N° 3069

—

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 10 juin 2020

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA MISSION D'INFORMATION COMMUNE [(1)],

*sur l'**évaluation** de la **loi du 24 juillet 2015 relative au renseignement***

ET PRÉSENTÉ PAR

M. GUILLAUME LARRIVÉ,
Président,

MM. LOÏC KERVRAN ET JEAN-MICHEL MIS,
Rapporteurs,

Députés

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information commune sur l'évaluation de la loi du 24 juillet 2015 relative au renseignement est composée de M. Guillaume Larrivé, *président, et de* MM. Loïc Kervran et Jean-Michel Mis, *rapporteurs*

SOMMAIRE

___

Pages

« Il faut l'avouer, je crois peu aux lois. Trop dures, on les enfreint, et avec raison. Trop compliquées, l'ingéniosité humaine trouve facilement à se glisser entre les mailles de cette masse traînante et fragile. » « J'ai effectué moi-même quelques-unes de ces réformes partielles qui sont les seules durables. » « Je me proposais pour but une prudente absence de lois superflues, un petit groupe fermement promulgué de décisions sages. »

Marguerite Yourcenar, *Mémoires d'Hadrien*.

MESDAMES, MESSIEURS,

Cinq années se seront bientôt écoulées depuis l'adoption de la loi du 24 juillet 2015 relative au renseignement [(1)]. Conformément aux prescriptions de son article 27, les commissions des Lois et de la Défense ont donc institué, le 30 octobre dernier, une mission d'évaluation de l'application des dispositions de cette loi consensuelle et fondatrice.

Consensuelle, car elle a été élaborée en réunissant, au Parlement, une très large majorité de suffrages [(2)], fédérant la plupart des députés siégeant parmi les groupes émanant des partis de gouvernement. Dès la présentation du projet de loi à l'Assemblée nationale par le Premier ministre Manuel Valls, le rapporteur Jean-Jacques Urvoas soulignait combien *« la nécessité de donner un cadre à l'activité des services »* faisait désormais *« consensus », « au nom du renforcement de l'État de droit », « au nom de la protection des libertés individuelles »* et *« au nom de l'efficacité des services. »* [(3)] De même, le président de votre mission d'information justifiait alors le soutien du groupe de l'UMP en exposant la nécessité d'assurer *« la continuité de l'État »* et de *« mieux protéger les Français dans le respect de ce que nous sommes, à savoir un État de droit qui garantit l'exercice des libertés. » « L'État de droit doit être fort. S'il est faible, il n'est plus l'État et il n'y a plus de droits. »* [(4)]

Fondatrice, car elle poursuivait deux ambitions majeures : **faciliter l'action opérationnelle et consolider le cadre juridique des services de**

---

(1) Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

(2) Lors du scrutin public du 5 mai 2015, en première lecture, sur 566 votants, 438 députés ont voté pour.

(3) Intervention du député Jean-Jacques Urvoas lors de la séance du 13 avril 2015, http://www.assemblee-nationale.fr/14/cri/2014-2015/20150212.asp#P511111

(4) Intervention du député Guillaume Larrivé lors de la séance du 16 avril 2015, http://www.assemblee-nationale.fr/14/cri/2014-2015/20150218.asp#P517687

renseignement, qui sont engagés dans la défense de la démocratie française et de nos concitoyens.

Faciliter l'action opérationnelle des services apparaissait comme une nécessité impérieuse à l'heure où les menaces qui pesaient sur la France, et en particulier la menace terroriste islamiste, se manifestaient avec une violence inouïe. La loi du 24 juillet 2015 n'est ni une loi de circonstance ni une loi spécifiquement antiterroriste, mais elle a été débattue dans les mois qui ont suivi les attentats de *Charlie Hebdo* et a été particulièrement marquée par la nécessité de donner aux services de renseignement les moyens juridiques de lutter le plus efficacement possible contre le terrorisme islamiste. Il convenait donc de leur octroyer des ressources adaptées au but poursuivi – des moyens humains, matériels, technologiques, mais aussi des instruments juridiques.

Consolider le cadre juridique des services de renseignement, **pour renforcer l'État de droit**, a été l'autre objectif majeur de cette loi.

Certains observateurs, dans les années précédentes, avaient pu souligner, à bon droit, « *l'opacité qui entoure les services dits " secrets " et qui tend à inquiéter davantage qu'elle ne rassure, même si les raisons en sont comprises* » (1). Il apparaissait désormais nécessaire que la loi – qui, selon l'article 34 de la Constitution fixe les garanties fondamentales accordées aux citoyens – vienne définir le cadre juridique régissant l'ensemble de l'action et les missions des services de renseignement. **Un contrôle approfondi et précis, dans ses différentes composantes (interne et externe ; administrative, parlementaire et juridictionnelle) est en effet la nécessaire contrepartie de la discrétion et, souvent, du secret qui caractérisent l'activité des services et des moyens qu'ils sont autorisés à utiliser, en tant qu'ils dérogent, par nature, au respect des libertés individuelles.**

Même si les services du renseignement, avant la loi de 2015, respectaient des procédures, « *l'association du mot droit à celui de renseignement est plus inédite* [que pour la plupart des politiques publiques] *ou du moins plus récente* », comme le soulignait récemment M. Laurent Nuñez, secrétaire d'État auprès du ministre de l'intérieur (2). En effet, « *sous la V^e^ République, le renseignement est resté jusque tardivement à l'écart, comme interdit de cité, de la vie démocratique et de la décision publique en France.* (…) *Longtemps, le rapport de l'espionnage, puis du renseignement au droit s'en tint essentiellement à la raison d'État.* » (3)

Plusieurs lois sont intervenues à compter des années 1990 pour régir certaines techniques de renseignement, mais sans élaborer un cadre global. C'est

---

(1) Éric Denécé, « L'absence du suivi des activités démocratiques des services de renseignement par le Parlement : une lacune de la démocratie française », note du Centre Français de Recherche sur le Renseignement (CF2R), 31 janvier 2006.

(2) In Introduction, Le droit du renseignement, *L'Académie du renseignement, Laurent Nunez, p. 11.*

(3) In Retour historique sur les institutions et les pratiques du renseignement français de 1991 à 2015, Le droit du renseignement*, L'Académie du renseignement, Olivier Forcade, pp. 19 à 22.*

le cas de la loi n° 91-646 du 10 juillet 1991 (1), sur l'initiative du Premier ministre Michel Rocard, qui est venue encadrer l'utilisation des interceptions de sécurité, puis de la loi du 23 janvier 2006 (2) présentée par le ministre d'État, ministre de l'intérieur Nicolas Sarkozy, s'agissant du recueil des données techniques de connexion.

La loi du 24 juillet 2015 est donc le fruit d'une lente maturation et d'une évolution de l'encadrement juridique des pratiques de renseignement en France, dans un environnement européen attentif.

L'enjeu de cette loi était de taille car il s'agissait de **concilier deux impératifs : la protection de la vie privée des citoyens** d'un côté, **et la protection des intérêts fondamentaux de la nation** de l'autre.

La loi du 24 juillet 2015 a été conçue comme une **loi-cadre, c'est-à-dire une loi conçue pour durer et échapper à toute obsolescence programmée**.

Elle a institué en préambule du livre VIII du code de la sécurité intérieure consacré au renseignement, l'article L. 801–1, article de principe qui rappelle notamment que le respect de la vie privée est garanti par la loi (3) et qu'il n'est possible d'y porter atteinte que dans les conditions prévues par la loi. Cette dernière s'articule autour de cinq principes fondamentaux que sont la proportionnalité, la subsidiarité, l'individualisation, la centralisation et la territorialité.

Depuis 2015, la **politique publique du renseignement a pris, notamment du fait de la menace terroriste, une place de plus en plus prégnante**. Cela s'est traduit par une nette augmentation des crédits, qui ont crû d'environ 32 % au cours des cinq dernières années (4) et par une hausse conséquente des effectifs des services.

---

(1) Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

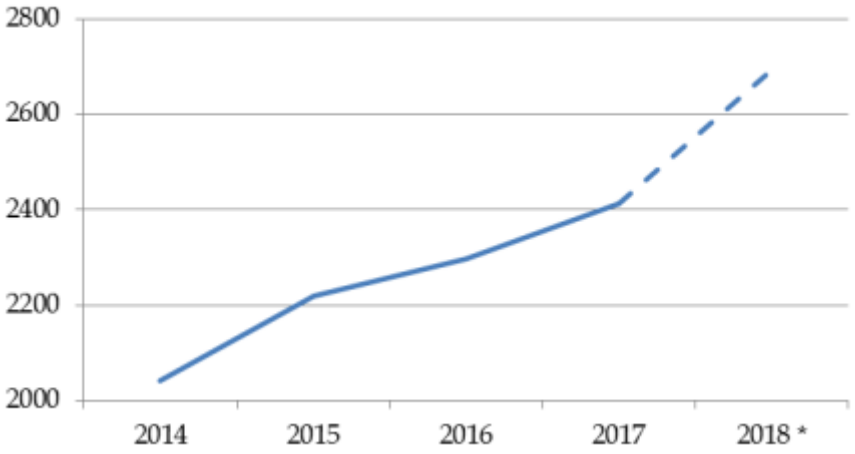
(2) Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

(3) Le Conseil constitutionnel a reconnu à ce principe une valeur constitutionnelle dans sa décision n° 99–416 DC du 23 juillet 1999, estimant que la liberté proclamée par l'article 2 de la déclaration des droits de l'homme et du citoyen impliquait le respect de la vie privée (cons. 45).

(4) Délégation parlementaire au renseignement, rapport n° 1869 de Mme Yaël Braun–Pivet relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018, avril 2019, p. 30.

CRÉDITS DE PAIEMENT CONSACRÉS À LA POLITIQUE PUBLIQUE DU RENSEIGNEMENT (1)

En millions d'euros



Source : Délégation parlementaire au renseignement, rapport n° 1869 de Mme Yaël Braun–Pivet relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018, avril 2019, p. 30

ÉVOLUTION DES EFFECTIFS DES SERVICES SPÉCIALISÉS DE RENSEIGNEMENT

	2014	**2015**	**2016**	**2017**	**2018**
DGSE	5 112	5 216	5 335	5 372	5 627
DGSI	3 250	3 548	3 812	3 999	4 043
DRM	1 557	1 640	1 722	1 808	1 861
DRSD	1 076	1 142	1 189	1 242	1 330
DNRED	726	737	760	774	763
TRACFIN	104	119	133	151	166
Total Services spécialisés	11 825	12 402	12 951	13 346	13 790
GIC	*138*	*126,5*	*134*	*162,5*	*197*

Source : Délégation parlementaire au renseignement, rapport n° 1869 de Mme Yaël Braun–Pivet relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018, avril 2019, p. 94.

La loi du 24 juillet 2015 est en application depuis presque cinq ans, l'essentiel de ses dispositions ayant été mises en place en octobre 2015. Les membres de la mission d'information, au terme des travaux qu'ils ont menés, en partie dans le contexte particulier de confinement imposé par la nécessité d'enrayer la propagation de l'épidémie de covid–19, font le constat que **cette loi donne aujourd'hui largement satisfaction.**

Tant les services de renseignement que l'autorité administrative indépendante chargée du contrôle, la commission nationale de contrôle des techniques de renseignement (CNCTR), ont fait part aux membres de la mission

(1) En fonds normaux.

de leur **attachement au cadre général posé par la loi du 24 juillet 2015, amendée depuis à plusieurs reprises.**

M. Francis Delon, président de la CNCTR, a ainsi indiqué ne pas avoir détecté de « *problème majeur* », en ajoutant qu'« *il y a[vait] des imperfections* » mais que « *le cadre légal a[vait] constitué un très net progrès par rapport à auparavant : avant, ce cadre était très limité tandis qu'aujourd'hui, il est assez global* » (1).

Le taux d'avis défavorables de la CNCTR aux demandes de techniques de renseignement s'établit en 2019 à 1,4 %, en recul constant depuis l'entrée en vigueur du nouveau cadre légal en 2015, et ce, alors même que le nombre de techniques de renseignement ne cesse d'augmenter (2). Il ne faut donc pas voir dans ce faible taux d'avis défavorables la conséquence d'une autocensure des services de renseignement, mais le **résultat d'un dialogue de qualité avec l'autorité en charge du contrôle.**

C'est d'autant plus remarquable que les **services de renseignement ont connu des évolutions majeures au cours des dernières années**. La révolution numérique a « *bouleversé les modalités d'action des services confrontés au défi du ciblage des données, aux cyberattaques et aux promesses de l'intelligence artificielle* » (3), la France a connu des attaques terroristes d'une ampleur dramatique et doit faire face au retour de djihadistes sur le territoire national et à la sortie de prison de détenus radicalisés.

Le législateur est déjà intervenu à plusieurs reprises afin de modifier des dispositions du code de la sécurité intérieure issues de la loi du 24 juillet 2015. Ces modifications visaient soit à faire face à des censures du Conseil constitutionnel, soit à compléter des dispositions prévues en 2015 en particulier pour mieux prendre en compte l'évolution de la menace terroriste. Ce **régime juridique est dorénavant largement stabilisé**, et les services de renseignement, qui ont fourni des efforts importants pour s'y conformer, se sont désormais bien approprié la loi du 24 juillet 2015.

Les **membres de la mission d'information ont pris acte de ce point d'équilibre. En responsabilité, il leur a semblé qu'il ne fallait donc pas appeler à un *big bang* mais procéder aux ajustements nécessaires.**

En conséquence, la **mission a structuré sa réflexion autour de trois axes.**

Elle a, dans une première partie, procédé à un **bilan du cadre juridique** régissant les services de renseignement depuis la loi du 24 juillet 2015 telle qu'elle a été modifiée. Dans une deuxième partie, elle a examiné les deux **grands enjeux**

---

(1) Audition de Francis Delon, président de la CNCTR.

(2) CNCTR, rapport d'activité 2019, p. 53.

