Ombres et lumières sur le droit fondamental à la protection des données personnelles confronté aux services de renseignement en matière de prévention du terrorisme

The shadows and highlights of the fundamental right to protection of personal data in the work of the intelligence services to prevent terrorism

Philippe Ch.-A. Guillot

Édition électronique

URL : <http://journals.openedition.org/add/340>

DOI : 10.4000/add.340

ISSN : 2606-1988

Éditeur

Presses universitaires de Rouen et du Havre

Édition imprimée

Date de publication : 1 juin 2016

Pagination : 165-196

ISBN : 979-10-240-0599-7

ISSN : 1955-0855

Référence électronique

Philippe Ch.-A. Guillot, « Ombres et lumières sur le droit fondamental à la protection des données personnelles confronté aux services de renseignement en matière de prévention du terrorisme », *Les Annales de droit* [En ligne], 10 | 2016, mis en ligne le 08 janvier 2018, consulté le 01 mai 2019. URL : <http://journals.openedition.org/add/340> ; DOI : 10.4000/add.340

Ombres et lumières sur le droit fondamental à la protection des données personnelles confronté aux services de renseignement en matière de prévention du terrorisme

Philippe Ch.-A. GUILLOT

« Nos sociétés ne feront pas l'économie de grands débats sur l'étendue de la protection de la vie privée et les atteintes qu'il est légitime d'y porter, et dans quel cadre juridique¹. » Cet avertissement du vice-président chargé de l'instruction au pôle antiterroriste au tribunal de grande instance de Paris lancé dans un ouvrage écrit peu avant la promulgation de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement résonne dans les controverses non encore éteintes sur la protection des données personnelles face aux moyens mis en œuvre pour prévenir le terrorisme, avatars postmodernes de l'antique querelle entre les partisans de la liberté et les tenants de la sécurité. Souvent dans l'histoire – y compris la plus récente – la vie privée² a eu à subir les ingérences du pouvoir au prétexte de prévention du crime ou de la sédition. À l'ère du numérique, ce phénomène s'amplifie car « la numérisation des existences et des sociétés n'[a] cessé de s'intensifier, générant une production exponentielle de données ainsi que le suivi toujours plus précis des comportements individuels et collectifs³ ». Les technologies de l'information et de la communication fournissent aux services de renseignement la possibilité de puiser dans

-
1. David Bénichou, « L'approche judiciaire: les défis de la répression », dans David Bénichou, Farhad Khosrokhavar et Philippe Migaux, *Le jihadisme. Le comprendre pour mieux le combattre*, Paris, Plon, 2015, p. 387.
 2. Ce thème a fait l'objet de récentes études. Voir les dossiers « Le Conseil constitutionnel et la vie privée », NCCC 2015 et « Special Issue: Privacy », *Montesquieu Law Review*, n° 2, juillet 2015, disponible en ligne à l'adresse suivante: <http://www.montesquieu-lawreview.eu/review.htm> (consulté le 22 novembre 2015).
 3. Éric Sadin, « Combattons politiquement la numérisation de nos vies », *Le Monde*, 14 avril 2015, p. 14.

les données personnelles indices et révélations allant au-delà de ce que George Orwell avait imaginé dans 1984 et évoquant *Minority Report* de Steven Spielberg⁴, mais ce qui est techniquement possible n'est pas nécessairement juridiquement fondé. En droit, la protection des données personnelles doit primer sur la surveillance administrative.

En effet, l'Union européenne et ses États membres considèrent la protection des données personnelles comme un droit fondamental ainsi que l'affirment les articles 8 de la Charte des droits fondamentaux de l'Union européenne (CDFUE) et 16 du traité sur le fonctionnement de l'Union européenne⁵. La protection des données personnelles est consacrée aussi par la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 et son protocole additionnel n° 181 du 8 novembre 2001⁶ ainsi que par l'interprétation de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales par la Cour européenne des droits de l'homme⁷ à laquelle font écho, en

-
4. Voir Marc Jankowski, « *Big Data* : de la police préventive à la police prédictive », *Revue Défense nationale*, n° 779, avril 2015, p. 19-21.
 5. Voir Sylvie Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la CJUE », dans Romain Tinière et Claire Vial (dir.), *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, Bruxelles, Bruylant, 2015, p. 213-231 ; Agostino Valerio Placco, « La protection des données à caractère personnel dans le cadre de la Cour de justice de l'Union européenne relative aux droits fondamentaux », dans Alain Grosjean (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 27-51.
 6. Voir Cécile de Terwangne, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », dans Céline Castes-Renard (dir.), *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, p. 81-120.
 7. CEDH, 26 mars 1987, *Leander c/ Suède* ; 25 mars 1998, *Amman c/ Suisse* ; 4 mai 2000, *Rotaru c/ Roumanie* ; 14 févr. 2006, *Turek c/ Slovaquie* ; 4 déc. 2008, *S. & Marper c/ Royaume-Uni* ; 10 févr. 2011, *Dimitrov-Kazakov c/ Bulgarie* ; 24 mai 2011, *Association « 21 Décembre 1989 » e.a. c/ Roumanie* ; 18 sept. 2014, *Brunet c/ France*. La cour reconnaît cependant que la lutte contre le terrorisme peut justifier des restrictions au secret de la correspondance et des télécommunications (6 sept. 1979, *Klass e.a. c/ Allemagne*) ou la conservation de certaines données par les services de sécurité (6 juin 2006, *Segerstedt-Wiberg e.a. c/ Suède*). Voir Athanasia Petropoulou, *Liberté et sécurité : les mesures anti-terroristes et la Cour européenne des droits de l'Homme*, Paris, Pédone, 2014, p. 443-461 ; Loredana Tassone, « La protection des données dans la jurisprudence de la Cour européenne des droits de l'Homme », dans Alain Grosjean (dir.), *op. cit.*, p. 53-70 ; Hélène Tran, *Les obligations de vigilance des États-parties à la Convention européenne des droits de l'Homme*, Bruxelles, Bruylant, 2013, p. 223-227.

France, les décisions du Conseil constitutionnel⁸ et du Conseil d'État⁹. La protection des données personnelles est régie notamment par la directive 95/46/CE du 24 octobre 1995 complétée par la décision-cadre 2008/977/JAI du conseil du 27 novembre 2008. Le régime inspiré de la loi française Informatique et libertés¹⁰ interdit l'inclusion de données sensibles – relatives à la race ou à l'origine ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale et celles concernant l'abus de drogue et d'alcool, la santé ou la vie sexuelle – dans les traitements de données et soumet ceux-ci à des contrôles par une autorité administrative indépendante – Commission nationale informatique et libertés (CNIL) en France « conçue à l'origine comme l'organe de la conscience sociale face à l'emploi de l'informatique¹¹ », Contrôleur européen de la protection des données (CEPD) pour l'Union européenne. L'article 29 de la directive instaure un groupe européen des autorités nationales de protection des données – le « G 29 » – pour contribuer à la mise en œuvre homogène des dispositions nationales. La personne dont des données personnelles ont été enregistrées dans un fichier a un droit de s'informer, un droit d'accès direct, un droit de rectification, un droit d'opposition et un droit à l'oubli récemment rebaptisé « droit au déréférencement¹² ». Ce ne sont pas

-
8. Cons. const., déc. n° 2012-652 DC, 22 mars 2012, *Loi relative à la protection de l'identité*, cons. 8 : le Conseil constitutionnel a jugé conforme à la Constitution les fichiers de police judiciaire ainsi que l'utilisation à des fins administratives de ces fichiers aux fins de prévention du terrorisme (Cons. const., déc. n° 2003-467 DC, 13 mars 2003, *Loi sur la sécurité intérieure*, cons. 17-46) et le fichier national automatisé des empreintes génétiques (FNAEG) concernant notamment l'identification des auteurs d'actes de terrorisme (Cons. const., déc. n° 2010-25 QPC, 16 sept. 2010, M. Jean-Victor C.).
 9. CE, ass., 26 août 2011, Association pour la promotion de l'image, *Recueil Lebon*, p. 505.
 10. L. n° 78-17, 6 janv. 1978 révisée par la L. n° 2004-801, 6 août 2004 ; voir Jean Harivel, « La difficile protection des données à caractère personnel dans une société numérique », dans Irène Bouhadana et William Gilles (dir.), *Droit et gouvernance des données publiques et privées à l'ère du numérique*, Paris, IMODEV, 2015, p. 57-64 ; Conseil d'État, *Le numérique et les droits fondamentaux*, Paris, La Documentation française, 2014, p. 70-76, 86-87.
 11. Valérie Lasserre, *Le nouvel ordre juridique. Le droit de la gouvernance*, Paris, LexisNexis, 2015, p. 285.
 12. CJUE, Gr. Ch., 13 mai 2014, *Google Spain SL & Google Inc. c/ AEPD & Mario Costeja Gonzalez*, C-131/12 ; voir Herke Kranenborg, « Google and the right to be forgotten », *European Data Protection Law Review*, vol. I, n° 1, 2015, p. 70-79 ; Bruno Hardy, « La géographie du droit à l'oubli », RTDE 2014, p. 879-897 ; Conseil d'État, *op. cit.*, p. 184-189 ; pour une présentation approfondie, voir Élise Defreyne et Romain Robert, « L'arrêt "Google Spain" : une clarification de la responsabilité

des droits réels sur les données personnelles mais des droits personnels sur les traitements qui s'exercent par l'intermédiaire d'un tiers¹³, même si le Conseil d'État préconise de « concevoir le droit à la protection des données comme un droit à "l'autodétermination informationnelle", c'est-à-dire le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel¹⁴ ».

