Droit et enjeu pénal à l'épreuve du renseignement numérique

Warren Azoulay

Droit pénal et procédure pénale/Renseignement numérique et juge judiciaire/Collecte de données et libertés individuelles

Droit et enjeu pénal à l'épreuve du renseignement numérique

Warren AZOULAY
Doctorant
Laboratoire de Droit privé et de sciences criminelles (EA 4690)
Aix-Marseille Université
Chercheur associé de l'ORDCS (MMSH, USR 3125)

Mots-clés : Loi renseignement / Commission nationale de contrôle des techniques de renseignement / CNCTR / Nouvelles technologies de l'information et de la communication / NTIC / Surveillance / Enquêtes incidentes / Collecte de données / Big data / Data mining

Introduction

1. (R)Evolution. La société connaissant aujourd'hui une transformation dont les technologies de l'information et de la communication sont le vecteur, le cyberespace et ses moyens modernes de communications ont pu être qualifiés d' *« outils d'anonymisations idéals doublés d'une capacité d'agir à distance, au-delà des frontières terrestres caractéristiques des limites d'action des services répressifs »*[1], une *« horrible convergence du monde physique et du monde virtuel »*[2] dans laquelle se seraient *« engouffrés »*[3] les terroristes. S'il est vrai que nous nous trouvons aux prémices d'une nouvelle ère, totalement interconnectée, et que la disparition du monde d'hier est amenée à poser des questions de sécurité redoutables[4], elles devront assurément

[1] Christian Aghroum, « Cyberterrorisme et sécurité des entreprises », *Sécurité et stratégie*, 2017, vol. 28, n° 4, p. 48.
[2] Barry C. Collin, « The Future of CyberTerrorism : Where the Physical and Virtual Worlds Converge », s.l., Institute for Security and Intelligence.
[3] C. Aghroum, « Cyberterrorisme et sécurité des entreprises », art cit, p. 48.
[4] Benoit Dupont et Olivier Hassid, « Le monde d'hier », *Sécurité et stratégie*, 2016, vol. 22, n° 2, p. 1.

être conjuguées avec celles relatives à la protection de la vie privée[5]. Une controverse féroce émerge alors, laquelle oppose les partisans d'un Internet décrit comme *« l'instrument de propagande privilégié des organisations terroristes et le principal lieu de radicalisation virtuelle »*[6] aux défenseurs des libertés individuelles voyant dans ces tentatives répétées d'encadrer les nouvelles technologies *« une insistance quasi paranoïaque sur les menaces potentiellement catastrophiques constituées par le cyberterrorisme »*[7].

2. Contexte. Partant de l'affirmation selon laquelle un Etat doit connaître ses adversaires pour pouvoir se défendre et protéger ses citoyens[8], la question de la surveillance suscite, dans un contexte soit d'effroi, soit post-Snowden suite aux révélations des écoutes de la National Security Agency, un intérêt jusqu'alors inégalé. Le printemps 2015 aura donc été celui du renseignement, alors que la France n'avait encore jamais légiféré sur la question[9]. Pour cause, le contexte y était propice. En décembre 2014, une voiture bélier fonçait dans une foule dijonnaise quand, le même jour, un autre individu procédait de même sur le marché de Noël de Nantes. Le 7 janvier 2015, 12 personnes perdront la vie dans les attentats de Charlie Hebdo, 11 seront blessées. Le lendemain, une fusillade éclatera à Montrouge, le surlendemain une prise d'otages aura lieu à l'Hyper Casher porte de Vincennes, et une autre le même jour dans une imprimerie de Seine-et-Marne. Des militaires seront attaqués à l'arme blanche le 3 février 2015 à Nice, et TV5 monde fera l'objet d'une attaque sans précédent par cryptovirologie asymétrique en avril 2015 revendiquée de façon très discutée par le groupe djihadiste CyberCaliphate, alors que l'enquête, désormais clause, s'orientait également vers une piste russe[10].

3. *Contra legem*. Tout comme l'ont fait les États-Unis qui adoptaient dans un contexte post 11 septembre 2001 de drastiques mesures remettant en cause les libertés fondamentales en promulguant, le 26 octobre 2001, le *USA Patriot Act*, le législateur français énonçait pour sa part que ces évènements *« ont mis en exergue les limites du dispositif actuel et la nécessité pour les services de renseignement de disposer d'un cadre juridique unifié conférant aux agents des moyens efficaces »*[11]. Le Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale relevait pour sa part que la France demeurait une des rares

---

[5] Laurence Burgorgue-Larsen, *Les nouvelles technologies*, Paris, Le Seuil, 2009, vol.3, p.71.

[6] Mathieu Guidère, « Internet, haut lieu de la radicalisation », *Pouvoirs*, 16 septembre 2016, n° 158, p. 115-123.

[7] Maura Conway, « Le cyber-terrorisme. », *Cités*, 20 novembre 2009, n° 39, p. 81-94.

[8] Alain Juillet, « Edito », *Sécurité et stratégie*, 5 mars 2015, vol. 20, n° 1, p.2.

[9] Emmanuel Daoud et Géraldine Péronne, « Loi renseignement: regards croisés France – Etats-Unis », *Sécurité et stratégie*, 5 mars 2015, vol. 20, n° 1, p.1.

