost of Racial Profiling*, Toronto, Ontario Human Rights Commission, 2003, cité par OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, ibidem,* p. 21.

[334] OPEN SOCIETY JUSTICE INITIATIVE, *(…) les contrôles d'identité à Paris, ibidem,* p. 11.

placée en la police et les autorités par rapport au traitement égal devant la loi.[335] En effet, nous assistons progressivement à une méfiance envers le système de la justice pénale.[336] En doutant de la loyauté et de l'efficacité des actions policières et sécuritaires, les citoyens questionnent de plus en plus la légitimité du pouvoir des autorités face au public.[337] Enfin, suite à ces surveillances disproportionnées et cette perte de légitimité généralisée, la contre-productivité de ces pratiques se fait sentir au niveau du faible soutien populaire pourtant nécessaire dans la lutte contre la radicalisation.[338] L'état de coopération entre les communautés et les acteurs luttant contre la menace terroriste n'est ainsi plus à même de combattre activement l'embrigadement djihadiste.[339] Si l'on en croit les arguments précédents, peut-être serait-il plus profitable de revoir nos priorités et oublier nos préjugés, afin de traiter ces communautés comme nos alliés dans cette lutte, et non comme des menaces.

Pour conclure, les autorités dressent progressivement le constat suivant : l'état d'urgence et les mesures antiterroristes, davantage maintenus pour des raisons *émotionnelles* plutôt qu'*opérationnelles*, ne sont plus efficaces.[340] C'est au moyen d'actions et procédures policières et judiciaires *ordinaires* que les attentats sont effectivement déjoués.[341] Il semblerait ainsi que le besoin se trouve plutôt du côté d'une meilleure compréhension et utilisation des techniques d'information dont nous disposons, et non dans la récolte infinie de données aléatoires.[342] Par ailleurs, comme nous le verrons dans le chapitre suivant, une solution pourrait plutôt consister en la mise en place d'un service de coopération, de déradicalisation et de réinsertion sociale.[343] En effet, comme nous le dit Marc Trévidic, ancien juge antiterroriste français : « une idéologie ne se combat pas par le Code pénal ».[344]

---

[335] OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, ibidem,* p. 20.

[336] OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, ibidem,* p. 11.

[337] J. MILLER, N. BLAND et P. QUINTON, *The Impact of Stops and Searches on Crime and the Community*, London, Home Office, 2000 ; R. WEITZER et S. A. TUCH, « Determinants of Public Satisfaction », in *Police Quarterly*, 2007 ; J. MILLER *et al.*, *Public opinions of the police: The influence of friends, family and the media*, Washington, U.S. Department of Justice, 2004 ; D. P. ROSENBAUM *et al.*, « Attitudes toward the police: The effects of direct and vicarious experience », in *Police Quarterly,* 2005, cité par OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, ibidem,* p. 20.

[338] D. DE BLOCK, *op. cit.*

[339] D. DE BLOCK, *ibidem.*

[340] T. LEGRAND, « Etat d'urgence permanent ? », in *France Inter – l'Edito politique*, juin 2017, https://www.franceinter.fr/ (consulté le 31 juillet 2018).

[341] Ainsi, aux Etats-Unis, tous les succès récents annoncés par la N.S.A sont venus de surveillances *classiques* des cibles. Malgré de grands espoirs, le programme de surveillance de la N.S.A. n'a pas stoppé une seule attaque de terrorisme majeure. Par exemple, un des terroristes du Marathon de Boston était déjà une cible du F.B.I., cité par EUROPEAN LIBERTIES PLATFORM, *Safe and Sorry*, *op. cit.*

[342] EUROPEAN LIBERTIES PLATFORM, *Safe and Sorry*, *ibidem*.

[343] D. DE BLOCK, *op. cit.*

[344] D. DE BLOCK, *ibidem.*

CHAPITRE 3. Solutions, alternatives et pistes d'action

Section 1. Dénonciation des dérives en lieu et place de leur banalisation

La première étape du changement consiste tout d'abord en la prise de conscience suivie de la reconnaissance publique de l'existence d'un problème[345] : la surveillance de masse et les différentes mesures de lutte antiterroriste limitent disproportionnellement nos droits et libertés. Plusieurs initiatives existent, plusieurs organisations se manifestent afin de défendre nos intérêts. Chez nous, c'est le cas par exemple d'Amnesty International[346], Human Rights Watch[347], la Ligue des Droits de l'Homme[348], Reporters sans frontières[349], Creis Terminal[350], la Quadrature du Net[351], et bien d'autres. Ces mouvements visent premièrement à sensibiliser la population, à dénoncer ces pratiques largement acceptées, pour ensuite approfondir l'examen des normes juridiques et politiques, et amener les organes européens à constater ces dangers et à incorporer dans leurs stratégies et législations des « garde-fous » contre ces dérives.[352] Ce travail de mise en conformité de toutes ces mesures de lutte antiterroriste avec les protections inscrites dans la Charte des Droits Fondamentaux de l'Union se révèle certes ambitieux et épineux. Néanmoins, nous espérons que les institutions nationales et européennes, grâce à l'appui de la société civile, des associations et des partis politiques, accorderont un « intérêt constant et une attention sourcilleuse » à cet enjeu défiant toute priorité.[353] Par ailleurs, la normalisation de la surveillance de masse, s'observant directement par le biais des nouvelles technologies que nous utilisons quotidiennement, est également extrêmement dangereuse. Pensons notamment à la reconnaissance faciale abordée ci-dessus, aux données de géolocalisation, aux enregistrements et stockages de nos photos et fichiers audios… Ce scannage perpétuel ne doit pas devenir la norme : soutenir ces mouvements de dénonciations est un premier pas vers une évolution respectueuse de notre vie privée et une protection effective de nos données personnelles.[354]

---

345 OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, op. cit.,* p. 11.

346 ONGI protégeant les droits humains à travers le monde de manière pacifique, en dénonçant les injustices.

347 ONGI défendant les droits de l'homme et le respect de la Déclaration universelle des droits de l'homme.

348 Association visant à l'observation, la défense et la promulgation des droits de l'homme, dans tous les domaines de la vie publique.

349 ONGI reconnue d'utilité publique en France, luttant en faveur de la liberté de la presse et la protection des sources journalistiques.

350 Centre de Coordination pour la Recherche et l'Enseignement en Informatique et Société.

351 Association de défense des droits et libertés des citoyens sur Internet fondée en 2008 intervenant dans les débats concernant la liberté d'expression, le droit d'auteur, la régulation du secteur des télécommunications, ou encore le respect de la vie privée sur Internet.

352 R. NEILD, R. DELSOL et I. GORIS, *op. cit*.

353 M.-L. BASILIEN-GAINCHE, *op. cit.*, p. 15.

354 A. TIELENS, *op. cit.*

Section 2. Importance de l'actualisation, la modernisation et l'adaptation des outils juridiques

Le droit doit vivre avec son temps. En effet, celui-ci ne peut se permettre d'être dépassé par les avancées technologiques, au risque de voir apparaître un Etat de non-droit, qui mènerait inévitablement à l'obsolescence juridique, à l'anarchie et à la disparition pure et simple du respect de nos droits et libertés. C'est l'objectif qu'a par exemple suivi le RGPD (abordé au Titre I) en développant le droit à l'oubli numérique[355] ou le droit à la portabilité des données[356] : adapter la réglementation des données personnelles aux défis de la numérisation – tels que par exemple les progrès aperçus dans le secteur de la « compression des données ».[357] Ces changements innovants et puissants[358] permettent au citoyen de mieux contrôler ses données personnelles et l'usage qui en est fait. Par ailleurs, de par leur dimension géopolitique, il faut espérer que l'approche européenne incitera un mouvement global et mondial dans le sens de la protection des données personnelles. Enfin, si certaines mesures se révèlent inefficaces (cf. Chapitre 2), en ce qu'elles ne permettent pas l'identification de réelles menaces tout en multipliant les conséquences négatives pour les citoyens, il est nécessaire de procéder à une réévaluation et à une réadaptation de ces outils. Pour ce faire, il est indispensable de mettre en place un suivi de ces pratiques, conduit par une autorité de contrôle extérieure et indépendante. Les travaux de recherche et de documentation commencent à faire leur apparition, afin de pousser à la concrétisation de ces suivis, comme par exemple le rapport de l'organisation Open Society Justice Initiative[359]. Ce genre d'analyse a pour avantage de mettre en évidence la « prévalence, l'ampleur, la gravité, les conséquences et le coût humain et financier » des différents types de surveillance, afin d'accompagner le suivi continu et indépendant de ces pratiques grâce à ces investigations.[360]