(3) Délégation parlementaire au renseignement, rapport n° 1869 de Mme Yaël Braun–Pivet relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018, avril 2019, p. 11.

auxquels les services de renseignement sont confrontés : **jurisprudentiels et technologiques**. Enfin, dans une troisième partie, elle a proposé des modifications qui pourraient être apportées pour **améliorer l'efficacité opérationnelle des services de renseignement**, dans le respect de la conciliation entre garanties des droits des citoyens et protection de la nation.

PREMIÈRE PARTIE : LA LOI DU 24 JUILLET 2015 : UNE NOUVELLE ARCHITECTURE DU RENSEIGNEMENT, ÉPROUVÉE ET APPROUVÉE

La loi du 24 juillet 2015 a consacré l'existence d'une politique publique du renseignement, qui concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la nation. Par ce choix, la loi a entériné le fait que l'État ne recourt pas au renseignement, pour reprendre les termes du professeur Bertrand Warusfel, *« comme à une pratique périphérique ou honteuse mais comme une politique officielle qu'il assume et qui fait partie de son cœur de métier* ». (1)

Elle n'a pas seulement affirmé l'existence de cette politique publique, elle en a également défini le périmètre d'intervention de manière précise, en créant un livre VIII consacré au renseignement au sein du code de la sécurité intérieure.

Ce cadre juridique a, d'une part, rassemblé des dispositions préexistantes éparses liées à certaines techniques de renseignement et a, d'autre part, innové en dotant les services de renseignement de nouveaux outils (**I**). Il a fait l'objet d'un certain nombre de modifications au cours des dernières années, liées notamment à plusieurs censures du Conseil constitutionnel et à diverses extensions du champ initialement prévu en 2015, mais il paraît néanmoins désormais largement stabilisé. Les services de renseignement, qui ont dû s'adapter pour se conformer aux nouvelles exigences posées par la loi, se sont bien approprié la loi du 24 juillet 2015 et y sont très attachés (**II**).

En donnant un cadre général aux activités de renseignement, la loi du 24 juillet 2015 a également renforcé le contrôle, en particulier externe, qui s'exerce sur certaines des activités de renseignement (**III**). Si une partie de ces contrôles préexistaient à la loi relative au renseignement, ils se sont nettement développés depuis.

Dans ses grands principes, la loi du 24 juillet 2015 a donc été approuvée et éprouvée. Elle comporte des garanties qui n'existaient pas auparavant dans un contexte de crise sécuritaire de grande ampleur.

---

(1) In Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement, Le droit du renseignement, *L'Académie du renseignement, Bertrand Warusfel, p. 67.*

I. UN CADRE JURIDIQUE NOVATEUR QUI A DÉJÀ CONNU HUIT MODIFICATIONS

La loi du 24 juillet 2015, reprenant sur de nombreux points la loi du 10 juillet 1991 sur les interceptions de correspondances précitée, a institué des finalités justifiant la mise en œuvre de techniques de recueil de renseignement (**A**), défini les techniques – certaines préexistant à la loi, d'autres, nouvelles – pouvant être mises en œuvre par les services du premier cercle et sous certaines conditions par ceux du second cercle (**B)**, en les enserrant dans une procédure permettant un contrôle à différents niveaux (**C**). Par ailleurs, les durées d'autorisation de mise en œuvre et de conservation des données recueillies grâce à la mise en œuvre de techniques de renseignement ont également fait l'objet d'un encadrement (**D**).

Ce cadre juridique novateur à bien des égards a été **retouché à huit reprises** (1). Les modifications apportées par le législateur l'ont été pour trois raisons principales :

– remédier aux censures du Conseil constitutionnel de certains aspects de la loi du 24 juillet 2015 (2) ou d'autres dispositions relatives au renseignement (3) ;

– étendre le champ de certaines dispositions, en particulier pour adapter les moyens des services de renseignement à l'évolution des menaces pesant sur le pays, en particulier la menace terroriste (4) ;

– procéder à des ajustements techniques (5).

A. LES FINALITÉS JUSTIFIANT LA MISE EN ŒUVRE DE TECHNIQUES DE RENSEIGNEMENT

Si la loi du 24 juillet 2015, à l'article L. 801–1 du code de la sécurité intérieure, énonce une règle générale de respect de la vie privée dans toutes ses composantes, elle pose parallèlement le principe d'une exception autorisant l'autorité publique à y porter atteinte dans les seuls cas de nécessité d'intérêt

---

(1) Une fois en 2015, deux fois en 2016, trois fois en 2017, une fois en 2018, une fois en 2019. Voir annexe n° 4.

(2) Ainsi, la loi n° 2015-1536 du 30 novembre 2015 relative aux mesures de surveillance des communications internationales tire-t-elle les conséquences de la censure par le Conseil constitutionnel d'une partie de l'article 6 de la loi du 24 juillet 2015 (décision n° 2015-713 DC du 23 juillet 2015).

(3) Ainsi, l'article 5 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a-t-il tiré les conséquences de la censure par le Conseil constitutionnel de l'exception hertzienne (décision n° 2016-590 QPC du 21 octobre 2016).

(4) Voir en particulier la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi de la loi n° 55–385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste s'agissant de la technique de recueil de données de connexion en temps réel et la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense s'agissant de la surveillance internationale.

(5) Voir par exemple la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes qui a harmonisé les dispositions applicables à la CNCTR avec celles du statut général.

public qu'elle énumère. Ce faisant, elle se rapproche d'autres textes internationaux – Constitution de l'Union internationale des télécommunications, Pacte international relatif aux droits civils et politiques, Convention de sauvegarde des droits de l'homme et des libertés fondamentales – qui reprennent également le modèle d'une règle générale garantissant les libertés individuelles et d'une exception autorisant les États parties à y déroger sous certaines conditions [(1)].

1. Les différentes finalités prévues à l'article L. 811-3 du code de la sécurité intérieure

Le recours aux techniques de renseignement s'exerce dans un cadre contraint. La première de ces contraintes est le **nombre limité de finalités pouvant justifier le recours aux techniques de renseignement**. Aux termes de l'article L. 811-3 du code de la sécurité intérieure, il doit s'agir de recueillir des renseignements relatifs à la **défense et à la promotion des intérêts fondamentaux de la Nation** suivants:

– l'indépendance et la défense nationales, l'intégrité du territoire **(1°)** ;

– 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 **(2°)**. Sont ainsi visés la contribution des services à vocation extérieure à la diplomatie française et le contre–espionnage ;

– les intérêts économiques, industriels et scientifiques majeurs français **(3°)**. Cela permet notamment de lutter contre l'espionnage industriel et de promouvoir les intérêts économiques français face à des pratiques déloyales de concurrents étrangers ;

– la prévention du terrorisme **(4°)**. Cette notion s'apprécie par référence aux articles 421–1 et suivants du code pénal, qui définissent les actes de terrorisme ;

– la prévention des atteintes à la forme républicaine des institutions (a), des actions tendant au maintien ou à la reconstitution de groupements dissous (b) et des violences collectives de nature à porter gravement atteinte à la paix publique (c) **(5°)**. Ces différentes notions font en particulier référence à diverses incriminations pénales et aux dispositions de l'article L. 212–1 du code de la sécurité intérieure ;

– la prévention de la criminalité et de la délinquance organisées **(6°)**. Cette notion renvoie aux incriminations pénales énumérées à l'article 706–73 du code de procédure pénale, précisées par la jurisprudence de la Cour de cassation [(2)] ;

---

(1) In Le droit du renseignement : un droit conforme aux traités internationaux, Le droit du renseignement, *L'Académie du renseignement, Fabien Lafouasse, p. 189.*

(2) Cour de cassation, crim., n° 14–88329, 8 juillet 2015.

– la prévention de la prolifération des armes de destruction massive **(7°)**, faisant référence aux incriminations pénales définies aux articles L. 2339–14 et suivants du code de la défense.

Cette liste a permis de compléter la rédaction qui prévalait antérieurement s'agissant des interceptions de sécurité [(1)]. Plusieurs changements ont ainsi été introduits par la loi du 24 juillet 2015 :

– le plus notable est la substitution des termes « *défense et promotion* » à celui de « *sauvegarde* » utilisé depuis 1991, afin d'acter la dimension offensive du renseignement aux côtés de sa dimension défensive. Comme l'a souligné le rapport sur le projet de loi de notre ancien collègue Jean–Jacques Urvoas, « *il paraissait indispensable d'assurer une démarche de collecte de renseignements au profit de certains secteurs vitaux pour notre pays, notamment dans le domaine économique, à l'instar de ce que pratiquent tous les services de renseignement de nos partenaires (souvent à notre détriment).* » [(2)]

– la suppression du concept de sécurité nationale introduit en 1991 par référence à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, au profit des notions d'indépendance nationale, d'intégrité nationale et de défense nationale figurant dans la Constitution à ses articles 5 et 21 ;

– le passage d'« *essentiels* » à « *majeurs* » pour définir les intérêts économiques, industriels et scientifiques défendus, confirmant l'intérêt du renseignement et de l'intelligence économiques [(3)] ;

– l'ajout ou l'explicitation de trois critères : les intérêts majeurs de la politique étrangère, la lutte contre les violences collectives antirépublicaines ainsi que la prévention de la prolifération des armes de destruction massive.

En outre, il faut noter que depuis la loi du 28 février 2017 [(4)], le service national du **renseignement pénitentiaire** peut, en application de l'article L. 855-1, recourir aux techniques de renseignement en application de **certaines finalités qui lui sont propres :**

---

(1) L'article 3 de cette loi disposait que pouvaient être autorisées, à titre exceptionnel, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant : « la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées. »

(2) Assemblée nationale, XIV^e^ législature, rapport n° 2697 de Jean–Jacques Urvoas sur le projet de loi relatif au renseignement, p. 101.

(3) La stratégie nationale du renseignement souligne que la promotion de nos intérêts économiques vise trois finalités : « identifier les actions susceptibles de contribuer à cette promotion ; appuyer les services de l'État chargés de la mise en œuvre de ces actions ; contribuer à la diffusion auprès des acteurs économiques des informations stratégiques utiles à leur développement international *». Présidence de la République, stratégie nationale du renseignement, p.5.*

(4) Article 35 de la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique.

– prévention des évasions ;

– organisation de la sécurité des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.

Cette liste marque en creux les domaines qui n'entrent pas dans le champ des finalités justifiant la mise en œuvre de techniques de renseignement, en particulier le renseignement politique (1). La CNCTR a d'ailleurs formulé un rappel en 2018 s'agissant des demandes de mise en œuvre de techniques de renseignement en matière de prévention des violences collectives de nature à porter gravement atteinte à la paix publique en indiquant « *qu'elle se montre particulièrement vigilante sur les demandes fondées sur cette finalité, considérant que la prévention de violences collectives ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, même extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré* » (2) .

Le Conseil constitutionnel, dans sa décision n° 2015–713 DC du 23 juillet 2015, a estimé que les finalités retenues par le législateur faisaient référence soit à des incriminations pénales existantes soit à des dispositions du code de la sécurité intérieure, du code des douanes ou du code de la défense et a donc estimé infondé le grief selon lequel elles seraient insuffisamment définies (3).

2. La place prépondérante de la finalité antiterroriste

Comme l'a montré la CNCTR dans son dernier rapport annuel, les différentes finalités de l'article L. 811–3 sont très diversement invoquées par les services de renseignement à l'appui de leurs demandes.

Avant 2015, la finalité de la prévention de la criminalité organisée, qui était déjà mentionnée dans la loi du 10 juillet 1991 précitée, constituait le premier motif de recours aux interceptions de sécurité (4). C'est au mois de **janvier 2015 que la prévention du terrorisme a, pour la première fois, été le fondement légal le plus fréquemment invoqué (5)**.

---

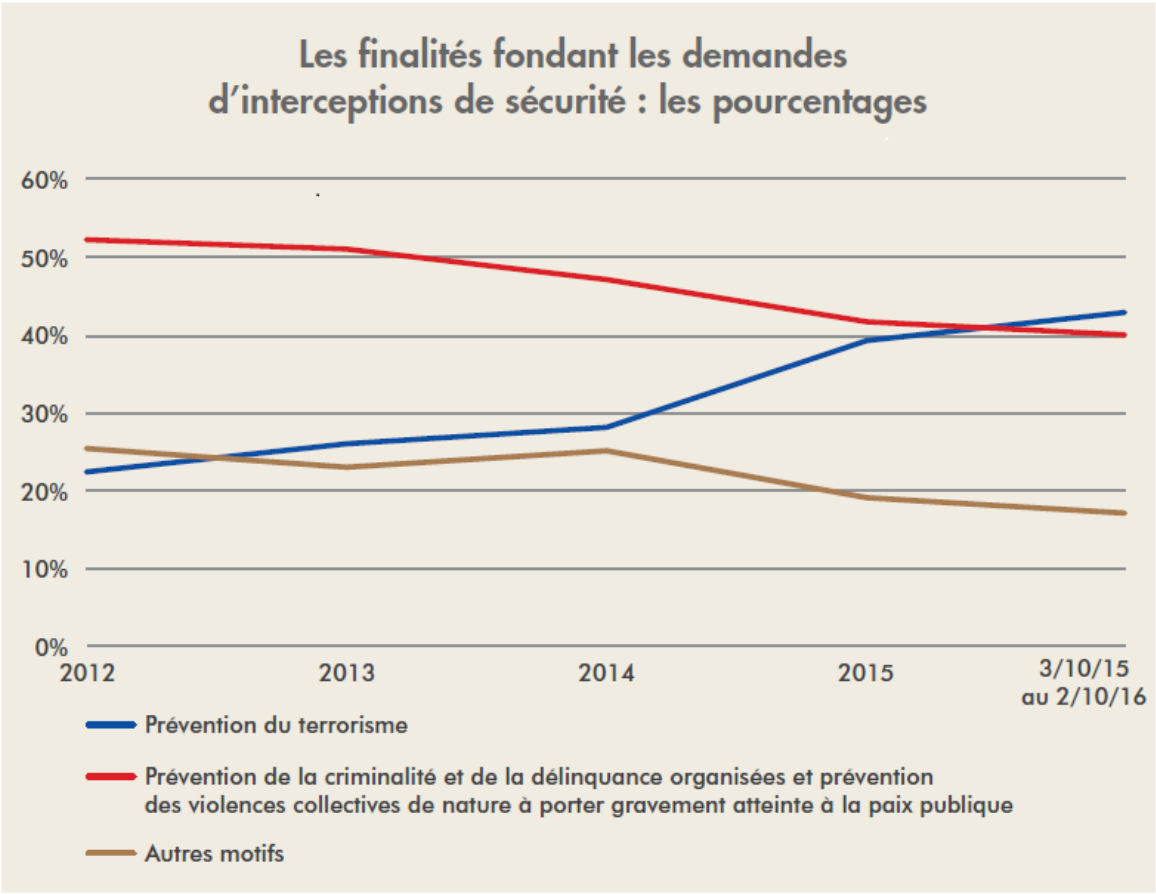
(1) In Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement, Le droit du renseignement*, L'Académie du renseignement, Bertrand Warusfel, p. 72 :* « on se rappelle les décisions anciennes prises à l'encontre des anciens services des renseignements généraux pour leur interdire de poursuivre des activités (ancestrales) de renseignement politique (lesquelles ont sans doute pesé lourd lors de la disparition de la DCRG au profit de la DCRI) » .