En revanche, il n'existe pas de texte conventionnel universel sur la protection des données personnelles autre que les articles 17 du Pacte international relatif aux droits civils et politiques du 16 décembre 1966 sur le respect de la vie privée et 37 § 1 de la constitution de l'Union internationale des télécommunications du 22 décembre 1992 relatif au secret des correspondances internationales, lesquels, compte tenu de leur date d'adoption, ne traitent que partiellement de la question. Toutefois, ces dernières années les Nations unies s'en sont emparées. Le Conseil des droits de l'homme ouvre la marche avec la résolution 20/8 du 5 juillet 2012 sur la promotion, la protection et l'exercice des droits de l'homme sur l'Internet. L'assemblée générale adopte ensuite la résolution 68/167 du 18 décembre 2013 intitulée « Le droit à la vie privée à l'ère du numérique » qui proclame : « si le souci de la sécurité publique peut justifier la collecte et la protection de certaines données sensibles, il ne dispense pas les États de respecter pleinement les obligations que leur impose le droit international des Droits de l'homme¹⁵ » et la résolution 68/178 du même jour ayant pour titre « Protection des Droits de l'homme et des libertés fondamentales dans la lutte antiterroriste » dont le point 6 g encourage les États à « préserver le droit au respect de la vie privée, conformément au droit international, en particulier au droit des Droits de l'homme, et prendre les mesures pour s'assurer que toute entrave ou restriction à l'exercice de ce droit n'est pas arbitraire, est réglementée par la loi, fait l'objet d'un contrôle effectif et donne lieu à une réparation adéquate, y compris par un contrôle judiciaire ou d'autres

des moteurs de recherches... aux conséquences encore floues », *Revue du droit des technologies de l'information*, n° 56, 2015, p. 73-114 ; Cécile de Terwagne, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », dans Alain Grosjean (dir.), *op. cit.*, p. 245-275.

13. Voir Thomas Saint-Aubin, « Les droits de l'opérateur de données sur son patrimoine numérique informationnel », dans Irène Bouhadana et William Gilles (dir.), *op. cit.*, p. 143-144 ; Jessica Eynard, *Les données personnelles. Quelle définition pour une protection efficace ?*, Paris, Michalon, 2013, p. 141-182.

14. Conseil d'État, *op. cit.*, p. 337 ; présentation détaillée, p. 264-269.

15. A/RES/68/167, p. 2.

moyens¹⁶ ». Une autre résolution, à nouveau dénommée « Le droit à la vie privée à l'ère du numérique », a été adoptée le 18 décembre 2014 ; elle précise : « si les métadonnées peuvent offrir des avantages, certains types de métadonnées peuvent aussi, par agrégation, révéler des informations personnelles et donner une idée du comportement, des relations sociales, des préférences personnelles et de l'identité des particuliers¹⁷ », à tel point que, selon un éminent juriste de l'Agence nationale de sécurité des États-Unis (NSA), une quantité suffisante de métadonnées dispense d'avoir accès au contenu des communications d'un individu¹⁸.

Conformément à la demande exprimée par la résolution 68/167, le haut-commissaire des Nations unies aux droits de l'homme présenta au Conseil des droits de l'homme et à l'assemblée générale un rapport, lui aussi appelé « Le droit à la vie privée à l'ère du numérique », lequel déplore « l'inquiétant manque de transparence dont les pouvoirs publics entourent leurs politiques, lois et pratiques en matière de surveillance, qui entrave tout effort pour vérifier la compatibilité de ces dernières avec le droit international des Droits de l'homme et à mettre en jeu les responsabilités » et préconise l'instauration d'« un dialogue entre toutes les parties prenantes intéressées, y compris les États membres, la société civile, les communautés scientifiques et techniques, les entreprises, les universitaires et les spécialistes des Droits de l'homme¹⁹ ».

De même, le rapporteur spécial du Conseil des droits de l'homme sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste présenta au conseil et à

16. A/RES/68/178, p. 4.

17. A/RES/69/166, p. 2 : « les métadonnées sont des informations périphériques aux données visant à les décrire dans leur contexte que celles-ci soient ou non structurées » ; Charlotte Maday et Marion Taillefer, « Un exemple de gouvernance des données à l'heure du numérique : les métadonnées du *records management* », dans Irène Bouhadana et William Gilles (dir.), *op. cit.*, p. 157 ; parfois appelées « données sur les données », il s'agit de données techniques afférentes à l'identification des numéros d'abonnement ou de connexion (« données de connexion ») à des services de communication électronique, y compris les factures détaillées (« fadettes »), elles comprennent les numéros appelés et appelant ainsi que la durée et la date des communications, ou à la localisation des équipements terminaux utilisés, à l'exclusion du contenu des communications.

18. *Metadata absolutely tells you everything about somebody's life. [...] If you have enough metadata you don't really need content... [It's] sort of embarrassing how predictable we are as human beings*, (Stewart Baker, cité par Alan Rusbridger, « The Snowden Leaks and the Public », *The New York Review of Books*, 21 novembre 2013, disponible en ligne à l'adresse suivante : <http://www.nybooks.com> [consulté le 27 novembre 2015]).

19. A/HRC/27/37, p. 18.

l'assemblée un rapport afférent notamment à la lutte antiterroriste et à la surveillance numérique de masse duquel il ressort que l'utilisation de cette surveillance « élimine en fait purement et simplement le droit au secret des communications sur l'Internet [...] élimine la possibilité de toute analyse individualisée de la proportionnalité²⁰ ».

Cette surveillance indiscriminée et disproportionnée diffère du contrôle mené par la police judiciaire ou les services fiscaux²¹, des mesures opérationnelles d'Europol ou de la coopération et de l'échange d'informations entre les autorités répressives²² qui ciblent des personnes déjà condamnées ou fortement suspectées dans le cadre de procédures contrôlées par des magistrats. Les règles strictes en matière de protection des données personnelles telles que celles qui s'imposent à Europol ou à la coopération policière offrent des garanties satisfaisantes, conciliant lutte contre le terrorisme et vie privée²³. Il en va différemment en matière de prévention du terrorisme, voire de la criminalité, où la tentation est grande d'accumuler toutes les informations possibles pour obtenir les meilleurs renseignements au risque d'un fichage de l'ensemble de la population. Risque d'autant plus grand que les services spécialisés opèrent généralement en dehors de tout cadre juridique. Il revient donc au législateur de s'emparer de la question pour assurer « la conciliation entre le respect de la vie privée et d'autres exigences constitutionnelles, telles que [...] la prévention d'atteintes à l'ordre public²⁴ » dont le terrorisme qui est à l'évidence la plus grave. Les répercussions des révélations d'Edward

20. A/69/397, p. 5.

21. Voir Xavier Cabannes, « L'administration fiscale et l'obtention de données sur le contribuable à l'ère du numérique », dans Irène Bouhadana et William Gilles (dir.), *op. cit.*, p. 98-101.

22. Voir Céline Castets-Renard, *Droit de l'internet*, Paris, Montchrestien, 2^e éd., 2012, p. 469-470.

23. Voir André Gattolin, Dominique Bailly, Pierre Bernard-Reymond et Colette Mélot, *Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust : perspectives d'avenir*, Sénat, 17 avril 2014, p. 17-19; Angeles Gutierrez-Zarza, *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Heidelberg, Springer, 2015, p. 95.

24. Cons. const., déc. n° 2011-209 QPC, 17 janv. 2012, M. Jean-Claude G. (procédure de dessaisissement d'armes), cons. 3.

Snowden²⁵ concernant le « piratage d'État²⁶ » auquel se livrent les États-Unis d'Amérique ont conduit la France – mais aussi le Canada, la Suisse et le Luxembourg²⁷ – à légiférer sur les services de renseignement et sur l'accès de ceux-ci à des données personnelles dans le cadre d'actions préventives. En ce qui concerne notre pays, ce n'est toutefois pas une nouveauté car la législation antiterroriste prévoyait déjà des contrôles préventifs (1), mais la loi nouvelle éclaire la matière d'un jour nouveau, même si persistent des zones d'ombres (2).

25. Voir Conseil d'État, *op. cit.*, p. 202-207 ; Antoine Lefébure, *L'affaire Snowden. Comment les États-Unis espionnent le monde*, Paris, La Découverte, 2014, 275 p. ; le Conseil de l'Europe s'est particulièrement intéressé à la question : voir le rapport commandité par la Conférence des ministres responsables des médias et de la société de l'information : Raegan MacDonald, Jochai Ben-Avie et Fabiola Carrion, *Liberté sur internet et droit à la vie privée, protection des données à caractère personnel et respect des formes légales*, MCM(2013)008, disponible en ligne à l'adresse suivante : <http://www.accesnow.org> (consulté le 27 novembre 2015) ; et le rapport pour la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire : Pieter Omtzigt, *Les opérations de surveillance massive*, doc. 13734, 18 mars 2015, disponible en ligne à l'adresse suivante : <http://assembly.coe.int> (consulté le 27 novembre 2015) ; l'Union européenne n'a pas été en reste : voir le rapport de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen : Claude Moraes, *Rapport sur la programme de surveillance de la N.S.A., les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures*, 21 février 2014, A7-0139/2014 et les études commanditées par l'Unité d'évaluation des choix scientifiques et technologiques du PE (STOA) : *Mass Surveillance Part 1. Risks, Opportunities and Mitigation Strategies*, janvier 2015, IP/G/STOA/FWC-2013-1/LOT9/C5/SC1, PE 527.409 et *Mass Surveillance Part 2. Technology Foresight*, janvier 2015, IP/G/STOA/FWC-2013-1/LOT4/SC1, PE 527.410.

26. L'expression est empruntée à Xavier Raufer, *Cyber-criminologie*, Paris, CNRS, 2015, p. 147.

27. Au Luxembourg, le projet de loi n° 6675/05 portant réorganisation du service de renseignement de l'État est toujours en cours de discussion ; voir CE, avis, 19 déc. 2014 et avis complémentaire, 22 juin 2015 ; Commission nationale pour la protection des données, avis, 31 juill. 2014, disponible en ligne à l'adresse suivante : <http://www.chd.lu> (consulté le 27 novembre 2015) ; pour une appréciation critique, voir Association Luxembourg ouvert et solidaire-Ligue des droits de l'homme, *Avis sur le projet de loi portant organisation du Service de Renseignement de l'État (dossier parlementaire 6675)*, 4 mai 2015, disponible en ligne à l'adresse suivante : <http://www.ldh.lu> (consulté le 27 novembre 2015).

1. L'arsenal législatif en matière de renseignement antiterroriste avant l'adoption de la loi relative au renseignement

Le recueil de données personnelles aux fins de prévention du terrorisme est organisé depuis près d'une décennie en ce qui concerne les voyageurs (1.1) et depuis plus de quinze ans pour les interceptions de communications, domaine qui n'a cessé de s'étendre (1.2).