---

[355] « L'article 17 du Règlement investit toute personne concernée par un traitement de données à caractère personnel d'un droit à l'oubli numérique et à l'effacement. L'apport majeur de cette disposition est de fixer et les conditions d'exercice du droit à l'oubli numérique, notamment l'obligation qui est faite au responsable du traitement ayant rendu publiques des données à caractère personnel d'informer les tiers de la demande de la personne concernée d'effacer tout lien vers ces données ou les copies ou reproductions qui en ont été faites. », cité par CABINET ULYS, *GDPR – Article 17 – Droit à l'effacement ("Droit à l'oubli")*, *op. cit.*

[356] « L'article 20 confère à la personne concernée un nouveau droit : le droit à la portabilité des données. Ce dernier apparaît comme un droit d'accès amélioré, auquel est associée une exigence d'interopérabilité. L'objet du droit serait, selon l'exposé des motifs de la première proposition de Règlement '*de transmettre des données d'un système de traitement automatisé à un autre, sans que le responsable du traitement puisse y faire obstacle*'. Pour ce faire, il permet à la personne concernée de recevoir les données qu'elle a fournies au responsable du traitement dans un '*format structuré, couramment utilisé et lisible par machine*'. », cité par CABINET ULYS, *GDPR – Article 20 – Droit à la portabilité des données, ibidem*.

[357] L. RAPP, « Au-delà de la réforme : synthèse et propositions pour l'amélioration de la protection des données », in *Quelles protections des données personnelles en Europe?* (sous la dir. de I. DE LAMBERTERIE, A. STROWEL et C. CASTETS-RENARD), Bruxelles, Larcier, 2015, p. 178.

[358] L. RAPP, *ibidem*, p. 182.

[359] OPEN SOCIETY JUSTICE INITIATIVE, *(...) les contrôles d'identité à Paris, op. cit.*

[360] R. NEILD, R. DELSOL et I. GORIS, *op. cit*.

Section 3. Une victoire de l'intégration face à la stigmatisation

Comme évoqué au Chapitre précédent, il serait sûrement plus efficace de troquer notre tactique de profilage – n'engendrant que stigmatisation et division – contre un climat de coopération et d'intégration. Pour combattre une idée, il serait intéressant de prendre le problème à la source, plutôt que d'accroître la surveillance de groupes entiers d'individus. Le « plan canal », par exemple, ne prévoit aucune mesure de prévention à la radicalisation.[361] Pourtant, un projet pluridisciplinaire de collaboration entre familles, écoles et associations luttant ensemble contre l'embrigadement djihadiste et favorisant la réinsertion sociale serait plus puissant que l'exploitation de préjugés.[362] Les violations des droits humains par la police et les services de renseignements n'en seraient que diminuées, respectant ainsi les engagements internationaux conclus entre autres par la Belgique.[363] Notons à ce sujet que la Belgique n'a pas encore lancé le « plan interfédéral de lutte contre le racisme » qu'elle s'était pourtant engagée à adopter en 2001 à Durban lors de la conférence mondiale contre le racisme.[364] En peinant de la sorte à dénoncer ce phénomène avec la ferveur nécessaire tout en continuant à pratiquer la politique de l'autruche, nos sociétés connaissent une régression en termes de protection des droits fondamentaux.[365] Pourtant, l'Europe semble se soucier du respect du pluralisme :

« L'histoire de l'Europe lui confère un devoir de mémoire, de vigilance et de résistance face à la montée des phénomènes de racisme, de discrimination raciale, (…) de xénophobie, d'antisémitisme, d'islamophobie, d'antitsiganisme et d'intolérance, (…) et du déni, de la banalisation, de la justification ou de la légitimation publics de ceux-ci »[366].

Par ailleurs, un renforcement de la formation des forces de police en amont couplé à un meilleur contrôle de leur indépendance et du bien-fondé de leurs opérations en aval garantirait une baisse des « comportements policiers abusifs et discriminatoires ».[367] Pour conclure, il serait opportun d'envisager des mesures préventives à long terme dans le cadre de la lutte antiterroriste qui encourageraient la « cohésion de nos sociétés » et le « dialogue multiculturel et inter-religieux », en lieu et place de l'implantation de formes d'intolérance, d'hostilité et de rejet entre les communautés.[368]

---

[361] D. DE BLOCK, *op. cit.*
[362] D. DE BLOCK, *ibidem.*
[363] C. MACQ et S. VAN OUTRYVE, *op. cit.*, pp. 33 et 34.
[364] CENTRE INTERFEDERAL POUR L'EGALITE DES CHANCES, *op. cit.*, p. 27.
[365] CENTRE INTERFEDERAL POUR L'EGALITE DES CHANCES, *ibidem*, p. 27.
[366] COMMISSION EUROPEENNE CONTRE LE RACISME ET L'INTOLERANCE (ECRI) et CONSEIL DE L'EUROPE, *Recommandation de politique générale n°15 sur la lutte contre le discours de haine*, Strasbourg, mars 2016, p. 3.
[367] C. MACQ et S. VAN OUTRYVE, *op. cit.*, pp. 33 et 34.
[368] COMITE DES MINISTRES DU CONSEIL DE L'EUROPE, *Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme*, *op. cit.*

Section 4. Rétablissement des équilibres

Plusieurs déséquilibres peuvent être identifiés dans le cadre de la surveillance antiterroriste. Tout d'abord, nous remarquons l'apparition de plusieurs anomalies dans les rapports de force. Premièrement, la séparation des pouvoirs semble dépérir dans le contexte de la lutte antiterroriste. Des glissements de compétences du pouvoir législatif ou judiciaire vers le pouvoir exécutif sont en effet de plus en plus courants[369] : réglementations pénales purement gouvernementales, perquisitions ne nécessitant nullement un mandat judiciaire, concepts juridiques larges aux définitions vagues laissées à la bonne interprétation de ses destinataires, absence de contrôle législatif ou judiciaire extérieur et indépendant… La liste s'allonge, et il est temps de rétablir les garanties contre ces concentrations de pouvoir. Deuxièmement, la relation autorités publiques-citoyens se fragilise. La confiance aveugle en la légitimité d'un Etat qui protège les droits et libertés de ses citoyens s'amenuise chaque jour un peu plus, la balance entre droits fondamentaux et sécurité donnant majoritairement priorité à la seconde. Afin de surpasser cet environnement de contrôle et de méfiance omniprésents, la promotion d'une participation citoyenne accentuée dans les structures de décision démocratiques permettrait de lutter contre « les asymétries de pouvoir »[370]. Une garantie de transparence en matière de protection des données personnelles redonnerait confiance et légitimité à la puissance publique. Nous espérons que les objectifs du RGPD (cf. *supra*) seront fructueux à ce sujet. Ensuite, nous observons une démesure dans le développement des technologies de surveillance, prenant la forme d'une réelle industrie toujours plus performante, plus chère et plus intrusive. Dans le même registre, nous, individus, pourrions également repenser notre relation à la technologie. En effet, en reconsidérant les usages sociaux que nous faisons des nouvelles techniques de communication et d'information[371], nous éviterions de coopérer à cette surveillance de manière directe et volontaire.[372] Enfin, une régulation plus stricte de l'utilisation – souvent invisible – des données personnelles éviterait des détournements prenant souvent pour cibles des lanceurs d'alerte, mouvements citoyens, opposants politiques et défenseurs des droits de l'homme en tout genre.