(2) CNCTR, rapport d'activité 2018, p. 67.

(3) Conseil constitutionnel, décision n° 2015–713 du 23 juillet 2015, Loi relative au renseignement, cons. 8 à 12.

(4) CNCTR, rapport d'activité 2016, p. 31.

(5) CNCTR, rapport d'activité 2016, p. 69.



CNCTR, rapport d'activité 2016, p. 69.

Elle est demeurée les années suivantes très nettement prédominante lorsqu'on considère les demandes portant sur l'ensemble des techniques de renseignement (1). Ainsi, cette finalité est invoquée dans **38 % des demandes en 2019.** Cela s'explique par la prégnance de la menace terroriste, principalement endogène depuis le recul territorial de l'organisation dite « État islamique » dans la zone irako-syrienne.

Elle est en **net recul relatif par rapport à 2018, où elle représentait 45 % des demandes (2) et 49 % en 2017.**

La place de la prévention du terrorisme dans la loi du 24 juillet 2015

La loi du 24 juillet 2015, qui n'est pas une loi antiterroriste, accorde cependant une **place particulière à la prévention du terrorisme**.

La **procédure d'urgence absolue**, qui permet d'autoriser une technique de renseignement sans l'avis préalable de la CNCTR, peut notamment être enclenchée sur le fondement de la prévention du terrorisme (3).

(1) CNCTR, rapport d'activité 2019, p. 55.

(2) CNCTR, rapport d'activité 2018, p. 67.

(3) De même que sur le fondement des finalités liées à l'indépendance nationale et la prévention des atteintes à la forme républicaine des institutions.

La prévention du terrorisme est la **seule finalité qui peut être invoquée pour l'ensemble des techniques de renseignement.** Certaines techniques peuvent être évoquées pour toutes les finalités, d'autres pour certaines finalités seulement [(1)], d'autres enfin, ne peuvent être utilisées que dans le cadre de la finalité de prévention du terrorisme : c'est le cas du recueil de données de connexion en temps réel, de l'algorithme et des vérifications ponctuelles sur des identifiants techniques rattachables au territoire français s'agissant de la surveillance des communications internationales (articles L. 851–2, L. 851–3 et IV du L. 854–2).

3. Des finalités diversement invoquées

Loin derrière la prévention du terrorisme, les finalités les plus invoquées, chacune dans moins de 20 % des demandes, sont la prévention de la criminalité et de la délinquance organisée et le groupe de finalités relevant des intérêts géostratégiques de la France [(2)].

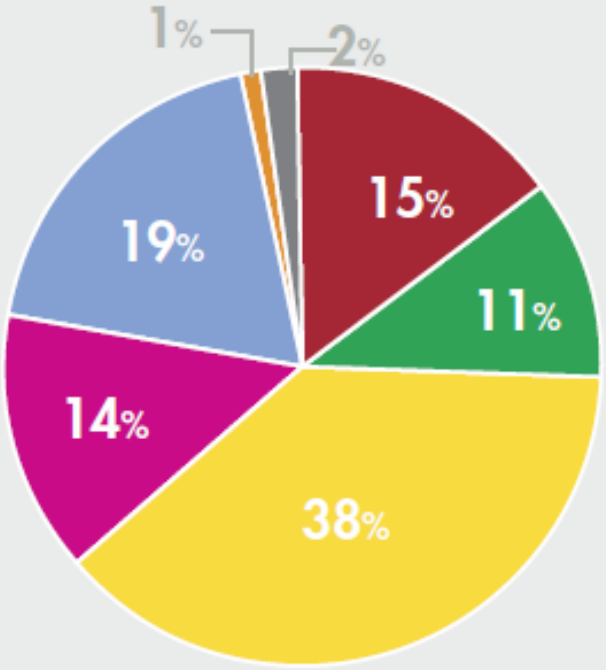
Viennent ensuite deux finalités : la défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France et la prévention d'activités particulièrement déstabilisatrices de l'ordre public, telles que les violences collectives de nature à porter gravement atteinte à la paix publique. Cette dernière finalité a été davantage invoquée au cours des deux dernières années, son poids relatif passant de 6 à 14 %.

S'agissant des finalités spécifiques au renseignement pénitentiaire, elles n'ont été invoquées en 2019 que dans 0,08% des demandes.

(1) C'est notamment le cas des IMSI–catcher quand ils permettent d'intercepter les correspondances (article L. 852–1), de l'autorisation d'exploitation de communications interceptées de numéros d'abonnement ou d'identifiants techniques rattachable au territoire national dont l'utilisateur communique depuis la France (V de l'article L. 854–2)

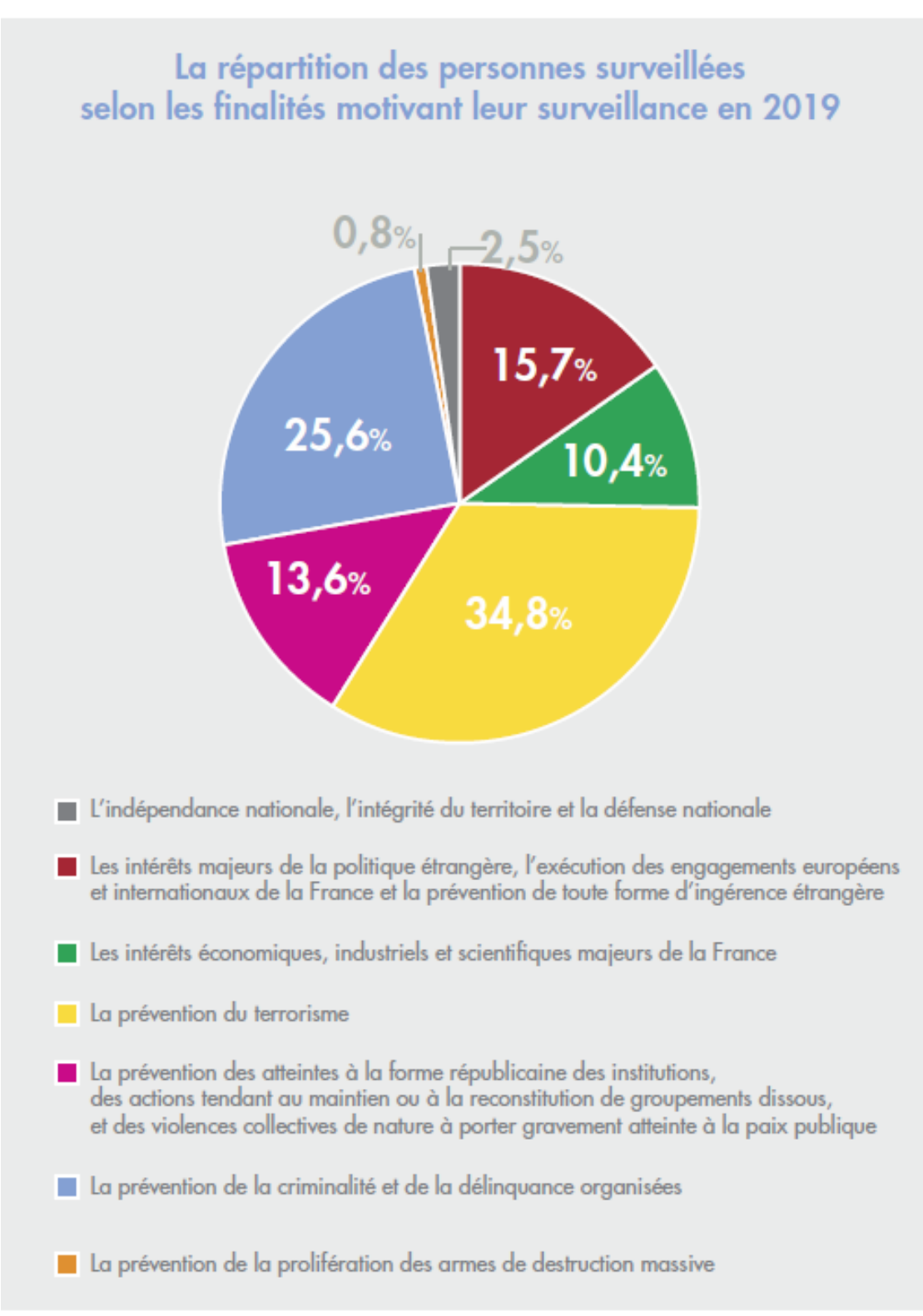
(2) Indépendance et défense nationales, intérêts majeurs de la politique étrangère de la France et prévention de l'ingérence étrangère, lutte contre la prolifération des armes de destruction massive.

Les finalités fondant toutes les techniques de renseignement en 2019



- L'indépendance nationale, l'intégrité du territoire et la défense nationale
- 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
- Les intérêts économiques, industriels et scientifiques majeurs de la France
- La prévention du terrorisme
- La prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, et des violences collectives de nature à porter gravement atteinte à la paix publique
- La prévention de la criminalité et de la délinquance organisées
- La prévention de la prolifération des armes de destruction massive

CNCTR, rapport d'activité 2019, p. 55



CNCTR, rapport d'activité 2019, p. 59

Comme l'a souligné la CNCTR, les différences de valeurs entre les deux diagrammes présentés ci–dessus reflètent le nombre de techniques employées pour surveiller une personne. Si 35 % des personnes surveillées en 2019 l'ont été au titre de la prévention du terrorisme, tandis que 38 % des demandes de techniques de renseignement étaient fondées sur cette finalité, c'est parce que les **personnes suspectées d'être impliquées dans un projet terroriste font, en moyenne,**

l'objet de davantage de techniques que les personnes surveillées sur le fondement d'autres finalités.

B. LES TECHNIQUES DE RECUEIL DE RENSEIGNEMENT

Les techniques de recueil de renseignement (1) font l'objet du titre V du livre VIII du code de la sécurité intérieure. Elles sont énoncées, en application du principe de subsidiarité, de la moins intrusive à plus intrusive.

1. Les accès administratifs aux données de connexion

Plusieurs techniques de renseignement prévues par la loi du 24 juillet 2015 sont relatives aux accès administratifs aux données de connexion. Ces données sont très larges. Il peut s'agir des 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'abonnements ou de connexion d'une personne désignée, à la localisation d'équipements terminaux, à la liste de numéros appelés ou appelants, à la durée et à la date des communications.

Ces informations ou documents **ne peuvent porter sur le contenu des correspondances échangées ou des informations consultées**, ainsi que le précise l'article R. 851–5 du code de la sécurité intérieure. Le Conseil constitutionnel l'a d'ailleurs rappelé dans sa décision n° 2015–713 DC du 23 juillet 2015, en estimant que « *le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu des correspondances ou les informations consultées* » (2).

a. Le régime juridique de la loi du 24 juillet 2015

Cette technique de réquisitions administrative des données de connexion, qu'il s'agisse de données relatives aux communications passées (les factures détaillées ou « fadettes ») ou à la localisation des équipements permettant ces communications, bénéficiait déjà d'un cadre légal antérieurement à la loi du 24 juillet 2015.

Si cette technique a été instaurée dès 1991 comme un préalable possible aux interceptions de sécurité (3), elle a été instituée en technique autonome en 2006 (1) et bénéficiait d'un régime unifié depuis 2013 (2).

---

(1) La loi du 24 juillet 2015, contrairement à d'autres lois-cadres comme la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, n'énonce pas de manière liminaire les définitions des différents concepts tels que renseignement ou donnée.

(2) Conseil constitutionnel, décision n° 2015-713 du 23 juillet 2015, Loi relative au renseignement, *cons. 55.*

(3) Outre le cadre juridique donné aux interceptions de communication, la loi du 10 juillet 1991 précitée autorisait également la collecte des données de connexion, car c'était une étape technique préalable aux interceptions de sécurité. Cependant, cette collecte n'était pas envisagée comme pouvant présenter un intérêt en tant que telle.

La loi du 24 juillet 2015 a distingué **plusieurs techniques permettant l'accès aux données de connexion :**

– le recueil et la transmission, sur sollicitation des opérateurs, **en temps différé**, des données de connexion, autorisés pour l'ensemble des finalités des activités de renseignement dans les conditions de droit commun de mise en œuvre des techniques de renseignement (**article L. 851–1 du code de la sécurité intérieure**). Cette technique de renseignement est souvent présentée comme un préalable à la mise en œuvre d'une autre technique de renseignement, dans la mesure où elle permet de recueillir des informations sur une personne avant la mise en œuvre d'une mise en œuvre d'une technique plus invasive ;

– l'accès **en temps réel** de toutes les données de connexion de personnes préalablement identifiées comme présentant une menace, pour les seuls besoins de la prévention du terrorisme (**article L. 851–2 du CSI**). Plus intrusive que l'accès aux données de connexion en temps différé, cette technique reste moins attentatoire à la vie privée qu'une interception de sécurité puisqu'elle ne permet pas d'écouter ou de lire des correspondances ;

– la technique dite de l'**algorithme** (**article L. 851–3 du CSI**), qui fait l'objet d'un développement *infra*.