1.1. Le contrôle des données personnelles des voyageurs

Les attentats perpétrés à Paris en janvier 2015 ont remis en selle le recueil des données *Passenger Name Record* (PNR²⁸). Il serait urgent d'adopter au niveau français comme au niveau européen un fichage généralisé menaçant, selon un ancien président de la CNIL, de mettre « la vie privée en péril²⁹ » alors même que l'efficacité de ces mesures est loin d'être prouvée. Il est, d'ailleurs, pour le moins ironique d'entendre plaider pour instituer un tel contrôle en France alors qu'il existe déjà ! (1.1.1). En revanche, au niveau européen, il est encore en gestation (1.1.2).

1.1.1. La mise en place subreptice d'un PNR à la française

L'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme autorise la collecte des données PNR et *Advance Passenger Information* (API³⁰) à l'occasion de déplacements internationaux en provenance ou à destination d'États tiers à l'Union européenne. Sont également concernées les données directement collectées à partir de la bande de lecture optique des documents de voyage, de la carte d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires.

En outre, un arrêté du 19 décembre 2006 institue, à titre expérimental, un fichier des passages aériens qui ne concerne que les données API des passagers de vols directs en provenance et à destination de l'Afghanistan,

28. Données contenues dans les dossiers des passagers aériens, collectées par les agences de voyage et les compagnies aériennes lors de la réservation du vol ; il s'agit notamment des données nominatives, sur les moyens de paiement et, éventuellement, relatives au régime alimentaire ou l'état de santé, voire afférentes aux contacts du passager.

29. Alex Türk, *La vie privée en péril. Des citoyens sous contrôle*, Paris, Odile Jacob, 2011.

30. Données recueillies par les compagnies aériennes lors de la phase d'enregistrement des passagers sur un vol.

du Pakistan, de l'Iran, de la Syrie et du Yémen. Toutefois, l'expérimentation a surtout révélé « un manque de rigueur dans la transmission des données par certaines compagnies et [...] la multiplicité d'erreurs imputables à des homonymies ou à des transcriptions inexactes des noms³¹ ».

Par ailleurs, l'article 65 du code des douanes permet expressément à l'administration douanière de requérir ponctuellement les données PNR de certains vols.

Enfin, l'article L. 232-7 du code de la sécurité intérieure (CSI), résultant de la loi de programmation militaire de 2013, institue le *système API-PNR France*, dont les données sensibles sont expressément exclues, pour les vols au départ ou à destination de la France, mis en œuvre par le décret n° 2014-1095 du 26 septembre 2014 – lequel crée les articles R. 232-12 à R. 232-18 CSI – et par le décret n° 2014-1566 du 22 décembre 2014 portant création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP), ainsi que par le décret n° 2015-1328 du 21 octobre 2015³². Ce système a été considéré comme satisfaisant par la CNIL car les garanties offertes réduisent le risque d'atteinte à la protection des données personnelles³³.

1.1.2. La question d'un éventuel PNR européen

En novembre 2007, la Commission européenne avait présenté une proposition de directive pour établir un PNR européen aux fins de prévention du terrorisme qui fut rejetée l'année suivante par le Parlement européen, les vicissitudes des accords PNR avec les États-Unis³⁴ et des

31. Claudine Guerrier, « Passenger Name Record 2012 », 2 juillet 2012, disponible en ligne à l'adresse suivante : <http://www.juriscom.net> (consulté le 27 novembre 2015).

32. Décret portant modification de l'article 5 du décret n° 2010-569, 28 mai 2010 relatif au fichier des personnes recherchées et des articles R. 232-14 et R. 232-15 du code de la sécurité intérieure.

33. Délib. n° 2014-308, 17 juillet 2014 portant avis sur un projet de décret relatif à la création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure et fixant les modalités de transmission au service à compétence nationale « Unité Information Passagers » des données relatives aux passagers par les transporteurs aériens.

34. Voir Marie-Françoise Labouz, « Le nouvel accord sur les données de passagers aériens (PNR) entre l'Union européenne et les États-Unis », dans Emmanuelle Saulnier-Cassia (dir.), *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne*, Paris, LGDJ, 2014, p. 265-275 ; Philippe Guillot, « Protection des données à caractère personnel et lutte anti-terrorisme : l'Accord U.E.-É.U. sur les dossiers de passagers aériens (P.N.R.) », *Annales de droit*, n° 2, 2008, p. 37-57.

accords dits *Society for Worldwide Interbank Financial Transactions – Terrorist Finance Tracking Program (SWIFT-TFTP)*³⁵ y étant pour beaucoup. La commission présenta, en 2011, une nouvelle proposition³⁶, mais le parlement s’y opposa le 24 avril 2013, ce qui n’a pas empêché la commission de participer au financement de projets PNR nationaux dans la moitié des États membres.

Le 11 janvier 2015, le ministre français de l’Intérieur a exhorté le Parlement européen à adopter la directive PNR européen, demande relayée le surlendemain par le président du Conseil européen qui craint qu’en l’absence d’une telle directive ne se mettent en place vingt-huit systèmes nationaux formant un « patchwork rempli de lacunes ». Cependant, de nombreux eurodéputés subordonnent leur vote à la prochaine décision de la cour sur l’accord PNR avec le Canada³⁷.

En attendant, le 11 février 2015, le parlement a adopté une résolution par laquelle il s’engage à tout mettre en œuvre pour finaliser la directive PNR et encourage les États membres à progresser sur le « paquet relatif à la protection des données » – c’est-à-dire le règlement³⁸ devant remplacer la directive 95/46 et la directive³⁹ devant se substituer à la décision-cadre 2008/977/JAI. Le 9 juillet, dans une nouvelle résolution, il a confirmé son engagement et encouragé le Conseil de l’Union européenne à progresser sur le « paquet » de sorte que les trilogues – négociations entre le parlement, le conseil et la commission – « puissent avoir lieu parallèlement », tout en insistant sur la nécessité pour la future directive PNR de respecter les droits fondamentaux et la

35. Voir Philippe Guillot, « The War on Terror and the Protection of Personal Data », *Montesquieu Law Review*, n° 2, 2015, p. 49-50 ; Constance Chevallier-Govers, « Personal Data Protection: Confrontation between the European Union and the United States of America », dans Yann Echinard, Albane Geslin, Michel Gueldry et Fabien Terpan (dir.), *L’Union européenne et les États-Unis. Processus, politiques et projets*, Bruxelles, Larcier, 2013, p. 162-166 ; Juan Santos Vara, « The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon », *CLEER Working Papers*, n° 2, 2013, p. 12-20 ; Valentin Pfisterer, « The Second SWIFT Agreement Between the European Union and the United States of America », *German Law Journal*, vol. XXI, n° 10, 2010, p. 1175-1180 ; Matthew R. VanWasshova, « Data Protection Conflicts Between the United States and the European Union in the War on Terror », *Case Western Reserve Journal of International Law*, n° XXXIX, 2007-2008, p. 839-846.

36. COM(2011)32 final.

37. Voir Sylvie Peyrou, « Le PNR européen à la croisée des chemins : protection des données et lutte contre le terrorisme », 25 janvier 2015, disponible en ligne à l’adresse suivante : <http://www.gdr-elsj.eu> (consulté le 27 novembre 2015).

38. COM(2012)11 final.

39. COM(2012)10 final.

protection des données personnelles, y compris telle qu'interprétée dans la jurisprudence de la Cour de justice⁴⁰. Le 2 décembre, les négociateurs du PE et du Conseil ont conclu un accord sur la directive laquelle a été adoptée par le PE le 14 avril 2016 (461 pour, 179 contre, 9 abstentions), qui a aussi voté en faveur du « paquet sur la protection des données »

1.2. L'extension progressive de la surveillance cybernétique

En matière de prévention du terrorisme, la cybersurveillance légale remonte à 1991 et a été constamment élargie jusqu'en 2013 avec la loi de programmation militaire qui en unifie le régime (1.2.1). Là encore, il faut tenir compte des développements en droit de l'Union européenne (1.2.2).

1.2.1. Une législation française étendant le domaine de la surveillance des données personnelles

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques fut la première à permettre des interceptions de sécurité aux fins de prévention du terrorisme⁴¹. Le ministre de la Défense, celui de l'Intérieur et celui chargé des Douanes adressaient alors des demandes d'avis préalable à la Commission nationale de contrôle des interceptions de sécurité (CNCIS), sauf en cas d'extrême urgence. Néanmoins, en 2003, à la demande du président de la CNCIS le contrôle *a priori* fut étendu aux cas d'extrême urgence.

La loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers avait introduit dans le code des postes et communications électroniques l'article L. 34-1-1 qui disposait : « Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des [opérateurs de communications électroniques et des fournisseurs d'accès à des services en ligne ou à des stockages de signaux de toute nature] la communication

40. P8_TA-PROV(2015)0269, § 27.

41. Codifiée à l'article L. 241-2 du code de la sécurité intérieure (ci-après « CSI »), la liste des motifs justifiant les interceptions comprenait aussi « la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention [...] de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ».

des données conservées et traitées par ces derniers », étant précisé que ces données « sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ». Ces dispositions étaient initialement provisoires, mais elles furent prorogées en 2008 et en 2012, avant d'être réformées par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

Cette loi a unifié le cadre juridique de l'accès aux données de connexion et de la géolocalisation en temps réel en matière administrative en créant l'article L. 246-1 CSI, lequel rend possible le recueil auprès des opérateurs de communications électroniques des « informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques » dont les données techniques précédemment décrites par l'ancien article L. 34-1-1 du code des postes et communications électroniques. L'article L. 232-7-I CSI permet aussi aux services de renseignement – y compris militaires – de créer un traitement automatisé des données personnelles sous le contrôle de la CNCIS qui se prononce *a posteriori*⁴².