[10] Kevin Limonier et Maxime Audinet, « La stratégie d'influence informationnelle et numérique de la Russie en Europe », *Hérodote*, 10 mai 2017, n° 164, p.123.

[11] « Etude d'impact, Projet de loi relatif au renseignement », 18 mars 2015.

démocraties à ne pas disposer d'une loi encadrant l'action des services de renseignement[12], une pratique qu'il qualifiait de « clandestine » et qui, sous le couvert de la théorie des *« actes de gouvernement »* créait une grande insécurité juridique, à plus forte raison que les agents des services de renseignement agissaient sur le territoire national et à l'étranger sans autorisation de la loi[13]. La loi sur le renseignement était alors annoncée comme étant un texte indispensable à la lutte contre la menace terroriste.

4. Urgence. Lors des discussions parlementaires, et plus particulièrement lors de la séance du 13 avril 2015 à l'Assemblée nationale, le Premier ministre de l'époque énonçait que cette réponse normative n'était *« en rien une réponse préparée dans l'urgence »*. Pourtant, l'étude d'impact mentionnait que suite aux attentats du 7 janvier 2015 à Paris le gouvernement décidait le 19 mars 2015 de légiférer dans l'urgence en engageant la procédure accélérée de l'article 45 alinéa 2 de la Constitution de 1958, une accélération extrême de la procédure législative dont la précipitation lui valait de vives critiques[14]. L'usage de cette faculté n'est ni nouveau ni surprenant. La loi de 1991 sur le secret des correspondances[15] électroniques naissait déjà dans le cadre d'une procédure d'urgence, tout comme celle relative à la géolocalisation[16]. Aucune de ces normes n'a aspiré à créer de nouvelles techniques de renseignement. Toutes ont encadré une pratique existante en dehors de tout cadre légal, certaines ayant par ailleurs déjà été avalisées par notre juridiction suprême qui a pu considérer, en matière de géolocalisation par exemple, qu'une telle méthode d'enquête était réalisée sous le contrôle d'un juge, ce qui était une garantie suffisante contre l'arbitraire[17].

5. Focus. Appréhender le texte sur le renseignement n'est pas des plus évident, et certains ont pu souligner que ces dispositions avaient suscité un certain trouble[18] en ce qu'elles s'apparentent à des *« normes de l'ombre »*[19]. L'objectif de la présente communication ne sera pas de présenter les nouvelles dispositions dans leur ensemble – travail déjà réalisé par le

---

[12] Note du CREOGN, « Comprendre la loi sur le renseignement », *Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale*, septembre 2015, n° 13, p.1.

[13] Note du CREOGN, « Comprendre la loi sur le renseignement », art cit.

[14] Christine Lazerges et Hervé Henrion-Stoffel, « Politique criminelle, renseignement et droits de l'homme. À propos de la loi du 24 juillet 2015 relative au renseignement », *Revue de science criminelle et de droit pénal comparé*, 1 juillet 2015, vol. 3, p.761.

[15] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques

[16] Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation

[17] Cass. crim. 22 nov. 2001, n°11-84.308 ; Carole Girault, « Les nouveaux moyens de surveillance des réseaux criminels », *Dalloz Actualité*, 15 décembre 2011.

[18] E. Daoud et G. Péronne, « Loi renseignement », art cit.

[19] Emmanuel Putman, « Le projet de loi relatif au renseignement : prééminence du droit ou restriction de la liberté ? », *Revue Juridique Personnes et Famille (RJPF)*, 1 juin 2015, vol. 6, p.15.

passé[20] – mais simplement d'en reprendre les grandes lignes à des fins d'intelligibilité (I). Dans un second temps, l'on s'intéressera à la Commission nationale de contrôle des techniques de renseignement (CNCTR), nouvelle autorité administrative indépendante créée pour contrôler le renseignement, et qui a rendu son premier rapport d'activité[21] (II). Celui -ci est tout aussi intéressant pour ce qu'il dit que pour ce qu'il ne dit pas, et permet de comprendre les enjeux posés par le renseignement numérique dans la sphère pénale.

I. D'une appréhension juridique confuse à une illumination des normes de l'ombre

6. Surabondance. Lors de sa présentation, le texte sur le renseignement se voulait être *« strictement localisé sur la prévention des menaces graves contre la vie de la nation »*[22]. Il était énoncé que pour cette raison *« la surveillance des citoyens, de la vie politique, du débat public et de la presse ne relève pas des missions de renseignement »*[23]. Ce faisant, tout raisonnement par analogique qui tendrait à dire que la loi sur le renseignement s'apparente à un *Patriot Act* à la française serait *« strictement mensonger et irresponsable »*[24]. De même, qualifier cette norme de dangereuse serait une *« contre-vérité »*[25]. Pour autant, le lecteur ne peut s'empêcher à sa lecture de constater que ses finalités vont bien au-delà de ses prétentions, et plus particulièrement de la seule lutte contre la menace terroriste (A). Par ailleurs, si le texte a pu paraître particulièrement généreux lors de son adoption définitive, l'arsenal de textes est encore venu discrètement s'étoffer l'été passé par la publication de décrets dont certains voyaient leur contenu classé secret défense, et par là même dispensé de publication de contenu (B).