---

[369] M. L. CESONI, « Terrorisme et involutions démocratiques », in *Rev. dr. pén. crim.,* vol. 82, n° 2, 2002*,* pp. 150 et s.

[370] B. BOUCHAT, *op. cit.*, p. 54.

[371] « La future maman cherchant un emploi tout en « twittant » son bonheur à ses proches et qui ne pourrait plus ainsi dissimuler son état, au risque de se voir opposer un refus systématique, le cadre supérieur ou le haut-fonctionnaire, candidats à une promotion et dont la vie personnelle imprudemment dévoilée sur Facebook, servirait de prétexte à une fin de non-recevoir, l'emprunteur ou l'assuré, porteurs de l'un de ces bracelets qui mesurent notamment le nombre de pas accomplis chaque jour et dont les performances physiques seraient étudiées pour justifier une réponse négative ? Ce monde est déjà là ; c'est le nôtre. », cité par L. RAPP, *op. cit.*, pp. 173 et 174.

[372] B. SCHNEIER, *op. cit*.

CONCLUSION

Dans ce travail, nous avons analysé en détails les enjeux de la problématique de la surveillance de masse et de la surveillance ciblée : techniques aujourd'hui omniprésentes au sein de nos sociétés dans le cadre du combat contre le terrorisme. Nous avons mis en avant l'équilibre délicat et intrinsèque à ce phénomène : celui tentant de balancer habilement la garantie de sécurité des citoyens et le respect de leurs droits fondamentaux – principalement le droit au respect de leur vie privée et la protection de leurs données personnelles. Ces droits fondamentaux, bien que non-absolus, sont en effet constamment menacés par des législations et des politiques renforçant la lutte antiterroriste.

Dans notre premier Titre, nous avons centralisé les constats caractéristiques principaux à cette question sous la forme d'un compte rendu tripartite : factuel, législatif et jurisprudentiel.

Premièrement, nous avons rappelé les grands axes de l'actualité de la menace, ainsi que les réponses fortes et parfois impulsives qui y sont apportées. Entre les attaques meurtrières, les révélations des lanceurs d'alerte, l'affaissement des relations diplomatiques et les prolongations de l'état d'urgence et de ses pouvoirs étendus, nous avons dressé le tableau du contexte qui se rapporte aujourd'hui à toute la matière de la surveillance antiterroriste. En effet, de plus en plus de mesures préventives « temporaires » viennent s'implanter profondément dans nos sociétés. Nous avons également mesuré l'ampleur économique et politique de la surveillance de masse pour les entreprises et « l'Etat surveillant ».

Deuxièmement, nous avons dressé un bilan législatif relatif à la protection des données personnelles, concomitant à l'essor de l'évolution numérique. Au niveau international, nous avons insisté sur le rôle clé détenu par la Charte des droits fondamentaux de l'Union européenne – en particulier par ses articles 7 et 8 consacrant respectivement deux droits distincts : respect de la vie privée et familiale, à distinguer de la protection des données à caractère personnel en tant que telle. Au-delà de celle-ci, plusieurs outils ont fait leur apparition. Ceux-ci sont tantôt symboliques (bien qu'affichant une solide force morale) – tels que les recommandations du Conseil de l'Europe, les Directives des Nations Unies, la Déclaration universelle des droits de l'homme ou encore les Lignes Directrices de l'OCDE –, tantôt juridiquement contraignants – tels que la Convention de Strasbourg n° 108 ou le Pacte international relatif aux droits civils et politiques. Au niveau européen, le progrès majeur se manifeste par l'abrogation et le remplacement de la directive 95/46/CE par le nouveau règlement européen 2016/679. Afin de palier à l'obsolescence de cette directive vis-à-vis de la protection des données

personnelles, le RGPD apporte des réponses renforcées aux nouveaux défis numériques, ainsi que, entre autres, des garanties en termes de cohérence, d'harmonisation européenne, de transparence, de proportionnalité, de responsabilité et de limitation dans la récolte et l'usage de ces données. Enfin, nous avons mené une courte étude comparée de législations nationales et constaté le durcissement généralisé des mesures antiterroristes au sein de la plupart des Etats membres de l'Union européenne.

Troisièmement, nous avons constaté que les juges des juridictions européennes soutenaient eux aussi ce mouvement de protection de la vie privée et des données personnelles, de respect des droits fondamentaux et de condamnation de la surveillance de masse. D'un côté, la Cour de justice de l'Union européenne a rendu plusieurs arrêts emblématiques et cohérents concluant à la « violation particulièrement grave » des articles 7 et 8 de la Charte, notamment en 2014 (*Digital Rights Ireland*), en 2015 (*Schrems*) et en 2016 (*Tele2*). La Cour a ainsi rappelé aux institutions européennes et aux Etats membres l'importance de la proportionnalité des atteintes aux droits fondamentaux, de l'existence d'un cadre protecteur contre les abus et de garanties spécifiques lors du transfert international des données personnelles récoltées. D'un autre côté, la Cour européenne des droits de l'homme s'est elle aussi préoccupée de ce système d'interception opaque et généralisé de données personnelles, et a entre autres prononcé deux arrêts phares en 2015 (*Zakharov*) et 2016 (*Szabo*). Dans ses développements, aboutissant à la violation de l'article 8 de la Convention européenne des droits de l'homme, la Cour a systématiquement conclu à l'absence de garanties adéquates et effectives suffisamment précises et complètes, l'absence de contrôle juridictionnel et a même réitéré l'application du critère de « stricte nécessité » condamnant les risques démesurés d'arbitraire. Dans les deux cas, les juges ont pu cerner les mêmes enjeux fondamentaux afin de défendre la forme démocratique de nos sociétés.

Dans notre second Titre, nous nous sommes consacrés à l'analyse progressive de différentes dérives substantielles identifiables en Europe et à l'échelle mondiale, pour ensuite s'atteler à une étude critique de l'efficacité de ces mesures de surveillance, et enfin tenter d'y apporter des solutions et de proposer des alternatives.

Au premier Chapitre, il a été question de recenser, développer et commenter les différentes dérives et les potentiels abus des mesures antiterroristes. Nous avons procédé en deux temps. Tout d'abord, nous nous sommes intéressés à la surveillance généralisée, c'est-à-dire celle qui, *a priori*, est susceptible de toucher tous les citoyens quels qu'ils soient. Nous avons par exemple détaillé le système du « Passenger Name Record » – récolte massive, proactive et préventive de données

personnelles des voyageurs dans le monde entier – et attiré l'attention sur le risque de suspicion généralisée. Cette polémique a pourtant été amortie par un avis de la CJUE du 26 juillet 2017 affirmant, contre toute attente, la validité implicite du système PNR. Nous avons également abordé la problématique des banques de données, en passant par les risques inhérents à la collecte des empreintes digitales, à l'interprétation des fiches de renseignement de « menaces potentielles » de la banque de données « Foreign Fighters Terrorism », au développement de la technologie de la reconnaissance faciale, ainsi que l'expansion des perquisitions dans l'intimité des citoyens – mesure d'enquête intrusive par excellence. Dans un second temps, nous avons creusé la question délicate des mesures de surveillance ciblée et discriminatoire. Cette réalité illégale – à savoir l'usage de stéréotypes raciaux, ethniques et religieux en vue de façonner et orienter les politiques antiterroristes – est néanmoins de plus en plus normalisée dans nos pratiques de lutte antiterroriste. A ce sujet, nous avons abordé les problématiques de contrôles d'identité au faciès, de la surveillance des mosquées et de la communauté musulmane d'une manière générale – en Belgique (« plan canal ») comme à l'étranger (affaire *Hassan*, cas du Japon) –, la fermeture des lieux de culte, etc. Nous avons conclu au laxisme excessif des législations antiterroristes et des formations policières, permettant la pérennité de tels traitements inégalitaires, le tout accompagné d'un pouvoir discrétionnaire souvent immodéré.