L'article L. 222-1 CSI dispose que « les agents individuellement habilités des services de police et de gendarmerie nationales » chargés de la lutte contre le terrorisme ainsi que ceux des services de renseignement, peuvent avoir accès au fichier national des immatriculations, au système national de gestion des permis de conduire, à celui des cartes nationales d'identité, à celui des passeports, au système informatisé de gestion des dossiers des ressortissants étrangers en France et aux données personnelles des étrangers en situation irrégulière – mais non au fichier de l'Office français de protection des réfugiés et des apatrides (OFPRA), le Conseil constitutionnel ayant considéré que « la confidentialité des éléments d'information détenus par l'OFPRA relatifs à la personne sollicitant en France la qualité de réfugié est une garantie essentielle du droit d'asile, principe de valeur constitutionnelle qui implique notamment

42. Voir Emmanuel Dupic, *Droit de la sécurité intérieure*, Issy-les-Moulineaux, Gualino, 2014, p. 98-99, 374-375 (interceptions de sécurité administratives) et 378-379 (géolocalisation administrative).

que les demandeurs du statut de réfugié bénéficient d'une protection particulière⁴³ » et que seuls les agents de l'OFPPRA peuvent accéder à ce fichier⁴⁴.

L'article L. 234-4 CSI autorise les personnels dûment habilités des services de renseignement à avoir « accès aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6 du code de procédure pénale⁴⁵, y compris pour les données portant sur des procédures judiciaires en cours et à l'exclusion de celles relatives aux personnes enregistrées en qualité de victimes ».

Les articles L. 246-1 à L. 246-5 CSI⁴⁶ obligeaient les opérateurs de communication à conserver pendant un an l'ensemble des métadonnées pour répondre, en temps réel, aux demandes des services de lutte anti-terroriste ou de renseignement. Les associations *French Data Network*, la Quadrature du Net et Fédération des fournisseurs d'accès à internet associatifs ont, à l'occasion d'un recours en excès de pouvoir devant le Conseil d'État à l'encontre du décret n° 2014-1576 du 26 décembre 2014 relatif à l'accès administratif aux données de connexion, soulevé une question prioritaire de constitutionnalité sur ces articles arguant, d'une part, de l'imprécision d'un certain nombre de définitions relatives aux données⁴⁷ pouvant faire l'objet de la procédure de recueil et à la procédure en elle-même, et, d'autre part, de l'absence de garanties particulières prévues pour les avocats et les journalistes par ladite procédure.

43. Cons. const., déc. n° 97-839 DC, 22 avr. 1997, *Loi portant diverses dispositions relatives à l'immigration*, § 26.

44. En revanche, au niveau européen, le système d'information Eurodac qui contient, entre autres, des données personnelles des demandeurs d'asile est consultable par d'autres agents que les officiers de protection. Voir François Lafarge, « L'accès des services répressifs des États membres et d'Europol à Eurodac », dans *Europe(s), Droit(s) européen(s). Une passion d'universitaire. Liber Amicorum en l'honneur du professeur Vlad Constantinesco*, Bruxelles, Bruylant, 2015, p. 327-341.

45. Il s'agit des « fichiers d'antécédents » comprenant des données personnelles recueillies « 1° au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant a) un trouble à la sécurité ou à la tranquillité publiques ; b) une atteinte aux personnes, aux biens ou à la sécurité de l'État ; 2° au cours des procédures de recherches de la mort [en cas de découverte d'un cadavre] ou de recherches des causes d'une disparition [venant d'intervenir ou d'être constatée] ».

46. Devenus les articles L. 851-1 et L. 851-4 du même code avec la loi relative au renseignement, les articles L. 246-2, L. 246-4 et L. 246-5 étant abrogés.

47. Les requérants soutenaient que l'absence de définition légale des notions « informations ou documents », « opérateurs de communications électroniques » et « sollicitation du réseau » portait atteinte au respect de la vie privée.

Considérant que le législateur avait prévu des garanties suffisantes, le Conseil constitutionnel a déclaré les dispositions contestées conformes à la Constitution⁴⁸.

L'appareil de prévention du terrorisme était donc déjà bien développé avant l'adoption de la loi relative au renseignement mais, d'une part, ces textes composaient une « mosaïque extrêmement complexe, peu lisible voire irrationnelle⁴⁹ » et, d'autre part, les missions des services de renseignement étaient mal définies et leurs actions se déroulaient souvent à la lisière de la légalité.

1.2.2. Le coup d'arrêt de la cour de justice de l'Union européenne à la captation et à la conservation excessives des données personnelles

Suite aux attentats de Madrid et de Londres, l'Union européenne avait adopté la directive 2006/24/CE du 15 mars 2006 relative à la conservation des données afin d'harmoniser les mesures nationales obligeant les fournisseurs de télécommunication et de services informatiques à conserver les métadonnées – et non le contenu des communications ou des sites internet visités – de leurs clients pour les transmettre sur requête aux services de police ou de renseignement. La cour de justice fut saisie de deux questions préjudicielles sur la compatibilité de cette directive avec la CFDUE ; elle trancha en faveur de l'incompatibilité étant donné que « ces données, prises dans leur ensemble, [étaient] susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées⁵⁰ », ce qui constituait une « ingérence [...] d'une vaste ampleur [...] susceptible de générer dans l'esprit des personnes concernées [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante », d'autant plus que la directive couvrait « de manière généralisée toute personne et tous les moyens de communication électronique », ne prévoyait « aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure⁵¹ » et que la durée de conservation

48. Cons. const., déc. n° 2015-478 QPC, 24 juil. 2015, Association *French Data Network* e. a. (accès administratif aux données de connexion).

49. Jean-Jacques Urvoas, *Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi (n° 2669) relatif au renseignement*, Assemblée nationale, 2 avril 2015, p. 13.

50. CJUE, Gr. Ch., 8 avr. 2014, *Digital Rights Ireland & Seitleinger*, aff. C-293/12 et C-594/12, § 27.

51. *Ibid.*, § 37, 57, 60.

était fixée sans tenir compte de l'utilité de la conservation par rapport aux objectifs poursuivis⁵².

Cette décision, saluée comme une nette interdiction de la cybersurveillance massive⁵³ et une victoire sur la « codification de l'arbitraire⁵⁴ », devrait avoir, selon une étude juridique commanditée par Les Verts/ Alliance Libre Européenne, des répercussions substantielles notamment sur l'accord PNR euro-états-unien⁵⁵, sur le projet PNR européen⁵⁶, sur l'accord *SWIFT-TFTP* et le projet d'institution d'un système européen de traçage du financement du terrorisme⁵⁷ présenté par la commission⁵⁸, sur Eurodac ainsi que les systèmes d'information de Schengen (SIS) et sur les visas (VIS) et sur les mesures nationales des États membres⁵⁹. Ces derniers, compte tenu de l'invalidation de la directive 2006/24/CE, n'ont plus l'obligation de demander aux opérateurs de téléphonie ou de communications électroniques l'accès aux métadonnées ; néanmoins, ils conservent la possibilité de le faire mais en respectant les principes de nécessité et de proportionnalité⁶⁰.

Ce n'est pourtant pas la voie que suit la France avec la loi relative au renseignement.

2. La loi relative au renseignement

Auparavant, les services spécialisés de renseignement avaient, selon l'adage militaire, « tous les droits sauf celui de se faire prendre » ; désormais, grâce à la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, ils sortent de l'ombre. Ainsi que le note un éminent spécialiste du droit de la défense et du droit des technologies de

52. *Ibid.*, § 63 et 64 ; sur cet arrêt voyez la note d'Ariane Wiedmann, « Chronique de jurisprudence de la Cour de justice et du Tribunal de l'Union européenne (avril-juin 2014) », RAE 2014, p. 423-432 ; Conseil d'État, *op. cit.*, p. 197-201.

53. Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », RDH 2014 (<http://revdh.revues.org/746>, consulté le 8 novembre 2015).

54. Tijmen Wisman, « Privacy: Alive and Kicking », *European Data Protection Law Review*, vol. I, n° 1, 2015, p. 84.

55. Voir Franziska Boehm et Mark D. Cole, *Data Retention after the Judgement of the Court of Justice of the European Union*, Münster, Luxembourg, 30 juin 2014, p. 58-65 (<http://www.janalbrecht.eu>, consulté le 8 novembre 2015).

56. *Ibid.*, p. 65-71.

57. COM(2013)842 final.

58. Voir Franziska Boehm et Mark D. Cole, *op. cit.*, p. 71-78.

59. *Ibid.*, p. 79-83 et 92-94.

60. Sur les principes de nécessité et de proportionnalité, voir avis 01/2014 du G 29 du 27 février 2015.

l'information et de la communication : « ces services devront pouvoir justifier en toutes circonstances (et non seulement à l'occasion de la mise en œuvre de telle ou telle technique de recueil d'information) qu'ils agissent dans les limites et au profit des finalités définies par la loi [...] là où les services d'État estimaient usuellement que leur légitimité l'emportait par principe et en toutes circonstances sur toute autre considération politique ou juridique (conformément à la doctrine implicite de la "raison d'État"), ils devront désormais vivre dans le respect du principe inverse, leurs prérogatives n'étant admises qu'à la condition qu'elles soient justifiées et strictement proportionnées à l'objectif public recherché⁶¹ ». Toutefois, si les actions des services spécialisés de renseignement entrent dans la lumière (2.1), cette dernière est quand même plutôt tamisée (2.2).

2.1. La mise en lumière du renseignement

L'article L. 811-1 CSI dispose : « La politique publique de renseignement concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation. Elle relève de la compétence exclusive de l'État ». Introduite par le *Livre blanc Défense et sécurité nationale* de 2008 et reprise dans celui de 2013, la notion de « sécurité nationale » estompe la distinction classique entre la sécurité extérieure et la sécurité intérieure. Il en découle une tentative de mise en synergie des services civils et militaires – ces derniers étant chargés par le Livre blanc d'une fonction de « connaissance et anticipation⁶² » – l'esprit de la loi étant de favoriser « la centralisation des données collectées au moyen des techniques de renseignements, seule à même de permettre l'organisation d'un contrôle effectif du cadre légal⁶³ ». Il sied de présenter les services spécialisés de renseignement (2.1.1) avant d'envisager les motifs pour lesquels ils peuvent recueillir des données personnelles (2.1.2).

61. Bertrand Warusfel, « Loi sur le renseignement : des avancées essentielles, au-delà des malentendus », 11 avril 2015, disponible en ligne à l'adresse suivante : <https://hestia.hypotheses.org> (consulté le 27 novembre 2015).