Elle a également inclus :

– la **géolocalisation** en temps réel des équipements terminaux (**article L. 851–4 du CSI**).

– le **balisage**, permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet (**article L. 851–5 du CSI**). Cette disposition est une création de la loi du 24 juillet 2015, même si elle existait déjà dans le domaine judiciaire [(3)] ;

– le recours au **dispositif de proximité dit « *IMSI–catcher* »** (**article L. 851–6 du CSI**), qui fait l'objet d'un développement *infra*.

b. Les évolutions postérieures à la loi du 24 juillet 2015

La loi du 21 juillet 2016 de prorogation de l'état d'urgence [(4)] a élargi le champ des personnes visées par la technique d'accès en temps réel des données de connexion. La référence à « *la personne préalablement identifiée comme présentant une menace* » a été remplacée par la référence à « *la personne*

---

(1) Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

(2) 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.

(3) Sur le fondement de l'article 230–32 du code de procédure pénale.

(4) Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.

préalablement identifiée susceptible d'être en lien avec une menace » et **l'entourage** de la personne a été inclus dans le dispositif. Enfin, la durée de l'autorisation de recueil a été portée de deux à quatre mois.

Dans sa décision n° 2017-648 QPC du 4 août 2017, le Conseil constitutionnel a estimé que cette nouvelle rédaction n'opérait pas une juste conciliation entre la prévention des atteintes à l'ordre public et le droit au respect de la vie privée.

Il a considéré que cette disposition, insuffisamment précise, permettait « *que fasse l'objet de cette technique de renseignement un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit* ». Il a également relevé que, contrairement aux interceptions de correspondances des personnes appartenant à l'entourage d'une personne concernée par une autorisation d'interception, le nombre d'individus susceptibles de voir leurs données de connexion recueillies en temps réel n'était pas limité en quantité.

Le Conseil constitutionnel a cependant reporté les effets de sa décision d'abrogation de la disposition au 1er novembre 2017. En conséquence, la loi du 30 octobre 2017 relative à la sécurité intérieure et à la lutte contre le terrorisme, dite « SILT » (1), a modifié le dispositif issu de la loi du 21 juillet 2016, en prévoyant que le Premier ministre arrête le nombre maximal des autorisations de procéder au recueil, après avis de la CNCTR.

En pratique, comme l'a noté notre collègue Raphaël Gauvain dans son rapport sur le projet de loi SILT, « *il appartien*[t] *au Premier ministre, après avis de la CNCTR, de s'assurer que la personne concernée par la demande de recueil appartient bien à l'entourage d'une personne préalablement identifiée comme représentant une menace au regard de la nature des liens, de leur intensité, de leur régularité et de tout autre élément de nature à justifier le bien-fondé de la mesure.* » (2)

c. Les dispositifs techniques de proximité, ou « IMSI-catchers »

Pour l'ensemble des finalités de l'article L. 811-3, les données de connexion, et dans certaines conditions restrictives, les correspondances, peuvent être recueillies par le biais de dispositifs techniques de proximité, plus communément appelés « *IMSI-catchers* » (**article L. 851–6 du CSI**).

Ce dispositif peut être défini comme une antenne relais mobile factice qui se substitue, dans un périmètre donné, aux antennes relais des opérateurs permettant ainsi aux services de renseignement de disposer d'informations sur les terminaux qui s'y sont connectés. Il permet de recueillir :

---

(1) Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

(2) Assemblée nationale, XVe législature, rapport n° 164, p. 245.

– les données techniques nécessaires à l'identification d'un équipement terminal ou du numéro d'abonnement de l'utilisateur, c'est-à-dire le numéro identificateur d'usager mobile (*International Mobile Subscriber Identity [IMSI*]), qui peut se définir comme un numéro unique, stocké dans la carte SIM, permettant à un réseau mobile d'identifier un usager et le numéro international de l'équipement mobile (*International Mobile Equipment Identity [IMEI]*), qui est le numéro unique de l'équipement mobile ;

– les données techniques relatives à la localisation des équipements terminaux utilisés ;

– les correspondances. Cette dernière utilisation, définie à l'article L. 852-1 du CSI est néanmoins très encadrée (voir *infra*).

Le nombre d'*IMSI-catchers* utilisés simultanément est contingenté (1).

Lors de l'examen du projet de loi relatif au renseignement, les *IMSI-catchers* avaient concentré une large part des débats au sein de l'hémicycle.

Comme cela a été confirmé aux membres de la mission d'information au cours de ses auditions, cette technique de renseignement était en réalité utilisée depuis plus de quinze ans, sans qu'il existe un cadre juridique régissant spécifiquement son utilisation. Au demeurant, à cette époque, d'autres puissances – les États-Unis, le Royaume-Uni, Israël notamment – y avaient également recours.

Cette technique de renseignement est en revanche largement menacée par le déploiement de la 5G (2).

d. Des techniques de renseignement très utilisées

Le rapport annuel de la CNCTR fournit des indications sur l'utilisation par les services de renseignement de ces différentes techniques de renseignement.

L'accès aux données de connexion en temps différé (article L. 851–1 du CSI) demeure, de très loin, la technique de renseignement la plus utilisée, tout en étant la moins intrusive de toutes. Ces demandes ont connu une baisse de 14 % en 2019, s'établissant à :

– 25 051 s'agissant des demandes d'identification d'abonnés ou de recensement de numéros d'abonnement ;

– 14 568 s'agissant des demandes de factures détaillées (fadettes).

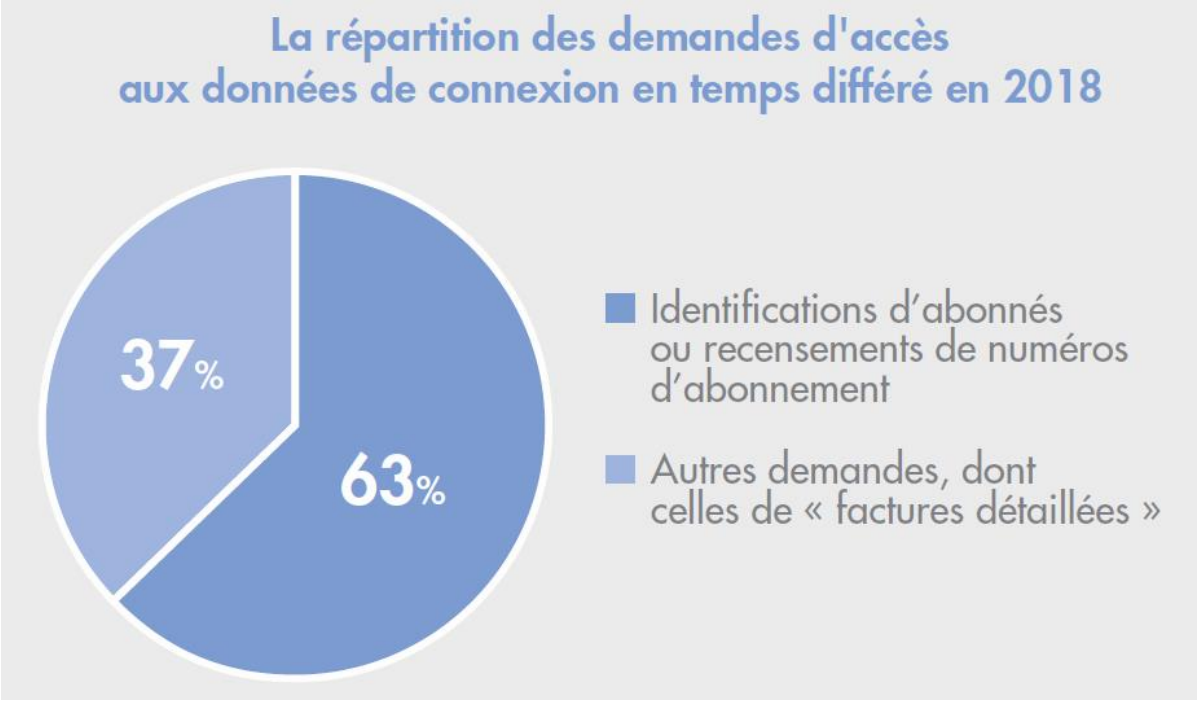
Dans son rapport, la CNCTR précise « *que les demandes comptabilisées au titre de cet article peuvent porter sur plusieurs accès à la fois. Ainsi, une même*

(1) Voir annexe n° 7.

(2) Voir deuxième partie du rapport.

demande de recensement de numéros d'abonnement téléphonique d'une personne peut entraîner le recueil de plusieurs numéros auprès de plusieurs opérateurs de communications électroniques. Le nombre de demandes examinées par la CNCTR représente donc un ensemble de dossiers comportant un ou plusieurs accès à des données de connexion en temps différé. » (1)

RÉPARTITION DES DEMANDES D'ACCÈS AUX DONNÉES DE CONNEXION EN TEMPS DIFFÉRÉ



Source : rapport d'activité de la CNCTR, 2019, p. 51.

La géolocalisation en temps réel semble être la technique auquel le recours a le plus progressé. D'après les données de la CNCTR, le recours à cette technique a augmenté de :

– 87 % en 2016 ;

– 55 % en 2017 ;

– 38 % en 2018 :

– 46,4 % en 2019, soit 7 601 demandes.

Les données relatives aux autres techniques ne sont pas publiques.

● Le contingentement du recueil des données de connexion par *IMSI-catcher* : un contigent stable depuis 2015

(1) CNCTR, rapport d'activité 2018, pp. 62 et 63.

Par un arrêté du 15 janvier 2016, le Premier ministre a fixé et réparti le contingent fixant le nombre maximal d'*IMSI-catchers* pouvant être utilisés simultanément en suivant les recommandations de la commission.

Le contingent n'a pas été modifié depuis lors. Comme l'a fait remarquer la CNCTR dans son rapport d'activité pour l'année 2018, les services chargés du renseignement pénitentiaire peuvent, depuis le 1er février 2017, former des demandes tendant au recueil de données de connexion par *IMSI-catcher*. Mais cette technique ne peut être directement mise en œuvre par eux, tant que le contingent n'a pas été modifié pour prévoir un nombre maximal d'autorisations en vigueur simultanément pour les services relevant du ministère de la Justice (1).

RÉPARTITION PAR MINISTÈRE DU CONTINGENT DE RECUEIL DE DONNÉES DE CONNEXION PAR IMSI–CATCHER

Ministère	2016
Intérieur	35
Défense	20
Douanes	5
Total	60

Source : CNCTR, rapport d'activité 2019, p. 40

● Le contingentement du recueil de données de connexion en temps réel : une mesure récente

Par une décision du 8 janvier 2018, le Premier ministre avait initialement fixé le contingent à 500.

Une augmentation de ce contingent a été décidée le 25 novembre 2019, après avis favorable de la CNCTR (2) .

RÉPARTITION PAR MINISTÈRE DU CONTINGENT DE RECUEIL DE DONNÉES DE CONNEXION EN TEMPS RÉEL

	2018	2019
Intérieur	430	650
Défense	50	50
Douanes	20	20
Total	500	720

Source : CNCTR, rapport d'activité 2019, p. 36

(1) CNCTR, rapport d'activité 2018, p. 39.

(2) Délibération de la CNCTR du 7 novembre 2019.

2. L’algorithme

a. Un outil de détection des signaux de faible intensité

Adoptée dans le contexte de l’affaire *Snowden*, la loi du 24 juillet 2015 a promu l’individualisation des techniques de renseignement s’agissant de leur cible, qui concerne essentiellement une personne spécifiquement désignée ou son entourage immédiat.

La technique de renseignement dite de l’« algorithme », prévue à l’article L. 851–3 du CSI, fait figure d’exception, même si elle est très rigoureusement encadrée.

Comme l’a souligné le rapporteur du projet de loi, notre ancien collègue Jean–Jacques Urvoas : « *l’objectif poursuivi est donc bien, pour l’État, de pouvoir recueillir, traiter, analyser et* ***recouper un grand nombre d’éléments techniques anonymes pour détecter des signaux de faible intensité*** *sur les données brutes qui témoigneraient d’une menace pesant sur la sécurité nationale. Cette disposition n’impose donc pas aux prestataires de services sur Internet une obligation générale de surveiller les informations qu’ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites, ce que prohibe l’article 15 de la directive sur le commerce électronique*. » (1)

Le I de cet article prévoit que le Premier ministre peut, après avis de la CNCTR, imposer aux opérateurs de communications électroniques et aux fournisseurs de services sur internet la mise en œuvre sur leurs réseaux de traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste. Les algorithmes ne peuvent porter que sur des données de connexion et ne doivent pas permettre l’identification des personnes auxquelles ces données se rapportent.

C’est uniquement si l’algorithme détecte des données susceptibles de caractériser l’existence d’une menace à caractère terroriste que le Premier ministre peut autoriser, après un nouvel avis de la CNCTR, l’identification des personnes concernées et le recueil des données afférentes (IV de l’article L. 853–1 du CSI).