Dans un deuxième Chapitre, nous nous sommes penchés sur la question de l'efficacité des mesures antiterroristes étudiées ci-avant. Nous avons insisté sur trois principes inhérents à ces mesures de surveillance. Premièrement, nous avons soutenu l'inefficacité globale des lois liberticides adoptées par nos représentants, exemples à l'appui. En effet, l'élaboration de « profils-type » de la menace s'est avérée être totalement improductive, en ce qu'elle est malheureusement aléatoire et imprévisible. De plus, les ingérences disproportionnées dans nos droits fondamentaux ainsi que les risques d'erreurs en termes d'interprétation ont été mis en avant, accompagnés de leurs conséquences désastreuses. Deuxièmement, nous nous sommes aperçus que les échelles de surveillance n'étaient pas adaptées au risque réel du terrorisme. En effet, que le filet soit trop vaste – noyant ainsi l'information – ou trop étroit – permettant ainsi aux réelles menaces de passer entre ses mailles –, les ressources attribuées au maintien de l'ordre et à la lutte antiterroriste ne sont pas optimisées. Autrement dit, le déploiement de diverses méthodes de recherche, plus agressives et intrusives les unes que les autres, n'apportent pas de résultats à la hauteur de l'investissement financier et humain. Troisièmement, nous avons démontré que la technique du profilage ethnique, racial ou religieux s'avérait être particulièrement problématique d'un point de vue juridique, se révélait inefficace, contradictoire et même contre-productive. En effet, en se servant davantage de stéréotypes sociaux et raciaux en lieu et place de comportements objectifs dans la lutte préventive contre le terrorisme, ces

méthodes banalisent et, partant, renforcent les stigmatisations et la division présentes en germe dans nos sociétés. Pourtant, nous trouvons dommage d'atrophier les garanties de non-discrimination en échange de résultats fictifs et, dans la foulée, de se priver d'une coopération avec ces communautés qui se montrerait plus prometteuse en termes d'efficacité face à cet objectif commun. De plus, ces actions engendrent la hausse de l'insécurité – provoquant de l'ascension de nombreux conflits et rébellions – et détériorent la confiance et la légitimité placées entre les mains des autorités de police et de l'Etat, répondant ainsi à l'image du « pompier pyromane ». Enfin, cette analyse nous a permis de conclure que les actions et procédures policières et judiciaires ordinaires étaient finalement plus efficaces que les mesures renforcées de surveillance de masse et de profilage, tout en garantissant un meilleur équilibre entre la protection de nos droits fondamentaux et la lutte pour notre sécurité.

Dans un troisième et dernier Chapitre, nous avons salué et encouragé toutes formes de mobilisation, défense des libertés fondamentales et dénonciation des dérives des mesures de récolte de données personnelles. Aucun changement d'une société n'est envisageable sans l'information de ses politiques ni l'éducation de ses citoyens. Par ailleurs, le droit doit faire l'objet de contrôles et d'évaluations, en vue de continuellement s'adapter aux avancées technologiques, dans le but d'envisager tous les cas de protection possibles, tel que l'a fait le RGPD. De plus, nous avons exposé les bienfaits d'une intégration sociale accentuée au sein de nos sociétés pluralistes, en termes de coopération entre les communautés et de protection des droits humains. Enfin, nous avons exprimé nos doutes quant à une application correcte du principe de la séparation des pouvoirs, le pouvoir exécutif se voyant attribué des compétences de plus en plus extensives. A ce sujet, nous promouvons plus de transparence dans les procédures de surveillance couplée à une réévaluation de l'importance de l'apport citoyen afin de se défaire de ces asymétries de pouvoir et de cette méfiance intarissable.

Le terrorisme a fait ses premières apparitions il y a de cela des décennies, et il est probable qu'il existera malheureusement toujours, malgré l'appui technologique dont nous disposons aujourd'hui. Georges Orwell a dit en 1948 : « *Chaque génération se croit plus intelligente que la précédente et plus sage que la suivante* ». La question que nous devons nous poser est dès lors celle-ci : quelle réponse voulons-nous apporter à cette menace ? Préférons-nous combattre ce fléau en apprenant de nos erreurs et en défendant nos valeurs démocratiques et droits fondamentaux en toutes situations, ou préférons-nous risquer de basculer dans un Etat surveillant et sécuritaire, offrant ainsi une première victoire au terrorisme ?

BIBLIOGRAPHIE

LEGISLATION

Législation supranationale

- Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981, approuvée par la loi du 17 juin 1991, *M.B.*, 30 décembre 1993, p. 29023.
- Pacte international relatif aux droits civils et politiques, signé à New York le 16 décembre 1966, approuvé par la loi du 15 mai 1981, *M.B.*, 6 juillet 1983, p. 8806.
- Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, p. 5028.
- Déclaration universelle des droits de l'homme, adoptée par l'Assemblée Générale des Nations Unies, signée à New York le 10 décembre 1948.

Législation européenne

- 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, *J.O.U.E.*, L. 119/1, du 4 mai 2016.
- Règlement (CE) n° 2252/2004 du Conseil, du 13 décembre 2004, *établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres*, JO L 385, p. 1, tel que modifié par le règlement (CE) no 444/2009 du Parlement européen et du Conseil, du 28 mai 2009, JO L 142.
- Dir. (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L.119/89, du 4 mai 2016.
- Dir. (UE) n° 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers des passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *J.O.U.E.,* L.119/132, du 4 mai 2016.
- Dir. (CE) n° 2006/24 du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de service de communications électroniques accessibles au public ou de réseaux publics de communication et modifiant la dir. (CE) n° 2002/58, *J.O.C.E.*, L.105/54, du 13 avril 2006 (invalidée).
- Dir. (CE) n° 2004/82 du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *J.O.U.E.,* L.261/24, du 6 août 2004.
- Dir. (CE) n° 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E,* L.201/37, du 31 juillet 2002.

- Dir. (CE) n° 95/46 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, *J.O.C.E.*, L.281/31, du 23 novembre 1995.

Législation nationale belge

- Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme, *M.B.,* 9 mai 2016, p. 30567.
- Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017, p. 12905.
- Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016, p. 44717.
- Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme, *M.B.*, 9 mai 2016, p. 30567.
- Loi du 20 juillet 2015 visant à renforcer la lutte contre le terrorisme, *M.B.*, 5 août 2015, p. 49326.
- Loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, *M.B.*, 12 mai 2003, p. 25351.
- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.
- Loi du 5 août 1992 sur la fonction de police, *M.B.,* 22 décembre 1992, p. 27124.
- Loi du 7 juin 1969 fixant le temps pendant lequel il ne peut être procédé à des perquisitions, visites domiciliaires ou arrestations, *M.B.,* 28 juin 1969, p. 6470.
- A.R. du 21 juillet 2016 relatif à la banque de données commune *Foreign Terrorist Fighters* et portant exécution de certaines dispositions de la section 1er *bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police, *M.B.,* 22 septembre 2016, p. 63970.
- Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme, Avis du Conseil d'Etat, *Doc. parl.*, Ch. repr., sess. ord. 2015-2016, n° 1727/001.

Législation nationale étrangère

France

- Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste, *J.O.R.F.*, 22 juillet 2016, n° 0169.
- Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, *J.O.R.F.*, 4 juin 2016, n° 0129.
- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *J.O.R.F.*, 26 juillet 2015, n° 0171.

Etats-Unis

- USA Freedom Act of 2015, H.R. 2048.
- Judicial Redress Act of 2015, H.R. 1428, 130 Stat. 282.
- Privacy Act of 1974, 5 U.S.C. § 552a.

DOCUMENTS DES NATIONS UNIES

Conseil de Sécurité

- Résol. 2354 adoptée par le Conseil de Sécurité des Nations Unies, S/RES/2354, 24 mai 2017.
- Résol. 2370 adoptée par le Conseil de Sécurité des Nations Unies, S/RES/2370, 2 août 2017.

Rapporteurs spéciaux

- J. CANNATACI, *Report of the Special Rapporteur on the right to privacy*, Human Rights Council, 34th session, A/HRC/34/60, mars 2017.

Haut-Commissariat des Nations Unies aux droits de l'homme

- HAMMARBERG (T.) (Commissaire aux droits de l'homme du Conseil de l'Europe), *Droits de l'homme en Europe : la complaisance n'a pas sa place – Chronique des droits de l'homme*, Edition du Conseil de l'Europe, Strasbourg, octobre 2011.