A. Prolixus : Un texte large au-delà de ses prétentions

7. Reliquat. Le texte sur le renseignement n'a pas pour seule finalité la matière terroriste. Elle n'est que l'une de ses modalités, soit un neuvième d'un vaste champ d'intervention codifié à l'article L. 811-3 du code de la sécurité intérieure (CSI). Si la rédaction de cette disposition traduit apparemment la volonté du législateur de recourir à une liste exhaustive de domaines relevant du renseignement, il est pour autant possible d'y voir une liste

[20] Warren Azoulay, « Loi sur le renseignement : entre sécurité d'Etat et panoptisme 2.0 », *En Quêtes pénales*, 2015, n° 10, p.5-8.
[21] Commission nationale de contrôle des techniques de renseignement, *1er Rapport d'activité 2015/2016*, Paris, CNCTR, 2016.
[22] Assemblée Nationale, « Compte rendu intégral », 13 avril 2015.
[23] *Ibid.*
[24] *Ibid.*
[25] *Ibid.*

énonciative en raison de l'usage de concepts indéterminés foisonnants et de critères extensifs, voir extensibles, de la part du législateur. Cela n'a semble-t-il posé aucune difficulté particulière au Conseil constitutionnel qui était pour la première fois de son histoire saisi par le Président de la République[26] et prononçait de maigres sanctions[27]. Font alors partie de ce champ, par exemple, les intérêts économiques, industriels et scientifiques majeurs de la France, tout comme la prévention de la criminalité et de la délinquance organisées, ou encore la prévention des violences collectives, une nouveauté de *lege lata* que le Syndicat de la magistrature avait qualifié d' *« inacceptable »*[28].

8. Hexapus. La loi du 24 juillet 2015 a eu pour effet de modifier six codes à l'instar du code pénal en aggravant la répression de certaines infractions comme les atteintes aux systèmes de traitement automatisé de données, sans véritable rapport avec le terrorisme mais s'inscrivant dans le droit fil d'une criminalisation des technologies numériques. De même, à titre d'illustration, le code des transports se trouve alimenté d'un nouvel article prévoyant que lorsque la distance à parcourir pour un voyageur sera supérieure à 250 kilomètres, les entreprises devront recueillir l'identité des passagers et la conserver durant un an[29]. Deux remarques s'imposent sur cet exemple. D'abord, si cette disposition se trouve dans un chapitre 1er intitulé *« Lutte contre le terrorisme »*, elle s'applique en revanche à l'encontre de tout individu. Ensuite, une lecture appariée avec le code monétaire et financier se veut inévitable, lequel prévoit que l'organisation chargé du Traitement du Renseignement et Action contre les Circuits FINanciers clandestins (TRACFIN) pourra demander à toute entreprise de transport des informations concernant les payeurs ou les bénéficiaires de ces prestations telles que les dates, heures et lieux de départs ou d'arrivées, ainsi que toute information relative aux bagages ou aux marchandises transportées. Enfin, les techniques de surveillance peuvent être mises en place tant dans le cadre de la défense que celui de la promotion des intérêts publics, la première permettant d'utiliser les renseignements collectés afin d'agir en réponse, et la seconde en attaque[30].

---

[26] Cons. constit., n° 2015-713 DC, 23 juil. 2015

[27] Christine Lazerges, « Politique criminelle, renseignement et droits de l'homme. À propos de la loi du 24 juillet 2015 relative au renseignement », *Revue de science criminelle et de droit pénal comparé*, 1 juillet 2015, vol. 3, p. 761-775.

[28] Syndicat de la magistrature, « Observations sur le projet de loi relatif au renseignement présentées par le Syndicat de la magistrature devant la Commission des lois », 2015, p. 5.

[29] C. transp., art. L. 1631-4.

[30] Marc Rees, « La loi sur le renseignement ou le grand méchant flou », *Revue Lamy droit de l'immatériel ex Lamy droit de l'informatique*, 1 août 2015, vol. 118, p. 47-50.

La question de la loi renseignement n'est donc pas non plus celle du recours à des techniques liberticides à des fins exclusivement préventives, pas plus que celle d'une seule modification du Code de la Sécurité Intérieure.

9. Exode judiciaire. Il n'existait jusqu'à ce texte aucune juridiction spécialement compétente concernant le contentieux du renseignement, les citoyens pouvant donc contester la décision administrative autorisant la mise en œuvre de l'une de ces techniques en saisissant le juge pénal[31]. Cette compétence est désormais celle de la juridiction suprême administrative et confère au juge judiciaire un rôle passif dans un domaine concernant pourtant les libertés individuelles. Les sages de la rue de Montpensier ont par ailleurs eu l'occasion d'énoncer que cela ne méconnaissait pas l'article 66 alinéa 2 de la Constitution posant le principe selon lequel l'autorité judiciaire est gardienne de la liberté individuelle et qu'elle assure le respect de ce principe, ces derniers ayant une définition plus étroite de la notion et considèrent qu'elle ne renvoie qu'au droit à la sureté, c'est-à-dire à celui de ne pas être arbitrairement détenu[32]. Le juge pénal est donc désormais évincé du renseignement, et ce en conformité avec la Constitution.