La nécessité d’un tel outil est apparue dans le sillage de la montée en puissance de l’antiterrorisme qui, « *en accroissant très fortement le nombre de cibles potentielles à surveiller, a poussé les services intérieurs (et non plus seulement extérieurs) à vouloir recourir massivement aux moyens de surveillance électronique, alors que traditionnellement le renseignement humain était la pratique dominante des services tels que la DST ou les RG. Tandis que le renseignement extérieur ou de contre-espionnage implique une pénétration longue et progressive dans le but d’utiliser sur le moyen et le long terme des sources fiables, la nécessité impérieuse de détecter en quasi-temps réel le potentiel*

---

(1) Assemblée nationale, XIV^e^ législature, rapport n° 2697, p. 42.

passage à l'acte du terroriste amène à rechercher un instrument qui puisse effectuer presque automatiquement du " décèlement précoce ". Les nouvelles technologies numériques (données mobiles, big data*, algorithmes,* deeplearning*...) sont donc arrivées à point nommé dans les dernières années pour développer un cyber-renseignement dont les lois de 2015 ont été la reconnaissance officielle, après que quelques textes antérieurs leur ont ouvert la voie, comme en 2006 avec la collecte des données de connexion en matière anti-terroriste ou le recueil en temps réel de ces mêmes métadonnées à partir de la loi du 18 décembre 2013*. » (1)

b. Une mise en œuvre strictement encadrée par la loi et par le contrôle de la CNCTR

La loi du 24 juillet 2015 a entouré cet outil de nombreuses garanties :

– une limitation à la seule finalité de la prévention du terrorisme ;

– un avis de la CNCTR sur la demande d'autorisation, sur les paramètres de détection retenus et sur la levée de l'anonymat en cas de détection d'une menace ;

– une autorisation initiale limitée à deux mois ;

– une levée de l'anonymat uniquement en cas de menace caractérisée ;

– une destruction des données exploitées dans un délai de 60 jours à compter du recueil, sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste.

c. Une application effective depuis 2017 seulement

La CNCTR a été consultée sur le projet d'architecture générale et a rendu une délibération classifiée le 28 juillet 2016. Cet avis était favorable « *sous réserve du respect de garanties renforçant la protection de la vie privée, des observations et des recommandations avaient été formulées sur la procédure de collecte des données de connexion, les caractéristiques des données collectées, la durée de leur conservation, les conditions de leur stockage et la traçabilité des accès*. » (2) Elle avait notamment préconisé que l'architecture générale du dispositif fût placée sous la responsabilité du groupement interministériel de contrôle (GIC).

Dans une décision classifiée du 27 avril 2017, le Premier ministre a fixé les règles générales de mise en œuvre des algorithmes, en reprenant « *l'ensemble des observations et des recommandations formulées par la CNCTR* ». (3)

Le 18 juillet 2017, la CNCTR a été saisie d'une première demande tendant à la mise en œuvre d'un algorithme. Elle a examiné cette demande sous l'angle

(1) Ibid.

(2) CNCTR, rapport d'activité 2017, p. 16.

(3) CNCTR, op. cit., p. 17.

juridique (afin de vérifier que le traitement envisagé correspondait bien à la définition légale donnée par l'article L. 851-3) et technique (afin de vérifier ses fonctions effectives, la commission s'étant assurée que l'algorithme, et notamment son code source, était conforme à la description qu'en faisait la demande). La commission a estimé que cette demande ne respectait pas les garanties préconisées dans son avis du 28 juillet 2016 et fixées par le Premier ministre dans sa décision du 27 avril 2017. Elle a donc émis un avis défavorable à cette première demande.

Le 25 septembre 2017, la CNCTR a été saisie d'une demande rectificative portant sur le même algorithme : elle a pris acte des mesures prises pour renforcer les garanties présentées par l'architecture générale de mise en œuvre du traitement envisagé et a émis un avis favorable à cette demande.

Le Premier ministre a suivi l'avis de la commission en autorisant la mise en œuvre de l'algorithme le 12 octobre 2017.

Le **premier algorithme a donc été autorisé par le Premier ministre le 12 octobre 2017** seulement. À l'issue des deux premiers mois de fonctionnement, la CNCTR a émis un avis favorable à un premier renouvellement pour une durée de deux mois [(1)], puis à de nouveaux renouvellements dans le cadre du droit commun, pour une durée de quatre mois. Il est toujours en fonctionnement aujourd'hui.

Depuis la mise en œuvre de cet algorithme, la CNCTR a été conduite à rendre plusieurs avis sur des demandes d'accès à des données détectées ainsi que d'identification des personnes concernées.

Deux nouvelles autorisations ont été accordées en 2018.

Cet outil fait l'objet d'une mise en œuvre très limitée puisqu'à la fin de l'année 2018, **trois algorithmes avaient été mis en œuvre depuis l'entrée en vigueur de la loi du 24 juillet 2015 et étaient en fonctionnement.**

d. Un dispositif expérimental, prolongé une première fois en 2017

Le caractère très novateur de cette technique a conduit le législateur à prévoir, à l'article 25 de la loi relative au renseignement, une application temporaire de ce dispositif, jusqu'au 31 décembre 2018, son renouvellement devant être autorisé par la loi. Afin d'en évaluer la pertinence et d'éclairer le Parlement sur l'opportunité d'en proroger l'usage, cet article prévoyait un rapport sur son application au plus tard le 30 juin 2018.

Eu égard à la mise en œuvre tardive du premier algorithme, la loi du 30 octobre 2017 précitée a prorogé de deux années l'expérimentation en cours de

(1) Cette condition plus restrictive était préconisée par la commission au regard des résultats constatés lors de la première période d'autorisation et afin de s'assurer de la pertinence et de la fiabilité des caractéristiques techniques de l'algorithme.

cette technique et, en conséquence, a reporté au 30 juin 2020 la remise du rapport d'application.

Pour le Gouvernement, « *la date de 2018 retenue par le législateur au moment de l'examen du projet de loi relatif au renseignement sembl[ait] (…) prématurée et il appara[issait] que le bilan qui pourrait être tiré de la mise en œuvre de cette technique (…) au 30 juin 2018 ne permettra[it] pas au Parlement de se prononcer de manière satisfaisante sur l'opportunité de pérenniser cette technique ou d'y mettre fin* » (1).

La CNCTR, dans son rapport d'activité 2017, a recommandé au Gouvernement d'informer le Parlement, sans attendre l'échéance légale, par un rapport déposé après une première année de mise en œuvre de l'algorithme.

e. Des mises en œuvre intéressantes mais limitées aux données de connexion téléphoniques

D'après les informations qui ont été transmises à la mission d'information, les trois algorithmes ont fourni des résultats intéressants. Ils sont néanmoins moins probants qu'ils ne pourraient l'être eu égard au champ relativement limité des données qui peuvent faire l'objet de l'algorithme. Les données pouvant nourrir l'algorithme sont en effet limitées aux seules données de connexion ne révélant aucun contenu, à l'exception donc des URL (2).

Les membres de la mission d'information ont donc envisagé plusieurs pistes de réflexion permettant d'améliorer l'efficacité des algorithmes (3).

3. Les interceptions de sécurité

Les interceptions de sécurité permettent d'accéder au contenu des communications et aux données de connexion qui y sont associées.

a. Un cadre juridique dont les fondements ont été définis par la loi du 10 juillet 1991

Avant l'entrée en vigueur de la loi du 24 juillet 2015, le régime des interceptions de correspondances était défini par la loi du 10 juillet 1991 précitée, codifié dans le code de la sécurité intérieure. Les demandes d'interceptions étaient adressées au Premier ministre par les ministres concernés. L'autorisation était accordée pour une durée de quatre mois renouvelable.

---

(1) Exposé sommaire de l'amendement n° CL270 du Gouvernement.

(2) URL (sigle de l'anglais : Uniform Resource Locator*, littéralement « localisateur uniforme de ressource »). Plus couramment appelée adresse web, l'URL est une chaîne de caractères uniforme permettant d'identifier une ressource du Web par son emplacement et de préciser le protocole internet pour la récupérer (par exemple http ou https). Elle peut localiser divers formats de données (document HTML, image, son…).*

(3) Voir troisième partie du rapport.

En application de l'article L. 243-8 du code de la sécurité intérieure, une autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) assurait un contrôle ***a posteriori*** de l'autorisation par le Premier ministre, en ayant la possibilité d'adresser des recommandations au Premier ministre en cas d'autorisation accordée en contradiction avec les dispositions applicables aux interceptions de sécurité.

Toutefois, une pratique différente, plus protectrice, s'est rapidement établie, sans qu'aucun Premier ministre ne la remette en cause : la CNCIS formulait son avis *a priori*, avant que le Premier ministre autorise la mesure, celui-ci se conformant en outre à l'avis rendu, à l'exception de quelques cas très exceptionnels.

L'exécution des opérations relatives aux interceptions de sécurité était centralisée au sein d'un service placé auprès du Premier ministre, le GIC.

Le nombre d'interceptions de sécurité pouvant être simultanément menées était contingenté par un arrêté du Premier ministre.

b. Un cadre juridique largement repris par la loi du 24 juillet 2015

La loi du 24 juillet 2015 a peu modifié le régime des interceptions de sécurité, qui, comme on vient de le voir, faisaient déjà l'objet d'un régime juridique précis et d'un contrôle par la CNCIS. Elles font désormais l'objet d'un chapitre dédié au sein du titre V.

La plupart des modalités du régime actuel relatif aux interceptions de sécurité ont donc été maintenues, à trois grandes exceptions près :

– la **pratique préexistante d'un avis préalable de l'autorité chargée du contrôle a été consacrée dans la loi** ;

– le principe d'un **contingentement** a été renforcé, puisque l'arrêté du Premier ministre de fixation du contingentement est pris après avis de la CNCTR ;

– la possibilité de demander l'interception des communications de personnes, qui, sans présenter par elles-mêmes une menace, appartiennent à l'**entourage** de la personne faisant l'objet d'une mesure de surveillance et sont « *susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation* ».

Cette dernière disposition était une innovation par rapport à la doctrine constante de la CNCIS, qui s'était toujours refusée à accorder des autorisations d'interception pour des personnes appartenant à l'entourage de personnes suivies, mais ne justifiant pas elles-mêmes une écoute, en exigeant une présomption d'implication directe et personnelle dans un projet en lien avec l'une des finalités permettant l'interception de la personne avec les faits motivant la demande d'écoute.

Les interceptions de sécurité peuvent être réalisées par le biais d'*IMSI–catchers*, mais pour certaines finalités uniquement (1).

c. La création d'une nouvelle modalité d'interception de sécurité après la loi du 24 juillet 2015 : les écoutes hertziennes

En 1991, le législateur a autorisé les services de renseignement à prendre les mesures « *pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne* » (2) sans les soumettre au régime juridique d'autorisation préalable ou de contrôle des interceptions de sécurité décidées par l'autorité administrative.

Les activités concernaient des mesures générales et non ciblées de surveillance et de contrôle des transmissions empruntant la voie hertzienne, c'est-à-dire les communications sans support filaire utilisant le champ électromagnétique pour transmettre un message entre deux antennes. Il s'agit des communications radio très longue distance (de type VLF ou très basses fréquences), longue distance (de type HF ou hautes fréquences) et courte distance (de type V/UHF ou très et ultra hautes fréquences, comme les talkies walkies). Ces mesures sont généralement utiles pour identifier, en amont d'une interception, une menace potentielle.

L'application à ces activités d'un régime dérogatoire du droit commun s'expliquait compte tenu de leurs modalités techniques – elles ne visent pas des communications individualisables, localisées et quantifiables – et de la nature de leurs cibles. En effet, les communications hertziennes consistent en des signaux envoyés depuis une antenne émettrice qui peuvent être captés par toute antenne réceptrice située dans le périmètre d'émission ; dans la mesure où aucun opérateur de communications électroniques n'intervient, le message émis ne comporte pas, en principe, d'informations sur l'identification ou la localisation de l'émetteur et du destinataire.

Ces dispositions, codifiées en 2012 à l'article L. 241-3 du code de la sécurité intérieure puis transférées en 2015 à l'article L. 811-5 du même code (3), sont demeurées inchangées, hors du cadre juridique applicable aux activités de surveillance des communications de droit commun.

Ce dispositif dérogatoire faisait l'objet d'une interprétation stricte de la part de la CNCIS puis de la CNCTR. La CNCIS a ainsi, dès 1998, exclu que ce régime puisse autoriser des recherches ciblées destinées à intercepter des communications individualisables et serve de fondement légal à l'interception de communications échangées par un téléphone mobile, même si une partie de celles-ci est acheminée par voie hertzienne, entre le terminal et l'antenne-relais.

---

(1) Indépendance nationale, intégrité du territoire et défense nationale (1° de l'article L. 811–3), prévention du terrorisme (4°) et prévention des atteintes à la forme républicaine des institutions (a du 5°).

(2) Article 20 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances.

(3) Article 11 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

Le Conseil constitutionnel, par sa décision n° 2016-590 QPC du 21 octobre 2016, a déclaré contraires à la Constitution ces dispositions, qui permettent, au moins en théorie, aux pouvoirs publics de surveiller toute transmission empruntant la voie hertzienne sans exclure l'interception de communications individualisables. Il a estimé que, « *faute de garanties appropriées* » – finalités des mesures envisagées, techniques utilisées, définition des conditions de fond ou de procédure préalables au recours à ces techniques –, l'article L. 811-5 précité portait « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration de 1789* » (1).

En conséquence, la loi SILT précitée a créé dans le code de la sécurité intérieure, outre un régime de l'hertzien ouvert (voir *infra*), un article L. 852–2 relatif à l'interception de correspondances au sein d'un réseau hertzien privatif et n'impliquant pas l'intervention d'un opérateur de communications électroniques. Ce régime obéit aux mêmes règles de procédure que les interceptions de correspondances classiques.

d. L'utilisation croissante des interceptions de sécurité

Cela peut sembler paradoxal car internet est très majoritairement chiffré et de plus en plus impénétrable mais les interceptions de sécurité – non seulement de voix mais aussi de flux internet – connaissent une forte croissance. Le recours aux interceptions de sécurité a ainsi crû en 2019, de façon importante, dans un contexte marqué par une menace terroriste persistante ainsi que par la nécessité de prévenir des violences collectives de nature à porter gravement atteinte à la paix publique. Le taux d'augmentation s'élève à 19 %. Par comparaison, les taux d'augmentation des trois années précédentes étaient également significatifs :

– + 5,6 % en 2016 ;

– + 7,6 % en 2017 ;

– + 20 % en 2018

Saisie par le Premier ministre le 15 mai 2019 d'un projet d'augmentation d'environ 11 % du contingent applicable aux interceptions de sécurité, précédemment fixé à 3 600 par une décision du 28 juin 2018, la CNCTR s'est prononcée par une délibération classifiée adoptée en formation plénière le 6 juin 2019. Après avoir constaté, comme lors des deux précédentes augmentations du contingent en 2017 et 2018, que le nombre maximal d'autorisations simultanément en vigueur était proche d'être atteint, elle a estimé avéré le besoin d'augmenter une nouvelle fois le contingent au regard notamment de la persistance, à un niveau élevé, de la menace terroriste.