DOCUMENTS DU CONSEIL DE L'EUROPE

- CONSEIL DE L'EUROPE, *La Convention 108 modernisée : aperçu des nouveautés*, mai 2018, www. rm.coe.int/ (consulté le 2 juillet 2018).
- CONSEIL DE L'EUROPE, *Rapport explicatif*, Strasbourg, 10.X.2018.
- CONSEIL DE L'EUROPE, *Communiqué de presse – Améliorer la protection des données au niveau mondial: le Conseil de l'Europe met à jour sa convention phare*, Elseneur (Danemark), 18 mai 2018, www.rm.coe.int/ (consulté le 12 juillet 2018).
- MUIZNIEKS (N.), *Lettre du Commissaire aux droits de l'homme du Conseil de l'Europe au Sénat français*, Strasbourg, Conseil de l'Europe, 10 juillet 2017.
- COMMISSION EUROPEENNE CONTRE LE RACISME ET L'INTOLERANCE (ECRI) et CONSEIL DE L'EUROPE, *Recommandation de politique générale n°15 sur la lutte contre le discours de haine*, Strasbourg, mars 2016.
- COUNCIL OF EUROPE, *Mass surveillance – Who is watching the watchers?*, Editions du Conseil de l'Europe, Strasbourg, mars 2016.
- SCHWIMMER (W.), "Préface", in *Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme* (sous la dir. du COMITE DES MINISTRES), Conseil de l'Europe, 2002.

DOCUMENTS DE L'UNION EUROPEENNE

Parlement européen

- PARLEMENT EUROPEEN, *Communication de presse – NSA : mettre fin à la surveillance massive ou faire face aux conséquences*, http://www.europarl.europa.eu, 12 mars 2014 (consulté le 10 juillet 2018).
- PARLEMENT EUROPÉEN, *EU-US 'Privacy Shield' for data transfers: further improvements needed, MEPs say*, UE, Communiqué de presse, Bruxelles, 26 mai 2016.
- PARLEMENT EUROPEEN, *Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*, Résolution 2013/2188 (INI), 12 mars 2014, www.europarl.europa.eu. (consulté le 10 juillet 2018).
- PARLEMENT EUROPEEN, *Résolution sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique*, Résolution, 9 mars 1982.

Commission européenne

- COMMISSION EUROPEENNE, *Protection de la vie privée – Protection des données à caractère personnel*, fiche informative, www.ec.europa.eu (consulté le 4 juillet 2018).
- COMMISSION EUROPEENNE, *Recommandation concernant une convention du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Recommandation, 29 juillet 1981.

AVIS DE COMMISSIONS

- COMMISSION DE LA PROTECTION DE LA VIE PRIVEE, *Avis n° 05/2015 sur le projet de loi visant à renforcer la lutte contre le terrorisme*, 25 février 2015, www.privacycommission.be (consulté le 5 juillet 2018).
- COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME, *Avis sur le suivi de l'état d'urgence,* Paris, assemblée plénière du 18 février 2016, http://www.cncdh.fr/ (consulté le 29 juin 2018).

COMMUNIQUES DE PRESSE

- Cour EDH (Unité de presse), *Fiche thématique – Protection des données personnelles*, juin 2018, www.rm.coe.int (consulté le 17 juillet 2018).
- CJUE, 21 décembre 2016, *Tele2*, Communiqué de presse n° 145/16, Luxembourg.

JURISPRUDENCE

Jurisprudence européenne

Cour européenne des Droits de l'Homme

- Cour EDH, 5e sect., 12 janvier 2016, *Szabo et Vissy c. Hongrie*, Req.n°37138/14.
- Cour EDH, Gr. Ch., 4 décembre 2015, *Roman Zakharov c. Russie*, Req. n°47143/06.
- Cour EDH, 12 janvier 2010, arrêt *Gillan et Quinton* c. *Royaume-Uni*.
- Cour EDH, Grande Chambre, 5 mai 2000, arrêt *Rotaru v. Romania.*
- Cour EDH, 6 septembre 1978, arrêt *Klass e.a. et autres c. Allemagne*.

- Cour EDH – DIVISION DE LA RECHERCHE, *Sécurité nationale et jurisprudence de la Cour européenne des droits de l'homme*, Editions du Conseil de l'Europe et de la Cour européenne des droits de l'homme, novembre 2013, www.echr.coe.int (consulté le 22 juin 2018).

Cour de justice de l'Union européenne / Cour de justice des Communautés européennes

- CJUE, 21 décembre 2016, *Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a*, affaire C-203/15.
- CJUE, 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, affaire C-362/14.
- CJUE, 16 avril 2015, *W.P. Willems c. Burgemeester Van Nuth*, affaires jointes C-446/12 et C-449/12.
- CJUE, Grande Chambre, 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, affaires jointes C-293/12 et C-594/12.
- CJUE, 8 avril 2014, *Commission/Hongrie*, affaire C-288/12.
- CJUE, 13 juin 2013, *Michael Schwarz c. Stadt Bochum*, affaire C-291/12.
- CJUE, 10 février 2009, *Irlande contre Parlement européen et Conseil de l'Union européenne*, affaire C-301/06.
- CJCE., 30 mai 2006, aff. jointes *Parlement européen c. Conseil de l'Union européenne* et *Commission des Communautés européennes*, C-317/04 et C-318/04.

- CJUE, Grande Chambre, avis 1/15 du 26 juillet 2017, ECLI:EU:C:2017:592.

Jurisprudence nationale étrangère

Allemagne

- C.C. fédérale allemande, arrêt n° 1 BvR 518/02, 4 avril 2006.

Etats-Unis

- US DISTRICT COURT (New Jersey), *Hassan v. City of New York – stipulation of settlement*, 4th May 2018, Case 12-CV-3401 (WJM)(MF), p. 14, https://ccrjustice.org/ (consulté le 24 juillet 2018).

DOCTRINE

Monographies

- BAUDRY (P.), SORBETS (C.) et VITALIS (A.), *La vie privée à l'heure des médias*, Bordeaux, Presses universitaires de Bordeaux, 2002.
- BENKLER (Y.), *The wealth of Networks : how social production transforms markets and freedom*, Yale, University Press, 2006.
- DAOUD (E.), *Le Safe Harbor est mort, vive le droit à la vie privée et à la protection des données!*, Dalloz actualité, octobre 2015.
- DE HERT (P.) et GUTWIRTH (S.), *Anthologie de la vie privée. Compilation d'articles, de législation et de jurisprudence concernant la protection de la vie privée et des données à caractère personnel pour la Belgique jusque 1998*, Bruxelles, Academic and Scientific Publishers, 2013.
- DE SCHUTTER (O.), *International Human Rights Law,* 2ème éd., Cambridge, Cambridge University Press, 2014
- FAYON (D.), *Géopolitique d'internet qui gouverne le monde ?*, Paris, Economica, 2013.
- FRANKLIN (B.), *The Works of Benjamin Franklin*, vol. VII (Letters and Misc. Writings 1775-1779), compiled and edited by John Bigelow, New York : G.P. Putnam's Sons, Knickerbocker Press, 1904.
- FRANCOU (L.) et VERREYCKEN (Q.), *Compte-rendu de : Armand Mattelart, André Vitalis, Le profilage des populations. Du livret ouvrier au cybercontrôle*, ENS de Lyon, 2014.
- HARCOURT (B.), *Against Prediction : Profiling, Policing, and Punishing in an Actuarial Age*, Chicago, University of Chicago Press, Chicago, 2007.
- HARCOURT (B.), *Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally*, University of Chicago Law Review, Chicago, 2004.
- JONES (C.) et HAYES (B.), *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, Secile, 2014.
- KENNEDY (R.), *Race, Crime, and the Law*, Pantheon, New York, 1997.
- LEE (N.), *Counterterrorism and Cybersecurity – Total Information Awareness*, 2nd ed., e-book, Springer, 2015.
- LEFEBURE (A.), *L'affaire Snowden – Comment les Etats-Unis espionnent le monde*, Paris, Editions La Découverte, 2014.
- MILLER (J.) *et al.*, *Public opinions of the police: The influence of friends, family and the media*, Washington, U.S. Department of Justice, 2004.
- MILLER (J.), BLAND (N.) et QUINTON (P.), *The Impact of Stops and Searches on Crime and the Community*, London, Home Office, 2000.
- MUIZNIEKS (N.), *Lettre du Commissaire aux droits de l'homme du Conseil de l'Europe au Sénat français*, Strasbourg, Conseil de l'Europe, 10 juillet 2017.
- NATIONAL RESEARCH COUNCIL, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, Washington DC, The National Academies Press, 2008.
- NEILD (R.), DELSOL (R.) et GORIS (I.), *La question du profilage ethnique en Europe*, Open Society Justice Initiative, 2015.
- ROCHELANDET (F.), *Économie des données personnelles et de la vie privée*, coll. Repères, Paris, La Découverte, 2010
- ROCHFELD (J.), Notes du colloque sur *"les biens numériques"* (sous la dir. de A. CHAIGNEAU et E. NETTER), Université d'Amiens, Paris, coll. CEPRISCA, 2014.