62. Voir *Livre blanc Défense et sécurité nationale*, 2013, p. 70-75, disponible en ligne à l'adresse suivante : <http://www.livreblancdefenseetsecurite.gouv.fr> (consulté le 27 novembre 2015).

63. CE, avis sur un projet de loi relatif au renseignement, 12 mars 2015, NOR : PRMX1504410L, § 6.

2.1.1. Les services spécialisés de renseignement

Les services spécialisés de renseignement visés à l'article L. 811-2 CSI sont exhaustivement énumérés par l'article R. 811-1 du CSI⁶⁴ ; il s'agit de la direction générale de la sécurité extérieure (DGSE⁶⁵), de la direction de la protection et de la sécurité de défense (DPSD⁶⁶), de la direction du renseignement militaire (DRM⁶⁷), de la direction générale de la sécurité intérieure (DGSi⁶⁸), de la direction nationale du renseignement et des enquêtes douanières (DNRED⁶⁹) et du service à compétence

64. Introduit par le décret n° 2015-1185, 28 sept. 2015.

65. Dépendante du ministère de la Défense mais composée à 30 % seulement de militaires, la DGSE recherche à l'étranger les informations intéressant la défense et la sécurité, maintient une présence là où les canaux diplomatiques ne peuvent plus être utilisés et dispose d'une capacité d'entrave et d'action clandestine ; sa direction du renseignement comprend les services de contre-prolifération, de contre-terrorisme, de sécurité économique et de renseignement géopolitique et de contre-espionnage. Voir Emmanuel Dupic, *op. cit.*, p. 364-366 ; voir aussi, par son directeur général, Bernard Bajolet, « La DGSE, outil de réduction de l'incertitude ? », *Revue Défense nationale*, n° 766, janvier 2014, p. 27-31. Le statut des fonctionnaires de la DGSE a été modifié par le décret n° 2015-386, 3 avr. 2015.

66. Service de renseignement du ministère de la Défense, la DPSD a une mission globale de « contre-ingérence défense » (protection des personnels, matériels, informations et installations sensibles contre le terrorisme, l'espionnage, le sabotage ou le crime organisé) ; elle contrôle la protection du secret de la défense nationale, elle s'assure de la sécurité économique des entreprises liées au ministère, elle surveille le commerce des armements et contribue à la sécurité des forces en opération. Voir Emmanuel Dupic, *op. cit.*, p. 370-372.

67. Relevant du chef d'état-major des armées, la DRM est spécialisée dans le renseignement d'intérêt militaire (ce qui a ou pourrait avoir des conséquences sur les forces et les intérêts nationaux) ; service essentiellement opérationnel et technique, la DRM appuie la planification et la conduite des opérations mais elle pratique également une veille stratégique permanente. Voir Emmanuel Dupic, *op. cit.*, p. 367-370 ; Pauline Fayolle, « Le renseignement d'intérêt militaire : indépendance nationale et perspectives européennes », *Revue Défense nationale*, n° 766, janvier 2014, p. 107-112 et l'entretien du général Christophe Gomart (directeur du renseignement militaire) accordé à *Défense et sécurité internationale*, hors-série, n° 43 (« La France face au terrorisme »), septembre 2015, p. 56-59.

68. Créée en 2014, la DGSi remplace la direction centrale du renseignement intérieur – elle-même née en 2008 de la fusion des renseignements généraux et de la direction de la sûreté du territoire – et est placée directement sous l'autorité du ministre de l'Intérieur ; elle est chargée, sur l'ensemble du territoire, de rechercher, de centraliser et d'exploiter le renseignement intéressant la sécurité nationale et les intérêts fondamentaux de la nation. Voir Emmanuel Dupic, *op. cit.*, p. 361-364.

69. Dépendant du ministère de l'Économie et du Budget, la DNRED comprend trois directions fonctionnelles : la direction du renseignement douanier (chargée notamment de la détection des transactions illicites sur l'internet), la direction des enquêtes douanières (qui procède aux enquêtes contre les fraudes d'importance

nationale « Traitement du renseignement et action contre les circuits financiers clandestins » (TRACFIN⁷⁰). Cependant, conformément à l'article L. 811-4 CSI, le décret n° 2016-67 du 29 janvier 2016 désigne les autres services pouvant être autorisés à mettre en œuvre des techniques de renseignement dans l'article R.851.1-1 : les services compétents en lutte antiterroriste de la direction centrale de la police judiciaire, de la direction centrale de la sécurité publique, de la direction régionale de la police judiciaire de Paris et de la gendarmerie (nationale, maritime, de l'air et de l'armement).

Selon l'article L. 811-2 CSI, ces services spécialisés « ont pour missions, en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation ». « Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et menaces. »

Sur ce dernier point, la loi relative au renseignement permet de passer à l'offensive puisque l'article L. 861-2 CSI dispose : « Pour l'exercice d'une mission intéressant la défense et la sécurité nationale, les agents des services spécialisés [...] peuvent, sous l'autorité de l'agent chargé de superviser ou de coordonner la mission, faire usage d'une identité d'emprunt ou d'une fausse qualité ». L'article L. 863-1 précise qu'ils peuvent ainsi être en contact avec des personnes susceptibles de porter atteinte aux intérêts fondamentaux de la nation et extraire, acquérir ou conserver des données sur ces personnes. La collecte de données sur de telles personnes – nécessairement identifiées de manière précise – n'a rien de contraire au droit des données personnelles car la justification semble claire de prime abord. Néanmoins, les motifs autorisant les autres formes de surveillance – moins intrusives mais portant sur une

nationale ou internationale) et la direction des opérations douanières (chargée de la lutte contre les contrebandes, de la recherche de renseignements opérationnels et de la mise en œuvre de techniques d'investigation spécialisées). Voir Emmanuel Dupic, *op. cit.*, p. 372-373.

70. La « cellule TRACFIN » du ministère des Finances a été créée en 1990 afin d'être le correspondant français du Groupe d'action financière internationale (GAFI) chargé de la lutte contre le blanchiment d'argent et les circuits financiers clandestins – puis contre le financement du terrorisme et de la prolifération d'armes de destruction massive ; depuis 2006, TRACFIN est devenue un service à compétence nationale qui comprend notamment un département de l'analyse, du renseignement et de l'information et un département des enquêtes. Voir Emmanuel Dupic, *op. cit.*, p. 72-80.

population beaucoup plus large – ne brillent pas nécessairement par leur clarté.

2.1.2. Des motifs d'intérêt public guère lumineux

L'article L. 811-3 CSI énumère sept motifs d'intérêt public qui autorisent l'utilisation de dispositifs techniques permettant la captation, la transmission et l'enregistrement de données informatiques transitant dans un système automatisé de données ou contenues dans un tel système, ainsi que des dispositifs de sonorisation de lieux ou de véhicules. Allant bien au-delà de la seule lutte contre le terrorisme, il s'agit de :

1. L'indépendance nationale, l'intégrité du territoire et la défense nationale.
2. Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère.
3. Les intérêts économiques, industriels et scientifiques majeurs de la France.
4. La prévention du terrorisme.
5. La prévention :
 - a) des atteintes à la forme républicaine des institutions ;
 - b) des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;
 - c) des violences collectives de nature à porter gravement atteinte à la paix publique.
6. La prévention de la criminalité et de la délinquance organisées.
7. La prévention de la prolifération des armes de destruction massive.

Selon le ministre de l'Intérieur, ces finalités sont « plus précises que celles figurant dans les normes conventionnelles⁷¹, ou que les notions constitutionnelles de “sécurité nationale” et “d'intérêts fondamentaux

71. Le ministre fait explicitement référence aux motifs pouvant justifier une ingérence dans la vie privée aux termes de l'article 8 § 2 de la Convention européenne des droits de l'homme et des libertés fondamentales (CSDHLE) : sécurité nationale, sûreté publique, bien-être économique du pays, défense de l'ordre et prévention des infractions pénales, protection de la santé ou de la morale et protection des droits et protection d'autrui.

de la Nation⁷² ». Il convient toutefois de noter que l'adjectif « majeurs » utilisé aux 2. et 3. paraît recouvrir un plus large spectre d'intérêts que ceux induits par l'adjectif « fondamentaux » employé par l'article 410-1 du code pénal⁷³ ou par le qualificatif « essentiels » figurant dans le projet de loi. Si certains parlementaires se sont contentés de souligner l'imprécision du 2., en revanche, le remplacement d'« essentiels » par « majeurs » dans le 3. a fait naître plus d'inquiétude parce qu'il traduirait une finalité plus large, à savoir « la surveillance économique et industrielle dans son ensemble », laquelle pourrait justifier les interceptions des communications des personnalités économiques, syndicales et scientifiques ou des opposants au nucléaire⁷⁴, ce qui ferait des services spécialisés – notamment de la DGSI – une police politique.

Si les 1., 4. et 6., voire le 5.b, sont des raisons dont la légitimité ne fait guère de doutes, en revanche, les autres motifs sont plus contestables. Le 5.a surprend de prime abord, les attentats perpétrés par les camelots du roi n'ayant plus défrayé la chronique ces dernières décennies. S'agirait-il alors de contrer ceux qui désireraient instaurer un émirat islamique en France ? Il ne semble pas que ce soit l'objectif immédiat des djihadistes qui cherchent avant tout à peser sur notre politique étrangère perçue comme colonialiste – ce qui entre dans le champ du 2. au cas où le 4. ne trouverait pas application – plutôt que de renverser notre régime politique. Comme l'invocation de la République ou des valeurs républicaines est récurrente dans les discours politiques et les lois ces dernières années, on peut avancer l'idée que la « forme “républicaine” semblerait revendiquer l'ensemble des libertés individuelles et collectives et mettre en cause certaines mouvances politiques⁷⁵ ». Seraient ainsi visés non seulement les islamistes radicaux, mais aussi les « identitaires », les indépendantistes, voire l'ultra-gauche comme l'a démontré l'affaire de

72. Bernard Cazeneuve, *Lettre du 24 avril 2015 à Madame Christine Lazergues, Présidente de la Commission nationale consultative des droits de l'Homme*, p. 6.