---

(1) Considérant 9 de la décision n° 2016-590 QPC du 21 octobre 2016

Par une décision du 5 juillet 2019, le Premier ministre a fixé et réparti le nouveau contingent comme suit.

RÉPARTITION PAR MINISTÈRE DU CONTINGENT D'INTERCEPTION DE SÉCURITÉ

	1991	1997	2003	2005	2009	2014	2015	2017	2018	2019
Intérieur	928	1190	1190	1290	1455	1785	2235	2545	3000	3050
Défense	232	330	400	450	285	285	320	320	400	550
Douanes	20	20	80	100	100	120	145	145	150	150
Justice								30	50	50
Total	1180	1540	1670	1840	1840	2190	2700	3040	3600	3800

Source : CNCTR, rapport d'activité 2019, p. 34

Les révisions du contingent sont de plus en plus fréquentes, il s'agit de la quatrième en cinq ans, alors qu'il n'y en avait eu que cinq entre 1991 et 2014.

4. La sonorisation de certains lieux et véhicules et la captation d'images et de données informatiques

a. Un cadre juridique novateur, inspiré du cadre judiciaire

La loi du 24 juillet 2015 a repris dans le cadre de la police administrative un certain nombre de techniques utilisées en police judiciaire (1), introduites par la loi dite « Perben II » (2) et par loi dite « LOPPSI 2 » (3) :

– la sonorisation de certains lieux et véhicules et la fixation d'image (**article L. 853–1**) ;

– le recueil de données informatiques et la captation de données informatiques, qui permet d'accéder à des données informatiques telles qu'elles s'affichent sur un écran pour l'utilisateur de données (**article L. 853–2**) ;

– l'introduction dans un lieu privé ou dans un véhicule pour mettre en place, utiliser ou retirer un dispositif technique (balise, sonorisation ou fixation d'image, recueil de données informatiques, captation de données informatiques) (**article L. 853–3**).

Eu égard à leur caractère intrusif, le recours à ces techniques est subsidiaire : les services de renseignement ne peuvent y recourir que si les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé.

---

(1) Les modalités de sonorisation ou de captation d'images sont définies à l'article 706-96 code de procédure pénale. Les modalités relatives à la captation de données informatiques le sont à l'article 706-102-1 du même code. L'article 57-1 du code de procédure pénale définit quant à lui les modalités d'extraction des données contenues au sein d'un système de traitement automatisée de données.

(2) Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité relative à la grande criminalité.

(3) Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

On remarquera que ces différentes techniques requièrent d'importants moyens techniques et matériels. Dans le cadre des consultations du livre blanc sur la sécurité intérieure, l'hypothèse de la création d'un service inspiré du service technique national de captation judiciaire [(1)], afin de répondre aux besoins des services du second cercle en la matière, a pu être évoquée.

b. Une évolution à la marge de la captation de données informatiques

Seule la technique de la captation de données informatiques a fait l'objet d'une modification depuis la loi du 24 juillet 2015.

En effet, l'article 15 de la loi du 30 octobre 2017 précitée a clarifié le champ d'application de l'article L. 853-2 du code de la sécurité intérieure afin d'anticiper les évolutions opérationnelles de la technique de captation de données informatiques émises ou reçues par tout type de périphérique, et pas seulement par les périphériques audiovisuels. Le rapporteur de la loi, notre collègue Raphaël Gauvain, a indiqué que « *cette disposition avait en pratique pour effet d'intégrer le recueil de certaines transmissions hertziennes, notamment les transmissions par protocoles de communication sans fil tels que le* wifi*, dans le champ d'application de la technique de captation de données informatiques*. » [(2)] Cette disposition a, en particulier, permis de donner une base légale à la captation de données informatiques échangées via des objets connectés.

5. Les mesures de surveillance internationale

La surveillance des communications internationales vise les communications qui sont émises de ou reçues à l'étranger. Elle peut concerner à la fois les données de connexion et les interceptions de correspondances.

Le législateur de 2015 a promu un **principe de territorialité** en différenciant les mécanismes d'autorisation et de contrôle selon que la technique vise ou non une surveillance nationale. Pour les membres de la mission d'information, cette distinction s'impose pour des raisons en particulier tactiques, nos homologues mettant également en œuvrent cette dichotomie.

a. La censure du dispositif prévu par la loi du 24 juillet 2015 par le Conseil constitutionnel pour incompétence négative du législateur

S'agissant des mesures de surveillance internationale, la loi relative au renseignement prévoyait un chapitre IV autonome du code de la sécurité intérieure, composé d'un article unique L. 854-1.

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel, sans se prononcer sur le fait de savoir si l'atteinte au droit au

---

(1) Arrêté du 9 mai 2018 portant création du service à compétence nationale dénommé « service technique national de captation judiciaire ».

(2) Assemblée nationale, XV^e^ législature, rapport n° 164, p. 240.

respect de la vie privée portée par les mesures de surveillance internationale était manifestement excessive, a procédé à une censure de ces dispositions. Il a en effet estimé qu'en ne « *définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1, ni celles du contrôle par la commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre, le législateur n'a pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* ».

Comme l'a souligné le président de la commission des Lois du Sénat Philippe Bas dans son rapport sur le projet de loi relatif aux mesures de surveillance des communications électroniques internationales, « *dès lors que ces dispositions n'ont pas vocation à permettre l'interception de communications émises ou reçues sur le territoire national, il aurait également été possible d'en conclure, comme l'a souligné le Gouvernement dans ses observations complémentaires, que les exigences liées à l'exercice des libertés fondamentales peuvent ne pas être les mêmes pour un résident français et pour une personne résidant à l'étranger, à l'instar du raisonnement suivi par le juge constitutionnel dans une décision de 2012, par laquelle il a estimé que certaines obligations constitutionnelles ne s'imposaient pas à l'État hors du territoire de la République*. » (1)

b. La loi du 30 novembre 2015

Une proposition de loi a été déposée par la présidente de la commission de la Défense d'alors, Mme Patricia Adam. Elle a été adoptée par le Parlement et a été promulguée le 30 novembre 2015 (2). Elle reprend l'économie générale des dispositions de l'article L. 854-1 de CSI tel qu'initialement adopté par le Parlement tout en répondant aux motifs de la censure du Conseil constitutionnel.

Les mesures de surveillance des communications électroniques internationales restent régies exclusivement par les articles L. 854–1 et L. 854–2, étoffés par rapport à la version initiale. Ils détaillent l'objet des mesures de surveillance internationale, ainsi que la procédure et le contenu des autorisations de mise en œuvre de ces mesures délivrées par le Premier ministre. Surtout, ils précisent le contenu du contrôle opéré *a posteriori* par la CNCTR sur ces mesures, lequel contrôle est rendu identique à celui exercé sur la mise en œuvre des techniques de renseignement sur le territoire national.

Les mesures de surveillance des communications internationales supposent deux types d'autorisations successives, l'une d'interception (3), l'autre

---

(1) Sénat, rapport n° 97 (2015-2016) de M. Philippe Bas sur le projet de loi relatif aux mesures de surveillance des communications électroniques internationales, octobre 2015, p. 15.

(2) Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

(3) I de l'article L. 854–2.

d'exploitation. Cette dernière autorisation diffère selon qu'elle permet une exploitation :

– non individualisée, auquel cas elle est limitée à des données de connexion [(1)] ;

– individualisée, auquel cas elle peut porter sur des correspondances et des données de connexion. En revanche, elle doit dans ce cas désigner la finalité poursuivie, les motifs des mesures, les zones géographiques, les organisations, les groupes de personnes ou personnes concernés, le service spécialisé en charge de l'exploitation [(2)].

Ce nouveau régime juridique de la surveillance des communications internationales a été **déclaré conforme à la Constitution par le Conseil constitutionnel** dans sa décision n° 2015-722 DC du 26 novembre 2015. Le Conseil constitutionnel a notamment relevé « *que le législateur a précisément défini les conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales, celles d'exploitation, de conservation et de destruction des renseignements collectes ainsi que celles du contrôle exercé par la commission nationale de contrôle des techniques de renseignement* ».

À cet égard, il a souligné « *que le législateur a prévu que la commission nationale de contrôle des techniques de renseignement reçoit communication de toutes les décisions et autorisations du Premier ministre mentionnées à l'article L. 854-2 et qu'elle dispose d'un accès permanent, complet et direct aux dispositifs de traçabilité, aux renseignements collectés, transcriptions et extractions réalisées ainsi qu'aux relevés mentionnés au quatrième alinéa de l'article L. 854-6 retraçant les opérations de destruction, de transcription et d'extraction ; que la commission peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de sa mission ; que sont applicables aux contrôles pratiques par la commission sur les mesures de surveillance internationale les dispositions de l'article L. 833-3 qui réprime de peines délictuelles les actes d'entrave à l'action de la commission* » (cons. 14).

Le Conseil en a déduit que l'ensemble des dispositions examinées *« ne portent pas d'atteinte manifestement disproportionnée au droit* au *respect de la vie privée et au secret des correspondances »* (cons. 15). S'agissant enfin du contrôle juridictionnel, il a jugé « *que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure ; qu'en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale* », admettant ainsi

(1) II de l'article L. 854–2.

(2) III de l'article L. 854–2.

que le recours susceptible d'être formé à l'encontre de mesures de surveillance internationale, qui présente un caractère intermédié, ne porte pas atteinte aux principes constitutionnels.

c. Des compléments substantiels apportés en 2018

Ces articles ont été substantiellement complétés par la loi du 13 juillet 2018 de programmation militaire (1), du fait de l'adoption au Sénat d'un amendement du Gouvernement visant à tirer les conséquences de l'intensification des menaces pesant sur les intérêts fondamentaux de la Nation.

Dans le dispositif imaginé en 2015, les interactions entre les deux régimes de surveillance nationale et de surveillance internationale étaient résiduelles : l'exploitation des communications vers ou depuis l'étranger liées à un numéro ou un identifiant français n'était possible que si son utilisateur était à l'étranger et présentait une menace avérée pour les intérêts fondamentaux de la Nation.

Il n'était donc pas possible d'exploiter les données légalement recueillies au titre de la surveillance des communications internationales pour apprécier la menace que présente un résident français en France du fait de ses liens hors du territoire national. L'expérience des années 2015-2018 a conduit à évaluer différemment le caractère transnational de la menace, qu'il s'agisse de terrorisme, de criminalité organisée ou de cyberattaques. La ministre des armées, Mme Florence Parly, a montré les difficultés opérationnelles posées par le cadre de la loi de 2015 : « *Il est donc difficilement compréhensible que l'on se coupe ainsi de données légalement recueillies. Par exemple, un résident français qui planifierait un attentat depuis le Yémen peut être surveillé. En revanche, ses complices, qui font des allers-retours entre la France et la Belgique, ne peuvent pas l'être*. »

● Les vérifications ponctuelles

Les services de renseignement peuvent désormais procéder à des vérifications ponctuelles sur les **données de connexion** légalement interceptées dans le cadre de la surveillance des communications internationales aux seules fins de détecter une menace pour les intérêts fondamentaux de la Nation liée aux relations entre des numéros d'abonnement ou des identifiants techniques rattachables au territoire français et des zones géographiques, des organisations ou des personnes faisant l'objet d'une surveillance internationale (2).

Ces vérifications ponctuelles prennent la forme d'opérations très rapides (quelques minutes), non répétées, et susceptibles de mettre en évidence un graphe relationnel ou la présence à l'étranger d'une personne. En permettant de confirmer ou, au contraire, d'infirmer l'existence d'une menace pour les intérêts

---

(1) Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

(2) IV de l'article L. 854–2.

fondamentaux de la Nation, elles offrent un élément d'appréciation supplémentaire pour décider de la mise en œuvre, à bon escient, des techniques de renseignement.

Ainsi que l'ont confirmé le Conseil d'État dans l'avis rendu le 4 mai 2018 et la CNCTR dans sa délibération du 9 mai suivant, des levées de doute ainsi délimitées ne caractérisent pas une surveillance individuelle, notion mentionnée au troisième alinéa de l'article L. 854-1 du code de la sécurité intérieure pour délimiter étroitement les liens entre surveillances nationale et internationale.

Une vérification ainsi délimitée n'apparaissant toutefois pas nécessairement suffisante au regard des enjeux posés par certaines menaces aux intérêts fondamentaux de la Nation, deux exceptions sont prévues qui permettent d'effectuer des vérifications ponctuelles sur des **correspondances** :

– pour prévenir des **menaces terroristes urgentes**, les services doivent pouvoir orienter plus précisément leurs investigations. Dans ce cadre, les vérifications ponctuelles ont une obligation de traçabilité renforcée (transmission immédiate des numéros et identifiants concernés au Premier ministre et à la CNCTR) ;

– pour détecter les **cyberattaques** qui sont susceptibles de mettre en cause l'indépendance nationale ou les intérêts de la défense nationale. La démarche est, dans ce cadre, très différente dès lors qu'il ne s'agit pas de mettre en évidence la menace ou la vulnérabilité que présente un individu du fait de son comportement ou de ses relations, mais des marqueurs techniques de flux malveillants circulant entre des machines victimes ou relais de l'attaque informatique.