10. Contrôle administratif lacunaire. Les travaux parlementaires se voulaient rassurants quant à la possibilité de saisir le Conseil d'État, lequel peut désormais l'être par *« toute personne »* selon les termes de l'article L. 841-1 du CSI, une procédure dont les carences ont déjà pu être exposées par la doctrine[33]. Pour autant, cette faculté paraîtrait presque dépourvue de sens puisqu'une personne ne disposera aucunement de la possibilité de savoir, le cas échéant, qu'elle fait l'objet d'une technique de renseignement. D'abord, les décisions des magistrats du Palais-Royal seront rendues en premier et dernier ressort conformément à l'article L. 311-4-1 du code de justice administrative (CJA), et le justiciable sera donc privé de son droit d'accès à un second degré de juridiction. En outre, les parties seront entendues séparément[34] et n'auront donc pas connaissance des moyens avancés par la partie adverse. Les documents et pièces en possession de la CNCTR ne seront pas non plus versés dans le cadre de l'instruction contradictoire, de sorte que la partie requérante n'aura pas accès à son entier dossier. Si l'on savait déjà qu'elle ne pouvait pas avoir connaissance du verbe adverse, elle n'en connaîtra pas non plus la plume. La règle de la publicité des débats a quant à elle disparu, la règle de droit commun devenant celle du huis

---

[31] « Etude d'impact, Projet de loi relatif au renseignement », art cit, p. 57.

[32] Cons. constit. 19 janv. 2006, n° 2005-532 DC, consid. 8

[33] Pascale Gonod, « Loi du 24 juillet 2015 relative au renseignement : quels contrôles ? », *Procédures*, 1 novembre 2015, vol. 11, p. 4-8.

[34] CJA., art. L. 773-3.

clos[35]. Enfin, les conseillers d'Etat rendront une décision sans motivation. Malgré cela, le Conseil d'État a récemment apaisé nos craintes en énonçant que cette procédure était conforme au principe du contradictoire prévu par l'article 6 de la Conv. EDH[36].

11. Fortuna. *In fine*, il ressort des discussions parlementaires que tous les amendements déposés en vue de rappeler l'Etat de droit, et de limiter cet effacement total du juge judiciaire en matière de renseignement, étaient systématiquement rejetés[37]. Le caractère relativement hasardeux de l'effectivité d'un tel recours soulève ici l'épineuse question de savoir ce qu'il reste des droits de la défense et du droit à un procès équitable lorsque se trouve brandie la carte de la raison d'État, *a fortiori* lorsque l'on constate que l'éventail des programmes de renseignement s'est encore étoffé depuis peu[38].

B. Extend : de la multiplication des programmes de renseignement au renforcement de l'arsenal de collecte de données

13. CRISTINA 2.0. Le champ ouvert par le développement des techniques de surveillance massive et généralisée paraît offrir des possibilités quasi-illimitées[39]. Chaque pays s'est doté d'outils pour mettre en place un monitoring permanent de ses citoyens. A titre d'exemple, les programmes *Xkeyscore* et *Prism* ont doté les États-Unis dans un contexte post 11 septembre 2001 d'un dispositif de surveillance massif sur leur territoire, et par-delà. La France n'a pour sa part rien à envier aux autres pays. Elle s'équipait il y a dix années déjà du fichier de centralisation CRISTINA, lequel a été mis à jour le 2 août 2017 par un décret dont le contenu était dispensé de publication[40].

14. ACCReD. Ce mois d'août aura également été l'occasion de créer un nouveau fichier de traitement automatisé de donnée à caractère personnel du nom d' « ACCReD »[41], le ministère de l'intérieur ayant entendu faciliter la réalisation d'enquêtes administratives. C'est une nouvelle fois sous le couvert d'un *« risque exceptionnel de menace terroriste »*[42] que le

---

35 CJA., art. L. 773-4.

36 Conseil d'Etat, formation spécialisée, 28 juin 2017, n° 402349.

37 Assemblée nationale, *op. cit.*

38 Warren Azoulay, « Du panoptique au technoptique : renforcement de l'arsenal de collecte de données », *Dalloz Actualité*, 19 septembre 2017.

39 *Ibid.*

40 Décret du 2 août 2017 modifiant le décret du 27 juin 2008 portant création au profit de la direction générale de la sécurité intérieure d'un traitement automatisé de données à caractère personnel dénommé « CRISTINA ».

41 Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « ACCReD ».

42 *Ibid.*

gouvernement préconisait sa mise en place. ACCReD conservera trois types de fichiers durant cinq années, dont les données relatives à la personne faisant l'objet de ladite enquête, ainsi que les données et informations relatives aux résultats de celle-ci. Enfin, il sera possible d'avoir accès, par l'intermédiaire d'ACCReD, à neuf types de fichiers, dont des fichiers judiciaires comme celui de Traitement des Antécédents Judiciaires (TAJ) et le fichier des personnes recherchées (FPR).