- SCHAUER (F.), *Profiles, Probabilities, and Stereotypes*, Harvard University Press, Cambridge (Mass.), 2003.
- SCHNEIER (B.), *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, mars 2015.
- TILLY (C.), *Coercion, capital, and European states,* AD 990-1990, Cambridge, Massachussets, Blackwell, 1990.
- TRULLEMANS (J.-L.), *Les actes de recherche de la preuve et les autres modes de preuve – Mise en oeuvre des méthodes particulières de recherche et de quelques autres méthodes d'enquête au sens de la loi du 6 janvier 2003*, Postal Mémorialis, Waterloo, Kluwer, 2004.
- WADDINGTON (D.), JOBARD (F.) et KING (M.), *Rioting in the UK and France – 2001–2008 : A comparative analysis,* Cullompton, Willan, 2009.
- ZEH (J.), TROJANOW (I.), MENASSE (E.) *et. al.* (Membres du collectif « WRITERS AGAINST MASS SURVEILLANCE »), *Pour une défense de la démocratie à l'ère numérique*, 2013, www.change.org (consulté le 25 juin 2018).

Contributions dans un ouvrage collectif

- BERGMAN (L.), LICHTBLAU (E.), SHANE (S.) et VAN NATTA Jr. (D.), « Spy Agency Data after Sept. 11 Led FBI to Dead Ends », in *The New York Times*, janvier 2006.
- CASTETS-RENARD (C.), « Introduction – Les enjeux et l'actualité de la protection des données personnelles en Europe », in *Quelles protections des données personnelles en Europe?* (sous la dir. de DE LAMBERTERIE (I.), STROWEL (A.) et CASTETS-RENARD (C.)), Bruxelles, Larcier, 2015.
- DELHAISE (E.) et FIEVET (C.), « Frontières intelligentes et nouvelles incriminations pénales: l'UE face à la problématique des "Foreign terrorist fighters" », in *Journal des tribunaux*, n° 6676, 11 février 2017.
- DE TERWANGNE (C.), « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », in *Quelles protections des données personnelles en Europe?* (sous la dir. de DE LAMBERTERIE (I.), STROWEL (A.) et CASTETS-RENARD (C.)), Bruxelles, Larcier, 2015.
- DE TERWANGNE (C.) et MOINY (J.-Ph.), « Rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », in *Rapport pour le Conseil de l'Europe*, Conseil de l'Europe, Strasbourg, juin 2011.
- DE TERWANGNE (C.) et MOINY (J.-Ph.), « Les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) face aux développements technologiques », in *Rapport pour le Conseil de l'Europe*, Strasbourg, novembre 2010.
- KREISSL (R.) et WRIGHT (D.), « European responses to the Snowden revelations », in *Surveillance in Europe,* New York, Routledge, 2015.
- MACQ (C.) et VAN OUTRYVE (S.), « Les droits fondamentaux à l'épreuve de la lutte contre le terrorisme », in *Etat des droits de l'homme en Belgique – Rapport 2016-2017* (sous la dir. de Ligue des droits de l'homme asbl), Bruxelles, 2017, www.liguedh.be (consulté le 28 juin 2018).
- PAP (A.), « Le profilage sur la base de l'appartenance ethnique et de la race dans la lutte contre le terrorisme, la répression et le contrôle aux frontières », in *Libertés civiles, justice et affaires intérieures*, Parlement européen, Bruxelles, novembre 2008.

- RAPP (L.), « Au-delà de la réforme : synthèse et propositions pour l'amélioration de la protection des données », in *Quelles protections des données personnelles en Europe?* (sous la dir. de I. DE LAMBERTERIE, A. STROWEL et C. CASTETS-RENARD), Bruxelles, Larcier, 2015.
- ROSENBAUM (D. P.) *et al.*, « Attitudes toward the police: The effects of direct and vicarious experience », in *Police Quarterly,* 2005.
- SCHWIMMER (W.), « Préface », in *Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme* (sous la dir. du COMITE DES MINISTRES), Conseil de l'Europe, 2002.
- WEITZER (R.) et TUCH (S. A.), « Determinants of Public Satisfaction », in *Police Quarterly*, 2007.

Articles de périodiques

- ADEN (H.), « L'Etat protecteur, mobilisation de nouveaux acteurs et repli sécuritaire. Les politiques de sécurité et de prévention en Allemagne dans les années 1990 », in *Déviance et Société*, 2001.
- BASILIEN-GAINCHE (M.-L.), « Une prohibition européenne claire de la surveillance électronique de masse », in *La Revue des droits de l'homme*, Actualités Droits-Libertés, 14 mai 2014
- BERNAERTS (M.), « Les transferts de données à caractère personnel entre l'Union européenne et les États-Unis : une valse à mille temps ? », in *R.D.C.,* 2017.
- CESONI (M. L.), « Terrorisme et involutions démocratiques », in *Rev. dr. pén. crim.,* vol. 82, n° 2, 2002.
- CLAVET (S.), « Les conséquences de l'accord Passenger Name Record sur la protection des droits fondamentaux en Europe », in *Droits Fondamentaux*, n°8, janvier 2010.
- COLE (D.), « Are we safer? », in *The New York Review of Books*, vol. 53, n° 4, Georgetown University Law Center, mars 2006.
- DUBUISSON (F.), « La Cour européenne des droits de l'homme et la surveillance de masse », in *Rev. trim. dr. h.*, n° 108/2016, Bruxelles, Anthemis, 2016, p. 872
- FOEGLE (J.-P.), « Chronique du droit "Post-Snowden" : La CJUE et la CEDH sonnent le glas de la surveillance de masse », in *La revue des droits de l'homme*, Actualités Droits-Libertés, 30 mars 2016.
- FOEGLE (J.-P.), « Sans doigt, ni loi : la CJUE donne son 'feu vert' à la biosurveillance », in *La Revue des droits de l'homme*, Actualités Droits-Libertés, juillet 2015.
- LAGRANGE (H.), « Après Villiers-le-Bel : quand on veut expliquer l'inexplicable », in *Esprit*, Janvier 2008.
- MILLIOT (V.), « L'oeil et la mémoire : réflexions sur les compétences et les savoirs policiers à la fin du XVIIIe siècle, d'après les "papiers" du lieutenant général Lenoir », in *Revue d'Histoire des Sciences Humaines*, n° 19, 2008.
- PARODI (M.), « De la discrimination statistique à la discrimination positive », in *Revue de l'OFCE, Centre de recherche en économie de Sciences PO*, OFCE, Presses de Science Po, éd. 2010/1 n° 112, 2010.
- PEYROU (S.), « Retour du balancier après le 'tout sécuritaire' : le printemps annoncé de la protection des données à caractère personnel », in *R.A.E.*, 2015.

- PEYROU (S.), « De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », in *R.A.E.*, 2013.