73. Les intérêts fondamentaux de la nation y sont définis comme la défense de l'indépendance, de l'intégrité du territoire, de la forme républicaine des institutions, des moyens de la défense et de la diplomatie, de la sauvegarde de la population en France et à l'étranger, de l'équilibre du milieu naturel et de l'environnement et des éléments essentiels du potentiel scientifique et économique et du patrimoine culturel.

74. Voir Claudine Guerrier, « Le nouveau régime d'autorisations dans la loi sur le renseignement : une rupture avec la loi de 1991 ? », 29 septembre 2015, disponible en ligne à l'adresse suivante : <http://www.juriscom.net> (consulté le 27 novembre 2015).

75. *Ibid.* Cet auteur cite les déclarations opposées au 5.a des députés Marion Maréchal-Le Pen (FN) et Sergio Corodano (EELV), ce dernier s'inquiétant au sujet des anarchistes et des régionalistes, voire des monarchistes non violents.

Tarnac même si finalement cette qualification n'a pas été retenue⁷⁶. Si ces différents mouvements autres qu'islamistes peuvent, ponctuellement, représenter une menace pour les biens ou les personnes, une surveillance excessive par sa généralité de l'ensemble des groupes politiques marginaux ferait glisser la société libérale, qui est ontologiquement une société de confiance, vers une société de défiance fatalement liberticide.

Surtout, le 5.c peut faire craindre des dérives en matière de surveillance des mouvements sociaux (agriculteurs, étudiants, chauffeurs de taxi, « zadistes », etc.), la trop grande imprécision de ce motif ayant été dénoncée par différents avis⁷⁷, ainsi que durant les débats parlementaires⁷⁸ et par le mémoire de saisine du Conseil constitutionnel par soixante députés de l'opposition – y compris du Front national – mais aussi de la majorité, et dans le mémoire de réplique aux observations du gouvernement. Certes, il est imaginable que les services spécialisés de renseignement aient suffisamment à faire pour surveiller des éléments terroristes pour ne pas s'occuper en plus de groupes de défense d'intérêts catégoriels, mais graver dans le marbre de la loi un motif aussi imprécis

76. Voir Lucie Soullier, « Comprendre l'affaire Tarnac, désormais sans "terrorisme" », 9 août 2015, disponible en ligne à l'adresse suivante : <http://www.lemonde.fr> (consulté le 27 novembre 2015) ; Michaël Hadjenberg et Fabrice Arfi, « Tarnac : pas de terrorisme malgré une "rhétorique guerrière", selon les juges », 10 août 2015, disponible en ligne à l'adresse suivante : <http://www.mediapart.fr> (consulté le 27 novembre 2015) ; Michaël Bloch, « Tarnac : le parquet de Paris fait appel de l'abandon de la qualification "terroriste" », 10 août 2015, disponible en ligne à l'adresse suivante : <http://www.lejdd.fr> (consulté le 27 novembre 2015).

77. Voir le communiqué de presse du Conseil national du numérique du 19 mars 2015 ; avis du défenseur des droits n° 15-04, 2 avril 2015, p. 3 ; Comité des droits de l'homme (Organisation des Nations unies), *Observations finales concernant le cinquième rapport périodique de la France*, 21 juillet 2015, CCPR/C/FRA/CO/5, § 12, qui affirme notamment : « L'État partie devrait veiller à ce que la collecte et l'utilisation de données relatives aux communications se fasse sur la base d'objectifs légitimes précis et que soient énoncées, en détail, les circonstances exactes dans lesquelles de telles immixtions peuvent être autorisées et les catégories de personnes susceptibles d'être placées sous surveillance ». Voir également le communiqué de l'Observatoire des libertés et du numérique (OLN), « Loi renseignement : tous surveillés ! », 24 mars 2015 (l'OLN réunit la Ligue des droits de l'homme, le Syndicat de la magistrature, le Syndicat des avocats de France, le Centre de coordination pour la recherche et l'enseignement en informatique et société-terminal, le Centre d'étude sur la citoyenneté, l'informatisation et les libertés, et la Quadrature du Net).

78. Devant l'Assemblée nationale, lors de la 2^e séance du 13 avril 2015, le ministre de l'Intérieur a rétorqué aux députés critiques : « Certaines formes de radicalité violente sapent les fondements de la République et de ses valeurs : face à elles, nous devons prendre des mesures de prévention ».

revient à mettre en place une surveillance indiscriminée de toute force contestatrice.

Il est regrettable que le législateur ne se soit pas inspiré de l'article 2 de la loi sur le service canadien du renseignement de sécurité révisée par la « loi de protection du Canada contre les terroristes⁷⁹ » du 18 juin 2015 qui dispose que les menaces envers la sécurité – c'est-à-dire les motifs justifiant la surveillance – ne visent pas « les activités licites de défense, de protestation ou de manifestation qui n'ont aucun lien avec les activités » d'espionnage, de sabotage, ou clandestines influencées par l'étranger, ou bien qui visent à favoriser l'usage de la « violence grave [...] dans le but d'atteindre un objectif politique, religieux ou idéologique » ou encore qui « visent à saper le régime de gouvernement constitutionnellement établi⁸⁰ ».

Enfin, le 7. est indéniablement un motif légitime – et proportionné dans la mesure où il n'est susceptible de concerner qu'une partie des plus réduites de la population – mais comme apparaît redondant avec le 2. puisqu'il ne fait que consacrer l'un des engagements internationaux de la France. Il est vrai que la loi fédérale sur le renseignement de la Confédération helvétique du 25 septembre 2015 contient ce même motif pour justifier la cybersurveillance⁸¹.

En dépit d'une rédaction problématique de bon nombre de motifs d'intérêt public, pour le Conseil constitutionnel, les finalités de l'article L. 811-3 CSI, faisant référence à des intérêts ou des incriminations des codes pénal, de procédure pénale, de la défense ou de la sécurité intérieure, ne sont pas susceptibles de porter des atteintes disproportionnées au droit au respect de la vie privée ou à la liberté d'expression. De surcroît, ces dispositions doivent être combinées avec celles de l'article L. 801-1 « aux termes desquelles la décision de recourir aux techniques

79. Intitulé officiel complet : Loi modifiant la loi sur le service canadien du renseignement de sécurité et d'autres lois ; les autres lois sont la loi renforçant la citoyenneté canadienne et la loi sur l'accès à l'information,

80. Le législateur canadien a été sensible aux critiques portées contre les termes trop vagues du projet initial, voir Association du barreau canadien, *Mémoire sur le projet de loi C-51, loi antiterroriste de 2015*, mars 2015, p. 11-12, disponible en ligne à l'adresse suivante : <http://www.cba.org> (consulté le 27 novembre 2015).

81. L'article 6a 3 est plus précis que la disposition française puisqu'il évoque « la dissémination d'armes nucléaires, biologiques ou chimiques, y compris leurs vecteurs et tous les biens et technologies à des fins civiles ou militaires qui sont nécessaires à leur fabrication (prolifération NBC) ou le commerce illégal de substances radioactives, de matériel de guerre et d'autres biens d'armement ».

de renseignement et les techniques choisies devront être proportionnées à la finalité poursuivie et aux motifs invoqués⁸² ».

Cependant, ces techniques de renseignement posent problème, même si le législateur a tenté de répondre à l'interrogation de Juvénal, *quis custodiet ipsos custodes*⁸³, en instituant la Commission nationale de contrôle des techniques de renseignement (CNCTR).

2.2. Moyens et limites de la cybersurveillance

L'attention du grand public et des médias a semblé se focaliser sur les techniques susceptibles d'être utilisées pour prévenir le terrorisme ou les autres fléaux visés par l'article L. 811-3 CSI, lesquelles sont très intrusives et déconcertantes pour beaucoup de technophiles béats qui découvrirent alors la face obscure de la cybernétique (2.2.1), les débats et polémiques ont finalement assez peu porté sur les timides garanties offertes par la loi relative au renseignement (2.2.2).

2.2.1. Des moyens de surveillance et d'investigation clairement intrusifs

L'article L. 851-1 autorise le recueil auprès des opérateurs de communications électroniques et des personnes assurant, même à titre gracieux, l'accès à des services de communication en ligne, à des stockages de signaux, d'écrits, d'image, de sons ou de messages de toute nature « des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques », les données techniques naguère décrites par l'article L. 34-1-1 du code des postes et communications électroniques. L'article L. 851-2 précise qu'un tel recueil en temps réel ne peut être autorisé pour une durée de deux mois renouvelable que « pour les seuls besoins de la prévention du terrorisme » et l'article L. 851-3 prévoit qu'« il peut être imposé aux opérateurs [...] la mise en œuvre sur leurs réseaux de traitements automatisés destinés [...] à détecter des connexions susceptibles de révéler une menace terroriste », étant précisé que la CNCTR « dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies ». Il s'agit des désormais célèbres « boîtes noires » destinées à détecter, grâce à des algorithmes, des communications suspectes et qui

82. Cons. const., déc. n° 2015-713 DC, 23 juill. 2015, Loi relative au renseignement, cons. 8-11.

83. « Qui gardera les gardiens ? »

mettent nécessairement en œuvre des technologies d'inspection des « paquets en profondeur », lesquelles n'étaient jusqu'à présent expressément autorisées qu'en Russie⁸⁴, mais dont l'utilité est loin d'être démontrée : « étant donné le faible nombre de terroristes dont le comportement peut être étudié, toute tentative d'extrapolation est vouée à générer un grand nombre de "faux positifs" »⁸⁵. »

De plus, l'article L. 871-4 dispose que les opérateurs précités sont tenus d'autoriser, à des fins de contrôle, les membres et les agents de la CNCTR à entrer dans leurs locaux où sont mises en œuvre des techniques de recueil de renseignement.

Surtout, il convient de noter que la CNIL a relevé qu'en raison « du caractère particulièrement intrusif de cette technique et de son utilisation à l'insu des opérateurs sur leurs propres systèmes, [...] les garanties prévues pour préserver les droits et libertés fondamentaux ne sont pas suffisantes pour justifier une telle ingérence dans la vie privée des personnes »⁸⁶. Le législateur passa donc outre et n'a pas non plus suivi l'invitation de l'Autorité de régulation des communications électroniques et des postes (ARCEP) à envisager un rapprochement des différents régimes d'accès administratifs aux données de connexion⁸⁷.