15. Satisfaction partielle. Si le décret prévoyait à l'origine la mise en place d'une collecte générale d'informations relatives *« aux origines raciales ou ethniques »* des personnes, cette proposition aura finalement achoppé dans sa version définitive. Trois remarques émergent alors. D'abord, sur un fond métajuridique[43], avoir fait disparaître le terme de *« race »* en janvier 2017[44] du Code pénal pour vouloir le reprendre en l'occurrence est surprenant et traduit la volonté d'un critiquable retour en arrière. En deuxième lieu, il est à porter au crédit de la Commission Nationale de l'Informatique et des Libertés (CNIL) d'avoir souligné avec pragmatisme que ces informations *« ne renvoient à aucune catégorie de données objectives liées à des agissements ou des comportements [et] ne saurai[en]t être justifi[ées] »*[45]. Enfin, si elle faisait part d'une réserve relative à l'imprécision rédactionnelle des dispositions nouvelles, et de la nature particulièrement sensible de certains fichiers, le texte restera pour autant brumeux et imprécis.

16. Biopex. Dernier né dans le but de renforcer les pouvoirs d'investigation des six services du renseignement français (v. *infra.* §21), un décret du 4 août 2017 crée le fichier BIOPEX[46] qui s'ajoute à la liste des fichiers dont le contentieux est soumis à la formation spécialisée du Conseil d'État, évinçant une nouvelle fois, s'il en fallait une, le juge judiciaire de tout contrôle sur celui-ci. En l'absence de publication, son contenu demeure inconnu.

II. Premier rapport de la CNCTR : dits et non-dits

Après plus d'une année d'exercice, la CNCTR a rendu son premier rapport d'activité, lequel se veut être tout aussi instructif pour ce qu'il apprend à ses lecteurs (A) que pour sa persévérance à l'obscurité (B).

---

[43] Pascal Mbongo, « Un antiracisme scripturaire : la suppression du mot "race" de la législation », *Recueil Dalloz*, 30 mai 2013, vol. 19, p. 1288-1289.

[44] Loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté.

[45] CNIL, délib. n° 2017-152, 18 mai 2007.

[46] Décret n° 2017-1231 du 4 août 2017 portant modification du décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

A. Amen dico : ce que l'on sait du contrôle de la commission sur le renseignement

17. AAI. La CNCTR est l'autorité administrative indépendante venant remplacer la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) mise en place par la loi de 1991[47]. Composée de neuf membres, dont deux députés, deux sénateurs, deux membres du Conseil d'État et deux magistrats de la Cour de cassation, elle ne dispose, de manière forte regrettable, que d'un seul spécialiste des nouvelles technologies. Ses moyens, qui n'ont pas évolué depuis 1991[48], demeureront donc insuffisants, et ce nonobstant la proposition du Conseil d'Etat de doter la commission *« de moyens humains renforcés sur le plan quantitatif et qualitatif, avec des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données »*[49], la volonté de la juridiction suprême étant, pourtant, d'assurer *« le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques »*[50].

18. Limites. Si l'autorisation du Premier ministre visant à recourir à une technique de renseignement est conditionnée au recueil préalable de l'avis de l'autorité administrative, le chef du gouvernement ne se trouvera pas lié par cette réponse. Il pourra passer outre ses avis défavorables, et Jean-Marie DELARUE, ancien président de la CNCIS, se disait préoccupé dans son 23ème rapport d'activité par le fait que le Premier ministre passait outre les avis défavorables de la commission pour plus d'un quart de ces derniers[51]. Plus encore, en cas d'urgence, le Premier ministre pourra se dispenser de cet avis, une procédure trop souvent invoquée selon la CNCIS[52]. Son budget annuel d'environ 3 millions d'euros se trouve bien loin derrière celui de ses sœurs cadettes comme celui de la CNIL et ses 17,5 millions d'euros de crédits en 2016, ou encore des 37 millions d'euros du CSA[53]. Enfin, dotée de 15 agents seulement, il est à regretter que les services cloisonnés se répartissent asymétriquement les effectifs.

---

47 v. *supra* § 4.

48 Emmanuel Dupic, « La loi relative au renseignement, un patriot acte français ? ; Projet de loi relatif au renseignement (PRMX1504410L), 5 mai 2015, numéro 2669 », *La Gazette du Palais*, 9 juillet 2015, vol. 189, no 190, p. 4-7.

49 Conseil d'Etat, *Le numérique et les droits fondamentaux*, Paris, La documentation française, p. 30.

50 *Ibid.*

51 CNCIS, *23e rapport d'activité*, Paris, La documentation française, 2016, 226 p.

52 CNCIS, *22e rapport d'activité*, Paris, La documentation française, 2015, p. 82.

53 J-Y. Leconte, « Projet de loi de finances pour 2017 : Protection des droits et libertés », Avis n° 146, 2016, p. 8.

19. Données quantitatives. La CNCTR rendait 48.202 avis sur l'année 2017 concernant l'accès aux données de connexion en temps différés[54]. Parmi ceux-ci, le tiers des demandes étaient destinées à recevoir les factures détaillées – les *fadettes* – d'une personne placée sous surveillance. Concernant les interceptions de sécurité, 43% d'entre elles invoquaient la prévention du terrorisme, et 40% celle de la criminalité et de la délinquance. Ce constat appelle alors deux remarques. D'abord, plus de la moitié des interceptions de sécurité autorisées (53%) n'était pas en rapport avec le terrorisme. En second lieu, 17% de ces interceptions étaient de cause inconnue, posant un évident problème de transparence de la part de l'autorité administrative indépendante. Enfin, concernant les personnes ayant fait l'objet d'au moins l'une des techniques de renseignement, elles étaient plus de 20.000 sur une année, soit 55 personnes chaque jour placées sous surveillance, ou encore une personne surveillée toutes les 25 minutes, un chiffre d'ailleurs sous évalué en raison des limites de ce rapport.