Cabinets d'avocats

- CABINET ULYS, *GDPR – Analyse détaillée*, www.gdpr-expert.eu (consulté le 2 juillet 2018).
- MUSLIM ADVOCATES, *Losing Liberty: the state of freedom 10 years after the Patriot Act*, California, october 2011.
- MUSLIM ADVOCATES, *Hassan v. City of New* York, https://www.muslimadvocates.org/ (consulté le 22 juillet 2018).

Notes de jurisprudence et conclusions générales

- BENOIT-ROHMER (F.), « Protection des données personnelles », note sous CJUE, arrêt Digital Rights Ireland, in *RTDE*, 2015.
- BOT (Y.), Concl. de l'avocat général, note sous CJUE, arrêt Maximilian Schrems c. Data Protection Commissioner, in *RTDE*, 2015.
- LABAYLE (H.), « La Cour de justice et la protection des données : quand le juge européen des droits fondamentaux prend ses responsabilités », note sous CJUE, arrêt Digital Rights Ireland, in *RTDE*, 2015.
- PAOLO MENGOZZI (M.), concl. générales CJUE présentées le 13 juin 2013, arrêt Michael Schwarz contre Stadt Bochum du 17 octobre 2013, X, 2013.
- PEERS (S.), « Data retention: a landmark court of justice's ruling. Will this saga continue and how ? », note sous CJUE, arrêt Digital Rights Ireland, X, 2014.
- PEYROU (S.), « Surveillance de masse : un coup d'arrêt aux dérives de la lutte antiterroriste », note sous CEDH, arrêt *Szabo et Vissy c. Hongrie*, janvier 2016, www.gdr-elsj.eu (consulté le 17 juillet 2018).

PUBLICATIONS EN LIGNE D'AUTEURS DE DOCTRINE

- BACH (G.), *Passagéierdaten : Schutz oder Gefor?*, 26 janvier 2015, https://csv.lu/ (consulté le 18 juillet 2018).
- LEMMENS (L.) et MEES (K.), *Un AR précise le fonctionnement de la banque de données 'Foreign Terrorist Fighters'*, Wolters Kluwer, 2016, https://legalworld.wolterskluwer.be (consulté le 27 juillet 2018).
- PEYROU (S.), *Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir !*, 28 juillet 2017, http://www.gdr-elsj.eu (consulté le 10 juillet 2018).
- PEYROU (S.)*, L'accord PNR entre l'Union et le Canada ne respecte pas, en l'état, la Charte des droits fondamentaux de l'UE, réflexions faisant suite aux conclusions de l'avocat général Mengozzi dans la demande d'avis 1/15*, 20 septembre 2016, http://www.gdr-elsj.eu (consulté le 19 juillet 2018).
- PEYROU (S.), *Diplomatie ou droits fondamentaux? Questions sur la conclusion de l'accord PNR entre les Etats-Unis et l'Union*, 3 mai 2012, www.gdr-elsj.eu (consulté le 12 juillet 2018).
- SABBAGH (D.), *Lecture critique de* B. HARCOURT, *op. cit.*, www.journals.openedition.org/ (consulté le 17 juillet 2018).
- SCHAUER (F.), *Profiles, Probabilities, and Stereotypes*, Harvard University Press, Cambridge (Mass.), 2003.
- TECHENE (V.), *L'accord UE/Canada sur le transfert de données de passagers aériens incompatible avec la Charte des droits fondamentaux de l'Union*, 31 juillet 2017, www.actualitesdudroit.fr (consulté le 3 juillet 2018).
- WERY (E.), *La Cour de justice va-t-elle interdire le transfert aux autorités US des données des passagers se rendant aux USA? L'avocat général le suggère*, 27 novembre 2005, www.droit-technologie.org (consulté le 9 juillet 2018).

ARTICLES DE PRESSE EN LIGNE

- AUFFRAY (C.) et WHITTAKER (Z.), *La surveillance de masse fonctionne-t-elle? Rien ou presque ne le prouve*, mars 2017, http://www.zdnet.fr (consulté le 31 juillet 2018).
- BEN (N.), *38 terroristes potentiels sont sous surveillance en Belgique*, mars 2018, www.lalibre.be (consulté le 26 juillet 2018).
- BODDAERT (M.), *Wikileaks – Ce que l'on sait des méthodes d'espionnage de la CIA*, Libération, 8 mars 2017, http://www.liberation.fr/ (consulté le 22 juin 2018).
- CENTER FOR CONSTITUTIONAL RIGHTS, *Settlement reached in NYPD Muslim Surveillance Lawsuit*, New York, avril 2018, https://ccrjustice.org (consulté le 24 juillet 2018).
- CNIL, *Reconnaissance faciale*, https://www.cnil.fr/ (consulté le 17 juillet 2018).
- COPPELIA, *Accord PNR (Passenger Name Record) avec les Etats- Unis : feu vert du Parlement européen*, avril 2012, https://europe-liberte-securite-justice.org (consulté le 13 juillet 2018).
- DE BLOCK (D.), *Plan antiterroriste de Jambon : tous suspects ?*, Bruxelles, février 2016, www.solidaire.org (consulté le 22 juillet 2018).
- DOLHEIN (A.), *Le premier rapporteur pour la défense de la vie privée de l'ONU, Joseph Cannataci, juge la surveillance au Royaume-Uni "pire" que dans "1984"*, 26 août 2015, http://reinformation.tv/ (consulté le 12 juillet 2018).
- EUROPAFORUM LUXEMBOURG, *Dossier PNR*, janvier 2015, http://www.europaforum.public.lu/ (consulté le 18 juillet 2018).

- EUROPAFORUM LUXEMBOURG, *Conseil JAI - Le ministre François Biltgen a salué la proposition de la Commission de procéder par voie de règlement uniforme en matière de protection des données*, 26 octobre 2012, http://www.europaforum.public.lu/ (consulté le 5 juillet 2018).
- GOLDMAN (A.) et APUZZO (M.) (The ASSOCIATED PRESS), *With cameras, informants, NYPD eyed mosques*, février 2012, https://www.ap.org/ (consulté le 23 juillet 2018).
- GREENWALD (G.), *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, 6 juin 2013, www.theguardian.com (consulté le 22 juin 2018).
- IBZ CRISISCENTRUM, *Sécurité publique – PNR,* 2017, https://crisiscentrum.be/ (consulté le 20 juillet 2018).
- LA REDACTION, *Plan Canal : Jan Jambon veut analyser la consommation des domiciles dans les zones radicalisées*, février 2016, www.lalibre.be (consulté le 23 juillet 2018).
- LAUSSON (J.), *L'ONU appelle la France à arrêter de jouer la "carte de la peur"*, mars 2017, http://www.numerama.com (consulté le 31 juillet 2018).
- LE BRECH (C.), *Au Japon, des musulmans surveillés sous couvert de lutte contre le terrorisme*, juillet 2016, http://geopolis.francetvinfo.fr (consulté le 24 juillet 2018).
- LEGRAND (T.), « Etat d'urgence permanent ? », in *France Inter – l'Edito politique*, juin 2017, https://www.franceinter.fr/ (consulté le 31 juillet 2018).
- MACHEREZ (F.), *La surveillance de masse ne peut pas stopper les attaques terroristes*, juin 2015, https://www.vice.com (consulté le 31 juillet 2018).
- MICKIEWICZ (J.), *Fermeture de quatre mosquées aux prêches radicaux en Ile-de-France*, novembre 2016, www.lefigaro.fr (consulté le 25 juillet 2018).
- MIHAELY (G.), *Japon : des musulmans sous surveillance*, juillet 2016, www.causeur.fr (consulté le 24 juillet 2018).
- MUNROE (I.), *Top court green-lights surveillance of Japan's Muslims*, juin 2016, www.aljazeera.com (consulté le 23 juillet 2018).
- PONCIAU (L.), *Déjà deux millions de passagers sont passés par le PNR*, 16 avril 2018, http://plus.lesoir.be/ (consulté le 20 juillet 2018).
- REES (M.), *Au Parlement européen, la commission Libe demande la suspension du Privacy Shield*, www.nextinpact.com, 12 juin 2018.
- ROSSI (T.), *L'ONU, nouvel adversaire de la surveillance de masse*, Libération, 15 mars 2017, http://www.liberation.fr/ (consulté le 3 juillet 2018).
- RTBF INFO, *Luc Hennart : "C'est une mauvaise idée de permettre les perquisitions de jour et de nuit",* décembre 2015, https://www.rtbf.be (consulté le 26 juillet 2018).
- RT FRANCE, *Assange à RT: "l'enjeu de la vie privé est perdu, la surveillance de masse est là pour de bon"*, 10 décembre 2015, https://francais.rt.com/ (consulté le 23 juin 2018).
- SNOWDEN (S.), *The UK has just legalized the most extreme surveillance in the history of western democracy*, Twitter, 17 novembre 2016 (consulté le 2 juillet 2018).
- STUPP (C.), *Le fichage des passagers aériens franchit une étape au Parlement européen*, juillet 2015, https://www.euractiv.fr/ (consulté le 18 juillet 2018).
- TIELENS (A.), *Les dérives de la reconnaissance faciale (opinion)*, avril 2018, www.lalibre.be (consulté le 27 juillet 2018).
- TRAVIS (A.), « Investogatory powers bill: the key points », in *The Guardian,* 4 novembre 2015, https://www.theguardian.com/ (22 juillet 2017).
- TUAL (M.), « L'essentiel de la loi sur le renseignement jugé conforme à la Constitution », in *Le Monde,* 23 juillet 2015, http://www.lemonde.fr/ (consulté le 3 juillet 2018).