Quel que soit le type de vérifications, et dès lors que celles-ci font apparaître la nécessité d'une surveillance, l'exploitation des communications ne peut être poursuivie que *via* les techniques de renseignement mises en œuvre sur le territoire national ou dans le cadre du régime de la surveillance des communications internationales.

● Une nouvelle mesure de surveillance individuelle

La loi du 13 juillet 2018 a créé une nouvelle mesure de surveillance individuelle, permettant l'exploitation des données de connexion et des correspondances d'un identifiant technique rattachable au territoire national interceptées dans le cadre de la surveillance des communications internationales alors même que son utilisateur est en France [(1)].

Cette mesure est strictement encadrée :

(1) V de l'article L. 854–2.

– elle ne peut être demandée que pour la promotion et la défense de certains des intérêts fondamentaux de la Nation [1] ;

– elle requiert une autorisation du Premier ministre, après avis de la CNCTR ;

– lorsqu'elles portent sur des correspondances, les autorisations d'exploitation en vigueur simultanément ne pourront être accordées que dans la limite d'un contingent défini par le Premier ministre, après avis de la CNCTR.

● Une mise en cohérence de l'exploitation de certaines données

La même démarche de réévaluation de la frontière entre les régimes de surveillance applicables sur le territoire national et à l'étranger a par ailleurs conduit le législateur à mettre fin à une situation peu cohérente, afin que certaines techniques de renseignement autorisées sur le territoire national puissent permettre l'exploitation des données strictement correspondantes interceptées dans le cadre de la surveillance des communications internationales, lorsque l'autorisation de mise en œuvre de ces techniques le prévoit (article L. 854–1).

● L'extension du contrôle *a priori* de la CNCTR

La loi du 13 juillet 2018 a inscrit dans la loi l'obligation pour le Premier ministre de recueillir un avis *a priori* de la CNCTR avant d'accorder toute autorisation d'exploitation ou de seules données de connexion interceptées, sur le fondement des III et V de l'article L. 854–2.

Pratiquée depuis mai 2016, d'abord à titre expérimental puis pérenne, en application d'un accord entre le Premier ministre et la CNCTR, cette consultation préalable, a, selon la CNCTR « *prouvé son utilité pour garantir la légalité, en particulier le caractère proportionné, des atteintes portées à la vie privée par les mesures de surveillance des communications électroniques internationales* » [2].

d. Usage des mesures de surveillance des communications internationales

● Une forte augmentation des demandes tendant à l'exploitation de communications internationales

En 2019, la commission a rendu 2 133 avis sur des demandes tendant à l'exploitation de communications internationales interceptées, contre 971 en 2018.

La CNCTR, dans son dernier rapport d'activité explique cette **forte hausse par deux motifs.** Le premier correspond à une modification de la pratique des services demandeurs, préconisée par la CNCTR, consistant à solliciter des

(1) Indépendance nationale, intégrité du territoire et défense nationale (1°), intérêts majeurs de la politique étrangère, exécution des engagements européens et internationaux de la France et prévention de toute forme d'ingérence étrangère (2°), prévention du terrorisme (4°), prévention de la criminalité et de la délinquance organisées (6°), prévention de la prolifération des armes de destruction massive (7°).

(2) CNCTR, rapport d'activité 2018, p. 34.

autorisations d'exploitation plus circonscrites et plus précises. Elle conduit, corrélativement, à une augmentation du nombre de demandes d'autorisation soumises à l'examen de la commission, sans que cela corresponde à une extension du champ de la surveillance.

Le second et principal motif d'augmentation du nombre des demandes est lié à l'**entrée en vigueur des dispositions du V de l'article L. 854-2** du code de la sécurité intérieure qui permet désormais aux services habilités à cet effet de solliciter, pour les seules finalités et dans les conditions prévues par ce texte, des autorisations d'exploitation concernant des identifiants techniques rattachables au territoire national, d'où communique l'utilisateur.

● L'augmentation du contingent de la mesure de surveillance internationale du V de l'article L. 854–2

Saisie par le Premier ministre le 15 janvier 2019 d'un projet fixant le nombre maximal d'autorisations simultanément en vigueur accordées sur le fondement du V de l'article L. 854-2 du code de la sécurité intérieure, la CNCTR s'est prononcée par une délibération classifiée adoptée en formation plénière le 7 février 2019. Elle a considéré que le contingent initialement proposé n'était pas suffisamment proportionné au regard des intérêts fondamentaux de la Nation susceptibles d'être invoqués pour recourir à cette mesure de surveillance individuelle et de l'atteinte que celle-ci porte au droit au respect de la vie privée. Elle a proposé de le limiter à 1 000 (1) .

Par une décision du 19 avril 2019, le Premier ministre a suivi l'avis de la CNCTR. Il a fixé et réparti le contingent de la manière suivante :

CONTINGENT DE LA MESURE DE SURVEILLANCE INTERNATIONALE DU V DE L'ARTICLE L. 854–2

	2019
Intérieur	750
Défense	210
Douanes	40
Total	1000

Source : CNCTR, rapport d'activité 2019, p. 39

6. Les mesures de surveillance de certaines communications hertziennes

Conséquence de la décision n° 2016-590 QPC du 21 octobre 2016, la loi du 30 octobre 2017 précitée a complété le champ des techniques de recueil de renseignement soumis à autorisation institué par la loi du 24 juillet 2015 par un régime légal – et résiduel – d'interception et d'exploitation des communications hertziennes échangées sur un réseau public.

(1) CNCTR, rapport d'activité 2019, p. 39.

Sont visées par ce nouveau régime « *l'interception et* (…) *l'exploitation des communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques lorsque cette interception et cette exploitation n'entrent dans le champ d'application d'aucune des techniques de renseignement* ». En pratique, est concerné par ce régime le trafic des radioamateurs, des cibis et talkies-walkies analogiques, soumis à aucun chiffrement et ouvert à toute antenne réceptrice réglée sur la bonne fréquence, ainsi que les communications radio longue et très longue distances (de type VLF et HF). En revanche, ne sont pas concernés par cette technique les réseaux gérés par un opérateur de communications électroniques (téléphone portable, réseau *wifi*, trafic des abonnées par satellite…).

En application de l'article L. 855–1 A du CSI, le régime encadrant le recours à cette technique est allégé par rapport au droit commun des techniques de recueil de renseignements.

Toutefois, certaines garanties sont prévues, qui répondent aux exigences posées par le Conseil constitutionnel :

– les écoutes hertziennes sont réservées à la finalité de défense et de promotion des intérêts fondamentaux de la Nation au sens de l'article L. 811-3 du même code ;

– seuls peuvent y avoir recours les services spécialisés de renseignement – dits du « premier cercle » – et ceux des services non spécialisés – dits du « deuxième cercle » – habilités par décret, pour des finalités précises.

L'article L. 855-1 C dote la CNCTR d'un pouvoir de contrôle global des mesures de surveillance des communications hertziennes au travers d'un droit d'information et de communication, d'un droit d'inspection sur place et d'un droit d'alerte auprès du Premier ministre et de la délégation parlementaire au renseignement. L'objectif de ce pouvoir de contrôle est notamment de mettre la CNCTR en mesure de vérifier le respect du champ d'application, d'une part, des interceptions des correspondances échangées au sein d'un réseau privé de communications électroniques hertziennes et, d'autre part, des communications hertziennes échangées sur un réseau public.

C. LES DIFFÉRENTES PROCÉDURES D'AUTORISATION

La loi du 24 juillet 2015 a fixé le cadre légal régissant les procédures d'autorisation permettant la mise en œuvre d'une technique de renseignement, en prévoyant une procédure de droit commun et une procédure d'exception, dite de « *l'urgence absolue* ».

1. La procédure de droit commun

Les articles L. 821-1 et suivants détaillent la procédure d'autorisation de droit commun, qui n'a pas évolué depuis la loi du 24 juillet 2015, à l'exception d'ajustements rédactionnels.

La mise en œuvre sur le territoire national des techniques de recueil de renseignement est soumise à autorisation préalable du Premier ministre, délivrée après avis de la CNCTR.

Cette autorisation est délivrée sur demande écrite et motivée du ministre concerné (1). La demande doit préciser un certain nombre d'éléments (2).

L'exercice du contrôle *a priori* de la CNCTR est enserré dans des délais de procédure contraignants : la commission dispose d'un délai de vingt-quatre heures pour statuer, si l'avis est rendu par un seul de ses membres. Le délai est porté à soixante-douze heures, si la commission se prononce en formation collégiale. Comme l'a souligné le président de la CNCTR aux membres de la mission d'information, ces contraintes légales ont conduit la commission à organiser un dispositif de permanence lui permettant de statuer à tout moment et dans des conditions adaptées à l'urgence de certaines demandes, urgence qui peut imposer de les traiter dans des délais inférieurs au délai légal.

Les avis sont communiqués sans délai au Premier ministre. En l'absence d'avis rendu dans les délais, celui-ci est réputé donné. Ce cas ne s'est cependant jamais produit, la commission ayant toujours rendu un avis exprès.

Lorsque l'autorisation est donnée après un avis défavorable de la CNCTR, elle indique les motifs pour lesquels cet avis n'a pas été suivi. Cette situation ne s'est encore jamais présentée d'après les informations transmises aux membres de la mission d'information.

Certaines professions ou mandats – parlementaire, magistrat, avocat, journaliste – font l'objet d'une procédure particulière. Ils ne peuvent pas faire l'objet d'une demande de mise en œuvre de technique de renseignement à raison de l'exercice de leurs fonctions. Si une demande de technique de renseignement les concerne, elle est alors examinée par la CNCTR en formation plénière. Ils ne peuvent faire l'objet d'une technique de renseignement en application de la procédure d'urgence absolue (cf. *infra*).

2. Une utilisation exceptionnelle de la procédure de l'urgence absolue

L'article L. 821-5 permet la mise en œuvre d'une procédure dérogatoire, en cas d'urgence absolue et pour certaines finalités limitativement énumérées (1).

---

(1) Ministres de la défense, de l'intérieur, de la justice, de l'économie, du budget et des douanes.

(2) Technique(s) à mettre en œuvre, service pour lequel la technique est demandée, finalité(s) poursuivie(s), motif(s) des mesures, durée de validité de l'autorisation, personne (s), lieu(x), véhicule(s) concerné(s).

Dans cette situation, le Premier ministre peut délivrer de manière exceptionnelle l'autorisation de mise en œuvre d'une technique de renseignement, sans avis préalable de la CNCTR. Il doit en informer cette dernière sans délai et par tout moyen.

Le Premier ministre doit lui faire parvenir, dans un délai maximal de 24 heures à compter de la délivrance de l'autorisation, tous les éléments de motivation et ceux justifiant le caractère d'urgence absolue.

Le Conseil constitutionnel, dans sa décision n° 2015-713 DC du 23 juillet 2015, a jugé cette procédure conforme à la Constitution, notamment car elle n'est pas applicable lorsque la mise en œuvre des techniques de renseignement implique l'introduction dans un lieu privé à usage d'habitation et « *n'est donc pas susceptible d'affecter l'inviolabilité du domicile* » (2).

Comme l'a souligné le président Delon, « *cette exception, très encadrée, est circonscrite à des cas exceptionnels d'extrême urgence et à la prévention d'atteintes particulièrement graves à l'ordre public et n'a eu, en plus de trois ans,* ***à s'appliquer qu'une seule et unique fois, en décembre 2015, alors qu'un risque imminent d'attentat terroriste était suspecté.*** *On peut donc aujourd'hui affirmer que le contrôle préalable de la CNCTR est réellement la règle.* » (3)

3. La censure de la procédure dite de « l'urgence opérationnelle »

Une deuxième procédure dérogatoire était initialement prévue par la loi du 24 juillet 2015, celle dite de « l'urgence opérationnelle », à l'article L. 821-6.

En cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement, des balises et des *IMSI-catchers* pouvaient, de manière exceptionnelle, être installés, utilisés et exploités sans autorisation préalable par des agents individuellement désignés et habilités. Le Premier ministre, le ministre concerné et la CNCTR en étaient informés sans délai et par tout moyen. Le Premier ministre pouvait ordonner à tout moment que la mise en œuvre de la technique concernée soit interrompue et que les renseignements collectés soient détruits sans délai.

Cette procédure s'inspirait de la procédure judiciaire, puisqu'un officier de police judiciaire peut, d'initiative, poser des balises de géolocalisation, en cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, et solliciter immédiatement auprès du

---

(1) Indépendance nationale, intégrité du territoire et défense nationale (1° de l'article L. 811–3), prévention du terrorisme (4°) et prévention des atteintes à la forme républicaine des institutions (a du 5°).

(2) Conseil constitutionnel, décision n° 2015–713 DC du 23 juillet 2015, Loi relative au renseignement, *cons. 24.*

(3) In La commission nationale de contrôle des techniques de renseignement, Le droit du renseignement, L'Académie du renseignement, Francis Delon, p. 125.

magistrat la validation de cet acte technique (article 230-35 du code de procédure pénale).

Elle a été déclarée contraire à la Constitution par la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015. Le Conseil a en effet estimé que ces dispositions, qui ne prévoyaient ni autorisation ni même information préalable du Premier ministre et de la CNCTR portaient « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* » (1).

Cette procédure n'est donc jamais entrée en vigueur. Son inexistence, au demeurant, n'a jamais été mentionnée, au cours des travaux de la mission d'information, comme devant susciter une évolution juridique.

D. L'ENCADREMENT DES DURÉES D'AUTORISATION ET DE CONSERVATION

1. Les durées d'autorisation

Aux termes de l'article L. 821-4 du CSI, la durée de droit commun de l'autorisation de mise en œuvre d'une technique de renseignement délivrée par le Premier ministre est de **quatre mois (2).**

Il existe néanmoins un certain nombre de techniques – plus intrusives – pour lesquelles l'autorisation est abaissée à **deux mois** : *IMSI-catcher*, sonorisation et fixation d'image, captation de données informatiques. S'agissant de l'algorithme, la première autorisation de mise en œuvre est délivrée pour une durée de deux mois. Les renouvellements sont ensuite autorisés pour quatre mois maximum.