B. Abscondam : la part d'ombre du renseignement

20. Comptabilisation partielle. Parler de dénombrement des personnes surveillées est insuffisant puisque la part d'ombre de la statistique fournie sur la CNCTR en l'occurrence ne nous permet pas d'en avoir une vision exacte. D'abord, son rapport ne tient pas compte de toutes les personnes surveillées en ce qu'il ne comptabilise pas celles qui ne sont pas nommément identifiées. Ensuite, parce que ce chiffre ne tient pas non plus compte des personnes faisant l'objet de demandes d'accès aux données de connexion à temps différés, c'est-à-dire les 48.202 susmentionnées[55]. Si elles y étaient intégrées, le total des personnes nouvellement surveillées chaque jour passerait à 187, soit 1 personne toutes les 7 minutes. Cela signifie qu'entre le début de la conférence des doctorants 2017 et son terme (soit 120 minutes d'interventions orales), ce sont environ 15 à 20 personnes qui auront été placées sous surveillance, ce chiffre ne tenant toujours pas compte des personnes surveillées mais non identifiées nominativement.

21. Répartition incomplète. Sur les 20 282 personnes faisant l'objet d'une surveillance au sens qu'en donne la commission, celle-ci nous renseigne de ce que 47% d'entre elles l'ont été au titre de la prévention du terrorisme, et 29% au titre de la prévention de la criminalité

[54] Commission nationale de contrôle des techniques de renseignement, *1er Rapport d'activité 2015/2016*, *op. cit.*, p. 65.
[55] v. *supra* § 18.

et de la délinquance organisée. La somme de cette répartition restituée n'étant pas égale à 100%, un inconnu demeure pour les 4.810 personnes surveillées restantes (24%). Le quart d'entre elles a donc connu une mesure de surveillance *stricto sensu* sans que l'on puisse en connaître le fondement.

22. Absence de centralisation. Concernant le stockage et la conservation des données recueillies, qu'il s'agisse des interceptions de sécurité par IMSI Catcher, de captation de paroles prononcées à titre privé et d'images obtenues dans un lieu privé, ou encore du recueil et de la captation de données informatiques en temps réels ou différé, toutes les données recueillies ont une caractéristique commune quant à leur stockage en ce qu'il se trouve décentralisé. Si l'article 822-1 alinéa 2e du CSI prévoit que *« le Premier ministre organise la traçabilité de l'exécution des techniques autorisées […] et définit les modalités de la centralisation des renseignements collectés »*, force est en l'espèce de constater qu'il n'en a défini aucune, une carence *contra legem* ayant une pléthore de conséquences néfastes. En premier lieu, la CNCTR se trouvant dépourvue d'un accès permanent, complet et direct aux renseignements collectés, son contrôle ne pourra assurément pas être effectif. La seconde difficulté relève d'une sécurité déficiente qui régit la transmission informatique d'éléments couverts par le secret de la défense nationale. Il est alors surprenant de trouver dans le rapport de la CNCTR une recommandation tendant à se doter de réseaux dédiés ou de dispositifs sûrs de chiffrement des données, alors que leur existence *a priori* semblait pourtant relever de l'évidence, d'autant que la communauté du renseignement se compose non seulement d'agents du premier cercle (DGSE[56] ; DGSI[57] ; DRSD[58] ; DRM[59] ; DNRED[60] et TRACFIN[61]), mais également d'agents du second cercle (Direction Générale de la Police Nationale et Direction Générale de la Gendarmerie Nationale). Or, l'article L. 863-2 du CSI autorisant les services de renseignement à échanger toutes informations utiles à l'accomplissement de leurs missions, qu'il s'agisse du premier ou du second cercle, la mise en place d'une sécurisation de celles-ci ne paraît pas surabondant de prudence.

23. « Fuites » de renseignements. En raison de cette absence de centralisation des données, la CNCTR mentionnait un *« risque d'avoir une diffusion non maitrisée, au sein des services,*

[56] Direction Générale de la Sécurité Extérieure.
[57] Direction Générale de la Sécurité Intérieure.
[58] Direction du Renseignement et de la Sécurité de la Défense.
[59] Direction du Renseignement Militaire.
[60] Direction Nationale du Renseignement et des Enquêtes Douanières.
[61] Traitement du Renseignement et Action contre les Circuits FINanciers clandestins.