- VANDERKELEN (L.), *Le "Plan Canal" de Jan Jambon inquiète les associations*, février 2016, www.lalibre.be (consulté le 23 juillet 2018).
- VIGNAL (F.), *Prolongation de l'état d'urgence : réponse à la menace terroriste ou « effet de communication » ?*, juillet 2016, https://www.publicsenat.fr (consulté le 31 juillet 2018).
- VILLEDIEU (A.-L.), *Données personnelles : la défense du droit à la vie privée face à la volonté des Etats membres d'imposer une surveillance généralisée*, mai 2017, www.lexplicite.fr (consulté le 14 juillet 2018).
- WHITLOCK (C.), *Terrorist proving harder to profile*, Washington Post Foreign Service, mars 2007, http://www.washingtonpost.com (consulté le 30 juillet 2018).

RAPPORTS et ETUDES

belges

- CENTRE INTERFEDERAL POUR L'EGALITE DES CHANCES, *Rapport annuel 2016 : pour une société inclusive, par où commencer ?*, Bruxelles, Unia, 2017.
- LIGUE DES DROITS DE L'HOMME, *Rapport 2015-2016*, Bruxelles, 2016, www.liguedh.be (consulté le 5 juillet 2018).
- LIGUE DES DROITS DE L'HOMME, *Rapport 2016-2017*, Bruxelles, 2017, www.liguedh.be (consulté le 28 juin 2018).

internationaux

- AMNESTY INTERNATIONAL, « Des mesures disproportionnées – L'ampleur grandissante des politiques sécuritaires dans les pays de l'UE est dangereuse », in *Rapport 2017*, Londres, 2017.
- AMNESTY INTERNATIONAL, *France. La prolongation de l'état d'urgence risque de normaliser des pouvoirs d'exception*, 16 décembre 2016, www.amnesty.fr (consulté le 7 juillet 2018).
- AMNESTY INTERNATIONAL, « France. Des vies bouleversées. L'impact disproportionné de l'état d'urgence en France », in *Rapport 2016*, Londres, 4 février 2016.
- COMMISSION EUROPEENNE CONTRE LE RACISME ET L'INTOLERANCE (ECRI) et CONSEIL DE L'EUROPE, *Recommandation de politique générale n°15 sur la lutte contre le discours de haine*, Strasbourg, mars 2016.
- EUROPOL, *EU Terrorism Situation and Trend Report (TE-SAT)*, 2016, www.europol.europa.eu/ (consulté le 27 juillet 2018).
- HUMAN RIGHTS WATCH, *Sources d'inquiétude : les réponses antiterroristes de la Belgique aux attaques de Paris et de Bruxelles*, Rapport, New York, 3 novembre 2016.
- NATIONAL RESEARCH COUNCIL, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, Washington DC, The National Academies Press, 2008.
- NATIONAL RESEARCH COUNCIL, *Protecting Individual Privacy in the Struggle Against Terrorists : A Framework for Program Assessment*, Washington DC, The National Academies Press, 2008, Executive Summary.
- ONTARIO HUMAN RIGHTS COMMISSION, *Paying the Price: The Human Cost of Racial Profiling*, Toronto, Ontario Human Rights Commission, 2003.
- OPEN SOCIETY JUSTICE INITIATIVE, *Police et minorités visibles : les contrôles d'identité à Paris*, Open Society Institute, New York, 2009.

- OPEN SOCIETY JUSTICE INITIATIVE, *Ethnic Profiling and Counter-Terrorism : Trends, Dangers and Alternatives*, juin 2006.
- ZEH (J.), TROJANOW (I.), MENASSE (E.) *et. al.* (Membres du collectif « WRITERS AGAINST MASS SURVEILLANCE »), *Pour une défense de la démocratie à l'ère numérique*, 2013, www.change.org (consulté le 25 juin 2018).

DIVERS

Interviews

- Interview de LAVENU (P.) (secrétaire national de la section Île-de-France du syndicat de police Alliance), DUVAL (V.) (Présidente de l'Union syndicale des magistrats (USM)), SCHLOSSER (J.-M.) (sociologue, ancien inspecteur de police, auteur d'une thèse sur les techniques de formation des policiers) et TROUVE (M.) (avocate pénaliste, membre du Syndicat national des avocats de France (SAF)), 12 janvier 2016, https://www.franceculture.fr/emissions/du-grain-moudre/menace-terroriste-la-police-t-elle-tous-les-droits?xtmc=Muižnieks&xtnp=1&xtcr=1 (consulté le 18 juillet 2018).
- Entretiens avec WATHELET (M.), Professeur de droit européen à l'Université Catholique de Louvain et avocat général à la Cour de justice de l'Union européenne, 2017-2018.

(Vidéo)conférences, discours et colloques

- ASSANGE (J.), *Sécurité ou surveillance : le droit à la vie privée et la sécurité anti-terroriste peuvent-ils coexister à l'âge digital ?*, Vidéoconférence depuis l'ambassade de l'Equateur à Londres, 20 décembre 2012.
- JUNCKER (J.-C.), « Discours sur l'état de l'Union 2016 : Vers une Europe meilleure – Une Europe qui protège, donne les moyens d'agir et défend », Discours autorisé, Strasbourg, le 14 septembre 2016, https://ec.europa.eu/ (consulté le 18 juillet 2018).
- ROCHFELD (J.), Notes du colloque sur *"les biens numériques"* (sous la dir. de A. CHAIGNEAU et E. NETTER), Université d'Amiens, Paris, coll. CEPRISCA, 2014.

Cours

- Cours de Contentieux européen, dispensé par WATHELET (M.), à l'Université Catholique de Louvain, aux étudiants de 2ème année de master en droit, année 2017-2018.

Documentaires et films

- EUROPEAN LIBERTIES PLATFORM, *Safe and Sorry – Terrorism & Mass Surveillance*, YouTube, https://www.youtube.com/watch?v=V9_PjdU3Mpo (consulté le 22 juin 2018).
- SMITH (A.), *On a plus de chance de gagner au loto que de mourir du terrorisme !*, www.youtube.com, 5 décembre 2015 (consulté le 8 juillet 2018).
- STONE (O.), film *Snowden*, 2 novembre 2016 (regardé le 15 mai 2018).

Mémoires

- BOUCHAT (B.), *Les mesures de lutte antiterroriste : une menace pour notre droit fondamental à au respect de la vie privée ?*, Université Catholique de Louvain, 2016-2017 (promoteur : M. VERDUSSEN).

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique **www.uclouvain.be/drt**