L'article L. 871-1 impose aux personnes « qui fournissent des prestations de cryptologie » de fournir dans les 72 heures aux services spécialisés « les conventions permettant le déchiffrement ». Cette possibilité qui

84. Voir Félix Tréguer, « Feu vert à la surveillance de masse », *Le Monde diplomatique*, juin 2015, p. 4.

85. Evgeny Morozov, « Surveillance : la fausse route française », *Le Monde*, 2 juin 2015, p. 15. « Tout algorithme de détection a une marge d'erreur c'est-à-dire va identifier des personnes sans intention terroriste (des "faux-positifs"). Si la marge d'erreur est de 1 %, ce qui est considéré à ce jour comme très faible, l'algorithme identifiera quelques 600 000 personnes sur une population totale de 60 millions de personnes. Si le nombre de vrais terroristes est par exemple de 60, ces vrais terroristes ne représenteront que 0,01 % de la population identifiée » (Institut national de la recherche en informatique et automatique, *Éléments d'analyse technique du projet de loi relatif au renseignement*, 30 avril 2015, p. 3. « Ce paradoxe [des "faux-positifs"] conduit à devoir effectuer le plus souvent des traitements intrusifs de masse, formellement inopérants en pratique et pouvant conduire à des erreurs de classification avec des conséquences potentielles sérieuses », *ibid.*, p. 1.

86. Délib. n° 2015-078, 5 mars 2015 portant sur le projet de loi relatif au renseignement.

87. Peuvent avoir accès à ces données l'administration fiscale (art. L. 83 et L. 96 G du Livre des procédures fiscales), l'Autorité des marchés financiers (art. L. 621-10 du code monétaire et financier), l'Agence nationale pour la sécurité des systèmes d'information (art. L. 2321-3 du code de la défense) et la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet, HADOPI (art. L. 331-21 du code de la propriété intellectuelle).

a pour effet de rendre lisibles des communications cryptées et donc d'attenter au secret des correspondances devra être utilisée avec retenue par les services spécialisés et par la CNCTR au risque, là aussi, de faire dériver notre société vers une nouvelle forme de totalitarisme. La cryptologie est le moyen d'assurer la confidentialité des communications électroniques et peut être utilisée par toute personne ayant un besoin professionnel ou une envie privée de ne pas divulguer à des tiers le contenu de ses correspondances (un courriel rédigé « en clair » étant aussi confidentiel qu'une carte postale), le déchiffrement ne doit concerner que des cas très limités et précisément identifiés.

L'article L. 853-2 autorise, « lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé », l'utilisation de dispositifs techniques permettant l'accès « à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre » pour une durée maximale de trente jours, ou permettant l'accès « à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels » pour une durée maximale de deux mois. Là aussi, la technique en cause est particulièrement intrusive et conduit à percer les filtres, mots de passe et codes confidentiels de l'individu surveillé – c'est d'ailleurs le but de la manœuvre – et devra être utilisée avec la plus grande parcimonie.

D'autre part, même si la collecte de données personnelles est moins directement concernée, il convient de signaler que l'article L. 851-4 autorise « l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet » et que l'article L. 851-6 permet le recueil direct de « données techniques de connexion permettant l'identification d'un équipement terminal ou d'un numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ».

Par ailleurs, l'article L. 853-1 permet « lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé ». À titre de comparaison, l'article 14 de la loi suisse du 25 septembre 2015 interdit au service de renseignement de la Confédération « d'observer et d'effectuer des enregistrements visuels et sonores d'événements et d'installations relevant de la sphère privée protégée ». Toutefois, une seconde phrase illustre

la relativité de cette interdiction en pratique puisqu'elle affirme que les « enregistrements visuels et sonores relevant de la sphère privée qu'il est techniquement impossible d'éviter doivent être immédiatement détruits ». L'article 26 c de la même loi soumet à autorisation « l'utilisation des appareils de surveillance pour écouter ou enregistrer des propos non publics ou pour observer ou enregistrer des événements se produisant dans des lieux non publics ou dans des lieux qui ne sont pas librement accessibles ». Ici aussi, il eût été souhaitable que le législateur se fût adonné au droit comparé.

2.2.2. Des garanties en clair-obscur

La loi relative au renseignement introduit aussi dans le CSI d'appréciables innovations, dont la garantie de la vie privée et – grâce à un amendement parlementaire – de la protection des données personnelles et la référence au principe de proportionnalité à l'article L. 801-1. Cette protection passe notamment par la destruction des extraits ou exploitations des traitements n'étant plus indispensables ainsi que le prévoit l'article L. 822-3 CSI, et par l'interdiction, par l'article L. 821-7 qu'un parlementaire, un magistrat, un avocat ou un journaliste puisse être surveillé à raison de l'exercice de son mandat ou de sa profession⁸⁸, mais surtout par l'institution de la CNCTR (2.2.2.1), par le renforcement du contrôle parlementaire (2.2.2.2) et par l'instauration d'un recours juridictionnel (2.2.2.3).

2.2.2.1. Le contrôle *a priori* de la CNCTR

Les mesures de collecte et de conservation des données personnelles sont surveillées par la CNCTR, autorité administrative indépendante, substituée à la CNCIS, et composée, aux termes de l'article L. 831-1 CSI, de deux députés, de deux sénateurs, de deux conseillers d'État, de deux magistrats de la Cour de cassation et d'une « personnalité qualifiée pour sa connaissance en matière de communications électroniques, nommée sur proposition du président de l'Autorité de régulation des communications électroniques et des postes ». Il est pour le moins

88. Cons. const., déc. n° 2015-713 DC, cons. 31-35 ; en revanche, le conseil note : « le principe d'indépendance n'implique pas que les professeurs d'université et les maîtres de conférences doivent bénéficier d'une protection particulière en cas de mise en œuvre à leur égard de techniques de recueil de renseignement dans le cadre de la police administrative », § 36.

surprenant que, sur un sujet si technique, une seule personnalité qualifiée soit appelée à siéger au sein de cette autorité.

La CNCTR doit rendre au Premier ministre un avis sur l'autorisation des captations, sauf en cas d'urgence absolue où, conformément à l'article L. 821-5 CSI, la commission est informée sans délai mais le chef du gouvernement a vingt-quatre heures pour lui fournir tous les éléments de motivation.

Le Premier ministre n'a toutefois pas compétence liée mais doit motiver l'autorisation délivrée en dépit d'un avis défavorable de la CNCTR, ainsi que le prévoit l'article L. 821-4 al. 2 CSI – l'expérience de la CNCIS prouvant que les avis peuvent être allègrement outrepassés, il faut avouer que ce n'est guère rassurant pour les libertés.

En cas d'urgence opérationnelle, c'est-à-dire « liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement », il était prévu que la CNCTR et le Premier ministre seraient simplement informés sans délai, mais le Conseil constitutionnel a considéré qu'il s'agissait d'une « atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances⁸⁹ ». Cependant, il sera toujours loisible « au Premier ministre de déléguer aux différents responsables des services de renseignement une compétence pour agir en son nom dans l'hypothèse d'une situation d'urgence opérationnelle⁹⁰ ».

Sur le plan pratique, le contrôle risque d'être ardu puisque c'est « un véritable océan numérique que la CNCTR doit sonder avec une époussette⁹¹ » mais cette abondance d'informations pourrait être finalement une garantie pour le citoyen ordinaire. En effet, « le système de cybersurveillance pourrait trouver en lui-même sa propre limite puisque la captation des données en masse, qui consiste à tout intercepter au motif que cela pourrait toujours servir un jour, n'est pas véritablement efficace puisque seule l'analyse fine des données interceptées est utile⁹² ».

89. *Ibid.*, cons. 29.

90. Roseline Letteron, « Loi renseignement : "Filtrer le moustique et laisser passer le chameau" », 24 juillet 2015, disponible en ligne à l'adresse suivante : <http://libertescherries.blogspot.fr> (consulté le 27 novembre 2015).

91. Christophe Labbé et Olivia Recasens, « Dans l'enfer du "secret-défense" », dans Fabrice Arfi et Paul Moreira (dir.), *Informé n'est pas un délit. Ensemble contre les nouvelles censures*, Paris, Calmann-Lévy, 2015, p. 178.

92. Cécile Doutriaux, « Données personnelles et cybersurveillance », *Revue Défense nationale*, n° 775, décembre 2014, p. 32.

2.2.2.2. Le contrôle parlementaire de la délégation parlementaire au renseignement

La loi relative au renseignement modifie l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires pour indiquer que la délégation parlementaire au renseignement⁹³ est destinataire d'un rapport annuel de synthèse des crédits consacrés au renseignement, d'un rapport annuel d'activité des services spécialisés de renseignement, d'éléments d'appréciation sur l'activité générale et l'organisation de ceux-ci, d'« une présentation, par technique et par finalité, des éléments statistiques figurant dans le rapport d'activité » de la CNCTR et des observations que celle-ci adresse au Premier ministre. En outre, la délégation parlementaire au renseignement peut saisir la CNCTR pour avis.

Par rapport à des exemples étrangers, le rôle de la délégation parlementaire apparaît modeste. En Suisse, la Délégation des commissions de gestion des chambres fédérales (DELCDG⁹⁴) a un accès illimité aux informations gouvernementales secrètes, un pouvoir d'inspection et de proposition et est d'ailleurs à l'origine de la loi sur le renseignement de 2015⁹⁵. En revanche, le Canada a préféré confier le contrôle de ses services de renseignement à un organe extra-parlementaire puisque le Comité de surveillance des activités de renseignement et de sécurité (CSARS) est composé, selon l'article 34 § 1 de la loi sur le service canadien du renseignement de sécurité, « du président et de deux à quatre autres membres, tous nommés par le gouverneur en conseil parmi les membres du Conseil privé de la Reine pour le Canada⁹⁶ qui ne font partie ni du Sénat, ni de la Chambre des communes ». Le CSARS a des pouvoirs d'inspection et d'enquête et rend compte au parlement⁹⁷,

93. Commune à l'Assemblée nationale et au Sénat, la délégation comprend quatre députés et quatre sénateurs, dont les présidents des commissions permanentes chargées des affaires de sécurité intérieure et de défense.