d'informations concernant la vie privée »[62] ainsi que l'impossibilité de contrôler la conformité tant de l'exploitation de ces données que de leur finalité, ou encore la durée de leur conservation. La défense ne s'étonne donc plus, ou si peu, des dossiers commençants, dès la côte D1, par la mention *« selon une information confidentielle parvenue à nos services »* ou l'une de ses variantes. Les exemples du passé sont par ailleurs légion, et l'on pourrait évoquer, à titre d'illustration, celui de l'affaire des fadettes de l'Elysée dans laquelle la DCRI (devenue DGSI) s'était dispensée de l'avis de la CNCIS et avait recueilli les factures téléphoniques détaillées de nombreuses personnes à l'Élysée, ceci dans le but d'identifier le responsable de la fuite d'un article de 2010 du journal *Le Monde*[63] dans le cadre de l'affaire Bettencourt. Le motif invoqué, à savoir le terrorisme, paraissait en l'espèce très surprenant et pour le moins incongru. Comme a également pu le relever une partie de la doctrine, de nombreuses enquêtes sont ouvertes sur la base d'un renseignement se trouvant par la suite judiciarisé, les services de renseignements rédigeant un rapport destiné à *« gommer la source »* de ce renseignement et ses éléments d'identification[64]. Les techniques mises en œuvre, qui n'ont donc pas de but de police judiciaire, produisent pourtant bien un résultat de police judiciaire[65], étant précisé que le juge pénal ne dispose d'aucun pouvoir d'en apprécier la légalité et que le procès-verbal en faisant état n'est pas considéré comme un acte de procédure et ne peut donc pas être annulé[66]. Ce passage de la matière administrative à la matière judiciaire, sans passer par les garanties de la procédure pénale, semble réduire la distinction entre prévention des infractions et constatation des infractions[67]. A ce sujet, Raphaëlle Parizot nous a efficacement invité à la prudence : « [Nous] ne [devons] *pas nous[*leurrer*] : si les informations recueillies par les services spécialisés de renseignement ne peuvent pas directement servir de preuve pour une infraction commise, elles permettront (et permettent déjà) de faire démarrer une enquête ou une instruction* »[68], ce à quoi l'on peut ajouter que la personne mise en

---

[62] Commission nationale de contrôle des techniques de renseignement, *1er Rapport d'activité 2015/2016*, *op. cit.*, p. 79.

[63] Pierre-Antoine Souchard, « Proposition pour une nouvelle loi sur le secret des sources des journalistes », *Légipresse*, 1 juillet 2012, vol. 296, p. 403-404.

[64] Camille Hennetier, « Le traitement judiciaire du terrorisme. La construction d'une justice spécialisée », *Cahiers de la sécurité et de la justice*, 2016, nº 35-36, p. 8.

[65] François Fourment, « La loi "Renseignement", le renseignement incident de commission d'une infraction et l'autorité judiciaire », *La Gazette du Palais*, 28 janvier 2016, vol. 4, p. 75.

[66] Jean-Baptiste Thierry, *L'articulation des dispositions administratives et judiciaires dans la lutte contre la radicalisation violence - 2ème partie*, article de blog, 13 janvier 2017, [en ligne], v. https://sinelege.hypotheses.org/3441.

[67] Raphaële Parizot, « Surveiller et prévenir... à quel prix ? », *JCP G Semaine Juridique (édition générale)*, 5 octobre 2015, vol. 41, p. 1816-1824.

[68] *Ibid.*

examen sera dans l'impossibilité de contester les conditions dans lesquelles ont été recueillis les éléments de preuve fondant l'engagement des poursuites.

24. Lanceurs d'alertes. Enfin, La CNCTR a pu se féliciter de ce que le dispositif instauré par la loi renseignement permettant aux lanceurs d'alertes de dénoncer une violation du texte, laquelle constituerait une infraction pénale relevant de la compétence du parquet, n'a donné lieu à aucune saisine de l'autorité administrative indépendante. Le justiciable pourra cependant opter pour une double interprétation de ce chiffre. D'abord, il pourra penser que les services et les agents du renseignement, particulièrement sensibilisés à la culture des données et à leur respect, ainsi qu'au respect de la vie privée et de la loi, observent à la lettre la loi du 24 juillet 2015. Ou bien, d'aucuns se souviendront d'un amendement de précision de dernière minute déposé par le gouvernement concernant les futurs Edward Snowden, lequel leur faisait finalement interdiction d'évoquer devant la CNCTR un quelconque élément classé secret défense. Il serait ironique de relever la difficulté d'évoquer autre chose que de tels éléments devant une AAI habilitée secret défense, de la part d'agents ne traitant que des éléments classés secret défense.

Conclusion

25. Liberté *VS* Sécurité. Il y a près d'un demi-siècle, Michel Foucault caractérisait déjà nos sociétés de sociétés de surveillance[69]. En observant un effacement d'une société spectaculaire[70] au profit d'une discrétion de la peine, l'enfouissement bureaucratique de la punition qui ne se donnait plus à voir supposait alors un autre régime du voir, celui de la surveillance[71]. En effet, la révolution apportée par les NTIC a également profondément transformé le travail des acteurs politiques qui y voient là de nouvelles possibilités d'action[72]. Le sujet, trop souvent résumé aux images de *Big Brother* et à la vision dystopique d'Orwell[73], se situe bien au-delà d'un totalitarisme électronique. Il s'agit davantage de la question d'une nouvelle articulation des pouvoirs s'exerçant entre citoyens et détenteurs du pouvoir créateur de la norme, surveillés et surveillants. Les nouvelles technologies créent alors un nouveau lieu de conflit dont le législateur s'est une nouvelle fois saisi à la hâte, la

[69] Michel Foucault, *La Société punitive. Cours au Collège de France*, Paris, Le Seuil, 2013, p. 25.
[70] Guy Debord, *La société du spectacle*, Paris, Gallimard, 1996, 208 p.
[71] Michel Foucault, *Surveiller et punir : naissance de la prison*, Paris, Gallimard, 1976, p. 15.
[72] Julien Boyadjian, Aurélie Olivesi et Julien Velcin, « Le web politique au prisme de la science des données », *Réseaux*, 22 août 2017, n° 204, p. 11.
[73] George Orwell, *1984*, Paris, Gallimard, 1972, 438 p.

redondance d'un processus de normalisation de l'urgence[74], créant parfois ce que d'aucuns ont pu appeler une *« prison algorithmique »*[75] remettant en cause les libertés individuelles du citoyen au nom de sa sécurité[76]. Si l'explication réside dans une volonté d'identification de la menace terroriste, le risque demeure d'opérer une neutralisation sélective[77] lorsque la méthode de collecte se veut être généralisée et les données non centralisées, l'ouverture d'informations judiciaires incidentes en étant un exemple patent. Par ailleurs, le dialogue entre le monde de la recherche et les services de renseignement constituerait pour certain l'un des points forts du renseignement américain, un dialogue avec l'univers académique dont d'autres organisations pourraient s'inspirer afin que le renseignement ressemble davantage à une science qu'à un art[78].

Comme a pu le rappeler la Cour européenne des droits de l'homme, s'il est exact que les Etats disposent d'une certaine marge d'appréciation lorsqu'ils décident du choix des moyens permettant d'atteindre le but légitime que constitue la protection de la sécurité nationale, l'abus d'un tel système de surveillance aurait pour conséquence de *« saper, voire de détruire, la démocratie au motif de la défense »*[79]. Pour l'heure, si la loi sur le renseignement était annoncée comme étant un texte indispensable à la lutte contre la menace terroriste, il a efficacement été relevé par la doctrine que l'on ne peut certes dénombrer les infractions qu'elle a permis d'empêcher, mais l'on peut malheureusement compter celles commises sous son bouclier[80].

26. Rien à cacher. Bernard E. Harcourt reprend dans ses travaux la pensée d'Ervin Goffman selon lequel le sujet et la structure ne sauraient être antagonistes et sont intrinsèquement liés[81]. Les structures n'existeraient que pour autant qu'elles soient mises en œuvre à chaque instant par les acteurs, mais les acteurs eux-mêmes ne peuvent les mettre en œuvre que sur la base d'un sens commun guidant leur conduite. Les technologies ont

---

[74] Karine Roudier, « Le Conseil constitutionnel face l'avènement d'une politique sécuritaire », *Les nouveaux cahiers du Conseil constitutionnel*, 1 avril 2016, vol. 51, p. 37.

[75] Simon Chignard et Louis-David Benyayer, *Datanomics Les nouveaux business models des données*, Limoges, FYP Editions, 2015, p. 139.

[76] Daniel Desurvire, « A propos de la loi relative au renseignement », *Les Petites Affiches*, 9 octobre 2015, vol. 202, p. 14.

[77] Bernard E. Harcourt, « Surveiller et punir à l'âge actuariel », *Déviance et Société*, 22 mars 2011, vol. 35, n° 1, p. 20.

[78] Damien Van Puyvelde, « L'analyse du renseignement aux Etats-Unis : entre art et science », *Sécurité et stratégie*, 5 mars 2015, vol. 20, n° 1, p. 31.

[79] CEDH, Grande Chambre, 4 déc. 2015, req. n° 47143/06, *Zakharov c/ Russie*, § 232

[80] Nicolas Catelan, « Les nouveaux textes relatifs au renseignement : un moindre mal », *Revue de science criminelle et de droit pénal comparé*, 1 octobre 2015, vol. 4, p. 922.

[81] Bernard E. Harcourt, *Exposed – Desire and Disobedience in the Digital Age*, Cambridge, Massachusetts, Harvard University Press, 2015, p. 217.

alors un effet sur notre subjectivité, et c'est d'une transformation de la morale dont il est question. En outre, les travaux sur la théorie d'une *« spirale du silence »*[82] ont pu être réutilisés afin de démontrer la façon dont le processus selon lequel les personnes ayant conscience d'être surveillées en ligne et l'acceptant agissaient comme modérateur de la volonté d'exprimer ses opinions, celles-ci s'autocensurant plus que celles refusant cet état d'hyper-surveillance[83]. Il résulterait alors de cet effet des technologies sur notre subjectivité une transformation de la morale, et une *« mortification du soi »*[84] se produisant lorsque les sujets cèdent volontairement à leur vie privée, lorsqu'ils déclarent ne rien avoir à cacher, et que l'affaire est *« trop grosse »* pour être vrai. Les difficultés posées par la convergence des nouvelles formes de surveillances correctionnelles avec la transparence virtuelle constituent un véritable défi sur lequel une réflexion doit être menée, le tout étant de ne pas être distrait par une nouvelle notification.

[82] Carroll J. Glynn et Jack M. Mcleod, « Public Opinion du Jour: An Examination of the Spiral of Silence », *Public Opinion Quarterly*, 1 janvier 1984, vol. 48, nº 4, p. 731-740.

[83] Elizabeth Stoycheff, « Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring », *Journalism & Mass Communication Quarterly*, 1 juin 2016, vol. 93, nº 2, p. 296-311.

[84] B.E. Harcourt, *Exposed – Desire and Disobedience in the Digital Age*, *op. cit.*, p. 217.