94. Composée de trois membres du Conseil national (chambre basse) et de trois membres du Conseil des États (chambre haute) dont, en principe, un député d'un parti politique qui n'est pas représenté au Conseil fédéral (gouvernement).

95. Voir *Rapport annuel 2014 des Commissions de Gestion et de la Délégation des Commissions de gestion des Chambres fédérales*, 30 janvier 2015, p. 4819-4839, surtout « Nouveaux moyens de recherche d'informations », p. 4834-4835.

96. Ce qui signifie qu'il s'agit nécessairement d'éminents juristes.

97. Voir CSARS, *Lever le voile du secret. Trente ans de reddition de comptes en matière de renseignement de sécurité. Rapport annuel 2013-2014*, Ottawa, Travaux publics et services gouvernementaux, 2014, disponible en ligne à l'adresse suivante : <http://www.sirc-csars.gc.ca> (consulté le 27 novembre 2015).

lequel a – selon le modèle de Westminster – d’importants pouvoirs. La Belgique s’est inspirée de l’exemple canadien : le Comité permanent de contrôle des services de renseignement et de sécurité (*alias* « Comité R ») est composé de non-parlementaires nommés par le Sénat et contrôlé par une commission sénatoriale *ad hoc* et comprend un service d’enquête soumis à l’autorité judiciaire⁹⁸. Ces pays ont une tradition parlementaire plus marquée que la France de la V^e République ; toutefois, rien n’empêche la constitution d’une commission parlementaire *ad hoc*...

2.2.2.3. Le contrôle juridictionnel du Conseil d’État

L’article L 841-1 CSI institue un recours devant le Conseil d’État⁹⁹ saisi par toute personne ayant un intérêt direct et personnel, par la CNCTR ou par toute juridiction à titre préjudiciel. Le Conseil d’État ne pourra pas se voir opposer le « secret défense », même s’il ne divulguera pas les informations ainsi classifiées¹⁰⁰. Cependant, le professeur Roseline Letteron estime que la personne qui se pense surveillée « ne dispose que d’un “droit d’accès indirect”, notion sans doute inventée par un humoriste, puisque la procédure ne donne aucun accès, ni direct, ni indirect, aux données recueillies sur son compte¹⁰¹ ». En effet, le requérant saura simplement si une illégalité a été commise ou non, mais ne saura pas de quelle illégalité il s’agissait. Incontestablement, le droit fondamental à la protection des données personnelles est malmené compte tenu du délicat équilibre à trouver entre l’exigence d’un contrôle juridictionnel et la nécessité d’une part de secret pour les activités de renseignement. La solution retenue est certes en demi-teinte, mais elle

98. David Stans, « Le contrôle des services de renseignement belges : émergence d’une légitimité », *Revue de la Faculté de droit de l’université de Liège*, vol. LIV, n° 3, 2010, p. 373-387 ; Guy Rapaille et Johan Vanderborght, « L’herbe est toujours plus verte ailleurs. Sur le contrôle belge des services de renseignement et de sécurité », *Cahiers de la sécurité*, n° 13, juillet-septembre 2010, p. 122-133 ; cet article est postérieur à l’adoption de la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, avant laquelle ces derniers ne pouvaient pas recourir aux interceptions de communications.

99. La loi relative au renseignement introduit dans le code de justice administrative notamment les articles L. 311-4-1 (compétence) et L. 773-1 à L. 733-8 (jugement).

100. Voir les contributions de Bertrand Warusfel, « Secret et Défense nationale » et de Christian Vigouroux, « Secret et fonctionnement des institutions administratives », dans Catherine Blaizot-Hazard (dir.), *Les NTIC face aux droits fondamentaux à travers le prisme du secret*, Paris, LGDJ, à paraître.

101. « Le projet de loi renseignement ou l’effet d’aubaine du terrorisme », 16 mai 2015, disponible en ligne à l’adresse suivante : <http://libertescherries.blogspot.fr> (consulté le 27 novembre 2015).

a le mérite d'exister alors qu'il n'y avait auparavant aucun contrôle. Le Conseil d'État peut, selon l'article L. 773-7 du code de justice administrative (CJA), ordonner la destruction des renseignements irrégulièrement collectés et condamner l'État à indemniser le préjudice subi. Cependant, il sera difficile pour le requérant ayant été irrégulièrement surveillé d'estimer si cette indemnisation correspond bien au préjudice subi puisqu'il ne connaîtra ni la nature, ni l'ampleur de la mesure illégale. Reste à savoir, si la Cour européenne des droits de l'homme considérera ce type d'indemnisation comme une satisfaction équitable. Ce qui est plus fortement probable est que la juridiction strasbourgeoise déclare que la procédure adaptée au secret de la défense nationale contrevient aux règles du procès équitable en n'assurant pas l'égalité des armes entre le requérant et l'administration puisque seule cette dernière aura tous les éléments pertinents en sa possession.

En revanche, il est peu vraisemblable que la Cour européenne des droits de l'homme donne raison à ceux qui déplorent « l'absence d'encadrement par l'autorité judiciaire, pourtant indispensable à la sauvegarde des libertés individuelles¹⁰² », car, ainsi que le rappelait l'ancien magistrat antiterroriste Gérard Thiel¹⁰³, le juge judiciaire est incompétent en raison de la séparation des pouvoirs. Effectivement, les opérations, par nature préventives, des services de renseignement sont des opérations de police administrative et relèvent par conséquent du juge administratif, comme le Conseil constitutionnel avait eu l'occasion de rappeler, à propos du traitement de données de trafic par ces services, il s'agit de pures opérations de police administrative ne pouvant pas relever du juge judiciaire¹⁰⁴. Or, bien qu'elle puisse être critique sur tel ou tel aspect de procédure administrative, la cour de Strasbourg ni ne remet en cause l'existence du juge administratif, ni ne considère que le juge judiciaire aurait l'exclusivité de la défense des droits et des libertés.

Conformément à une tendance lourde, depuis la fin du siècle dernier, à privilégier l'aspect sécuritaire par rapport aux libertés individuelles, la loi

102. François-Pierre Lani, « Loi sur le renseignement : une atteinte aux libertés individuelles inquiétante », Les Échos, 23 avril 2015 ; voir aussi le mémoire d'*amicus curiae* remis au Conseil constitutionnel par Amnesty International France, CECIL, CREIS-Terminal, la Ligue des droits de l'homme, le SAF et le SM, Observations sur la loi relative au renseignement, sans date, p. 17.

103. Lors des Entretiens de Pétrarque à Montpellier, retransmis sur France-Culture le 13 juillet 2015.

104. Cons. const., déc. no 2005-532 DC, 19 janv. 2005, loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, cons. 5.

relative au renseignement offre certes des garanties mais qui ne devraient guère entraver l'action des services spécialisés. Pour ne pas être nouveau, le phénomène n'en est pas moins inquiétant. Non pas qu'il faille adopter face au terrorisme une attitude irénique – voire angélique – mais, à trop faire pencher le plateau de la balance du côté de la sécurité, fort est le risque de faire basculer notre société dans les bras du « monstre doux » prophétisé par Tocqueville¹⁰⁵.

De surcroît, la pertinence des techniques intrusives de cybersurveillance n'est pas prouvée. Le fait que la NSA, en dépit d'une surveillance de masse inégalée, n'ait pas vu venir les attentats de Boston souligne *a contrario* le caractère aléatoire d'une démarche fondée sur la seule technologie. Il n'est pas certain que, si les moyens désormais autorisés en France avaient été à l'époque mis en œuvre, les attentats commis par Mohamed Merah ou les frères Kouachi auraient pu être prévenus. Si la technologie peut s'avérer indispensable, c'est surtout des moyens humains diversifiés – avec notamment des compétences linguistiques ou, plus généralement, en sciences humaines – qui sont nécessaires. Le choc des attentats de janvier 2015 a généré un flot de candidatures, dont des « profils rares et chers », pour les services de renseignement¹⁰⁶, ce qui devrait leur permettre de mieux s'adapter aux menaces présentes et à venir. De même, l'article L. 4211-1-V du code de la défense – issu de la loi relative au renseignement – qui permet aux services spécialisés de renseignement d'avoir recours aux membres de la réserve militaire, vivier de compétences variées, peut offrir aux services les spécialistes qui leur manquent dans certains domaines. Affûter les services de renseignement grâce aux ressources humaines, plutôt que

105. « Je veux imaginer sous quels traits nouveaux le despotisme pourrait se produire dans le monde : je vois une foule innombrable d'hommes semblables et égaux qui tournent sans repos sur eux-mêmes pour se procurer de petits et vulgaires plaisirs [...]. Au-dessus de ceux-là s'élève un pouvoir immense et tutélaire qui se charge seul d'assurer leur jouissance. Il est absolu, détaillé, régulier, prévoyant et doux » (Alexis de Tocqueville, *De la démocratie en Amérique*, 1840, tome II, 4^e partie, chapitre 6, p. 146, disponible en ligne à l'adresse suivante : <http://classiques.uqac.ca> [consulté le 27 novembre 2015]). Plus largement, voir Jean-Jacques Lavenue, « Gouvernance des données et naissance du “Monstre doux” », dans Irène Bouhadana et William Gilles (dir.), op. cit., p. 33-56, pour qui le « monstre doux » résulte d'une « coalition d'intérêts des principaux acteurs du numérique vivant de l'exploitation des données qui y circulent, et de leurs alliés objectifs, institutionnels ou politiques qui, au nom d'approches idéologiques, y trouvent les moyens d'ancrer leur domination sur les systèmes économiques et sociaux » (p. 35, notes omises), approche qui dépasse le cadre de la présente étude.

106. D. M., « Les services de renseignement croulent sous les candidatures », *Le Figaro*, 17-18 octobre 2015, p. 3.

compter sur les seuls algorithmes éviterait une surveillance de masse inutile et dangereuse, et serait plus efficace puisque, comme l'indique un spécialiste des services secrets : « [s]urveiller de manière moins extensive, mais mieux, c'est-à-dire plus ciblée : l'efficacité, la vraie, est à ce prix¹⁰⁷ ».

Professeur de relations internationales à l'École de l'air

107. Rémi Kauffer, *Histoire mondiale des services secrets*, Paris, Perrin, 2015, p. 12.