Pour les techniques les plus attentatoires à la vie privée, les délais d'autorisation sont encore plus courts :

– 30 jours pour le recueil de données informatiques et l'introduction dans un lieu privé ;

– 48 heures s'agissant de l'utilisation de l'*IMSI-catcher* pour intercepter des correspondances.

S'agissant des mesures de surveillance des communications internationales, l'exploitation non individualisée de données de connexion est autorisée pour une durée maximale d'un an.

---

(1) Conseil constitutionnel, décision n° 2015–713 DC du 23 juillet 2015, Loi relative au renseignement, *cons. 29.*

(2) Voir annexe n° 7.

2. Les durées de conservation des données

a. Les règles générales

Aux termes de l'article L. 822-2 du CSI, les durées de conservation des données à compter de leur recueil sont les suivantes (1) :

– 30 jours pour les interceptions de sécurité et pour les paroles captées ;

– 120 jours pour les fixations d'image, le recueil des données informatiques et la captation de données informatiques ;

– 4 ans pour les données de connexion.

b. Les dérogations

Certaines dérogations à ces durées sont prévues :

– la durée maximale est de six ans à compter du recueil pour les **renseignements chiffrés** ;

– les renseignements collectés qui contiennent des éléments de **cyberattaque** ou qui sont chiffrés ne font pas l'objet d'une limitation de durée. Néanmoins, de strictes garanties sont prévues, ces renseignements sont conservés dans une mesure strictement nécessaire aux besoins de l'analyse technique et à l'exclusion de toute utilisation pour la surveillance des personnes concernées (2) ;

– les renseignements qui concernent une requête dont le Conseil d'État a été saisi ne peuvent pas être détruits mais ils sont conservés pour les seuls besoins de la procédure ;

– les données désanonymisées de l'algorithme sont exploitées dans un délai de 60 jours et sont détruites, passé ce délai, sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste attachée à l'une ou plusieurs des personnes concernées ;

– les données recueillies par le biais des *IMSI-catchers* sont conservées dans les conditions de droit commun si elles se rapportent à l'autorisation de mise en œuvre. Elles ne sont conservées que 90 jours si elles ne s'y rapportent pas ;

– les renseignements collectés sur l'hertzien ouvert sont détruits à l'issue d'une durée de 6 ans à compter de leur recueil, 8 ans s'ils sont chiffrés.

Les renseignements collectés en application de la surveillance des communications internationales sont détruits à l'issue d'une durée de :

---

(1) Voir annexe n° 7.

(2) Cette dérogation concerne aussi bien les données issues de renseignements collectés sur le territoire national que celles issues de la surveillance des communications internationales.

– 6 mois à compter de leur recueil pour les correspondances renvoyant à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national ;

– 12 mois à compter de leur première exploitation pour les correspondances, dans la limite de quatre ans à compter de leur recueil ;

– 6 ans à compter de leur recueil pour les données de connexion ;

– 8 ans à compter de leur recueil pour les renseignements chiffrés.

c. Quelques incohérences

Lors des auditions menées par les membres de la mission d'information, la critique la plus récurrente portée au cadre juridique actuel a été celle de la différence de traitement en matière de durée de conservation entre les images et le son. Les images peuvent être conservées 120 jours alors que les paroles ne peuvent l'être que 30 jours. Cela aboutit à des situations inopportunes où une même vidéo ne peut plus être exploitée après 30 jours que sans le son.

La durée de 30 jours est calquée sur celle des interceptions de sécurité, mais il paraîtrait logique d'harmoniser, à la hausse, cette durée s'agissant de la sonorisation avec celle de la fixation d'image.

Au demeurant, la CNCTR, dans son rapport annuel de 2018, avait également pointé cette incohérence et plaidé pour une harmonisation, sans toutefois exprimer de préférence pour la durée à retenir [(1)].

II. L'APPROPRIATION DU CADRE JURIDIQUE PAR LES ACTEURS DU RENSEIGNEMENT

Si la loi du 24 juillet 2015 n'a pas eu d'impact direct sur la structuration de la communauté du renseignement (**A**), elle a néanmoins consacré la distinction entre les services spécialisés du renseignement du premier cercle et ceux du second cercle. Surtout, elle a nécessité une véritable acculturation des services au nouveau cadre légal (**B**) et à la doctrine de la CNCTR (**C**).

L'expérience a montré que cette assimilation est désormais très largement acquise et que les services sont attachés à l'architecture de la loi du 24 juillet 2015 modifiée, qui a amplement contribué à sécuriser leur action et à renforcer la protection à laquelle ils ont droit.

(1) CNCTR, rapport annuel 2018, p. 43.

A. LA STRUCTURATION DE LA COMMUNAUTÉ DU RENSEIGNEMENT

1. Une approche par l'autorisation de recourir aux techniques de renseignement qui s'est imposée

La loi du 24 juillet 2015 n'a pas eu d'impact sur la structuration de la communauté du renseignement, qui relève essentiellement du domaine réglementaire – il n'appartient pas à la loi de définir quels sont les services spécialisés de renseignement. C'est la raison pour laquelle l'article L. 811-2 du CSI renvoie cette liste à un décret en Conseil d'État. Cette appartenance ou non à la catégorie des « services spécialisés » a toutefois un impact dans la mesure où ce sont ces services qui peuvent avoir accès, pour le seul exercice de leurs missions, aux techniques de renseignement.

a. Les services du premier cercle : six services clairement identifiés

Aux termes du décret du 28 septembre 2015 (1) – codifié à l'article R. 811-1 du CSI – les services spécialisés de renseignement sont :

– **la direction générale de la sécurité extérieure (DGSE)**, qui relève du ministère des armées;

– **la direction du renseignement et de la sécurité de la défense (DRSD)**, qui relève du ministère des armées;

– **la direction du renseignement militaire (DRM)**, qui relève du ministère des armées;

– **la direction générale de la sécurité intérieure (DGSI)**, qui relève du ministère de l'intérieur ;

– le service à compétence nationale dénommé « **direction nationale du renseignement et des enquêtes douanières » (DNDRED)**, qui relève du ministère de l'économie et des finances ;

– le service à compétence nationale dénommé « **traitement du renseignement et action contre les circuits financiers clandestins » (TRACFIN)**, qui relève du ministère de l'économie et des finances.

Textes réglementaires relatifs aux services spécialisés de renseignement

– DGSI : décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure ;

– DGSE : articles D. 3126-1 à D. 3126-4 du code de la défense ;

– DRSD : articles D. 3126-5 à D. 3126-9 du code de la défense ;

(1) Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement.

– DRM : articles D. 3126-10 à D. 3126-14 du code de la défense ;

– DNRED : arrêté du 29 octobre 2007 portant création d'un service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » ;

– TRACFIN : articles R. 561-33 à R. 561-37 du code monétaire et financier.

À l'exception de la DRM et de TRACFIN, ces services ont vocation à accéder à l'ensemble des techniques de renseignement prévues par le livre VIII du code de la sécurité intérieure (1).

b. Les services du second cercle : un ensemble très hétérogène

La loi du 24 juillet 2015 a également prévu que certains autres services, communément appelés services du « second cercle », peuvent recourir aux techniques de renseignement (article L. 811-4 du CSI). Ils sont désignés par décret en Conseil d'État, pris après avis de la CNCTR. Ce décret précise, pour chaque service, les finalités et les techniques qui peuvent donner lieu à autorisation.

L'article R. 811-4 du CSI établit la liste de ces services (2), reproduite ci-dessous :

(1) CNCTR, rapport d'activité 2016, p. 32.

(2) Décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure.

Direction générale	Direction	Service	Finalité
Direction générale de la police nationale (Ministère de l'Intérieur)	Direction centrale de la police judiciaire	Service central des courses et jeux	Prévention de la criminalité et de la délinquance organisées
		Office anti–stupéfiants	
		Sous-direction de la lutte contre la criminalité organisée	
		Sous-direction de la lutte contre la criminalité financière	
		Sous-direction anti–terroriste	Prévention du terrorisme
		Sous-direction de la lutte contre la cyber–criminalité	Prévention du terrorisme Prévention de la criminalité et de la délinquance organisées
		Directions interrégionales et régionales de police judiciaire, services régionaux de police judiciaire et antennes de PJ	
	Direction centrale de la police aux frontières	Unités chargées de la PJ au sein des directions déconcentrées de la police aux frontières et des directions de la police aux frontières d'Orly et de Roissy	Prévention de la criminalité et de la délinquance organisées
		Brigades mobiles de recherche zonale	
		Office central pour la répression de l'immigration irrégulière et de l'emploi des étrangers sans titre	
		Unité judiciaire du service national de la police ferroviaire	
	Direction centrale de la sécurité publique	Service du renseignement territorial	Indépendance nationale Prévention du terrorisme Prévention : a) Des atteintes à la forme républicaine des institutions b) Des actions tendant au maintien ou à la reconstitution de groupements dissous c) Des violences collectives de nature à porter gravement atteinte à la paix publique Prévention de la criminalité et de la délinquance organisées
		Sûretés départementales	Prévention de la criminalité et de la délinquance organisées
Direction générale de la gendarmerie nationale (Ministère de l'Intérieur)	Direction des opérations et de l'emploi	Sous-direction de l'anticipation opérationnelle	Indépendance nationale Prévention du terrorisme Prévention : a) Des atteintes à la forme républicaine des institutions b) Des actions tendant au maintien ou à la reconstitution de groupements dissous c) Des violences collectives de nature à porter gravement atteinte à la paix publique
		Sous-direction de la PJ	Indépendance nationale, Prévention du terrorisme Prévention de la criminalité et de la délinquance organisées
		Sections de recherche	Prévention du terrorisme Prévention de la criminalité et de la délinquance organisées
Préfecture de	Direction du	Sous– direction de la sécurité intérieure	Indépendance nationale, Prévention du

police (Ministère de l'Intérieur)	renseignement	Sous-direction du renseignement territorial	terrorisme Prévention : a) Des atteintes à la forme républicaine des institutions b) Des actions tendant au maintien ou à la reconstitution de groupements dissous c) Des violences collectives de nature à porter gravement atteinte à la paix publique Prévention de la criminalité et de la délinquance organisées
	Direction régionale de la PJ	Sous-direction des brigades centrales	Prévention du terrorisme Prévention de la criminalité et de la délinquance organisées
		Sous-direction des affaires économiques et financières	Prévention de la criminalité et de la délinquance organisées
		Sous-direction des services territoriaux	Prévention du terrorisme Prévention de la criminalité et de la délinquance organisées
	Direction de la sécurité de proximité de l'agglomération de Paris	Sûretés territoriales	Prévention de la criminalité et de la délinquance organisées
		Sous-direction spécialisée dans la lutte contre l'immigration irrégulière	
Ministère de la Défense		Section de recherche de la gendarmerie maritime	Indépendance nationale, Prévention du terrorisme Prévention de la criminalité et de la délinquance organisées
		Section de recherche de la gendarmerie de l'air	
		Section de recherche de la gendarmerie de l'armement	
Ministère de la justice	Directeur de l'administration pénitentiaire	Service national du renseignement pénitentiaire	Prévention du terrorisme Prévention : a) Des atteintes à la forme républicaine des institutions b) Des actions tendant au maintien ou à la reconstitution de groupements dissous c) Des violences collectives de nature à porter gravement atteinte à la paix publique Prévention de la criminalité et de la délinquance organisées + finalités spécifiques

On relèvera que **l'activité de quatre de ces services est exclusivement ou essentiellement consacrée au renseignement** : c'est le cas du service central du renseignement territorial (SCRT) (au sein de la direction générale de la police nationale), de la sous-direction de l'anticipation opérationnelle (SDAO) (au sein de la direction générale de la gendarmerie nationale), de la direction du renseignement (DRPP) (au sein de la préfecture de police de Paris) ainsi que du service national du renseignement pénitentiaire (SNRP) (au sein du ministère de la justice). Les autres services n'ont pas cette caractéristique, de sorte que le paysage du « second cercle » apparaît très hétérogène [(1)].

(1) Ce qui ne signifie pas qu'il serait inutile qu'ils puissent recourir à des techniques de renseignement dans le cadre de la loi de 2015. Ainsi, un service de police judiciaire a indiqué à votre mission d'information que « la phase proactive de recueil et d'exploitation du renseignement criminel, menée en amont de la phase judiciaire, s'avère bien souvent déterminante pour les enquêtes ».

Les finalités pouvant être invoquées par ces services du second cercle sont principalement :

–la prévention de la criminalité et de la délinquance organisées (24 services) ;

– la prévention du terrorisme (15 services) ;

– l'indépendance nationale, l'intégrité du territoire et la défense nationale (8 services).

c. La question du positionnement des quatre services de renseignement du second cercle

La question du positionnement du SCRT, du SNRP, de la DRPP et du SDAO, qui concourent à titre principal à des activités de renseignement, a été évoquée devant les membres de la mission d'information.

M. Olivier Forcade a montré l'ancienneté de ce débat : « *Les tenants d'une " communauté restreinte " ont fait valoir que seuls les services spécialisés dans le renseignement fermé devaient être inclus : si la gendarmerie fait du renseignement, celui-ci ne serait pas systématiquement collecté selon un plan de recherche et ne procéderait pas essentiellement des opérations secrètes. Quant à la DRPP, elle consacrait alors bien un quart de ses moyens humains au renseignement, mais assumait des missions de sécurité plus larges qui n'englobent pas nécessairement le renseignement. En 2019, pour ne pas être d'actualité, le débat n'est pas totalement refermé quant à l'évolution éventuelle du périmètre de la communauté française du renseignement opérant une distinction entre les services relevant tantôt du " premier ", tantôt du " second " cercle de la communauté, face à des enjeux de sécurité intérieure*. » (1)

Les membres de la mission n'estiment ni opportun ni nécessaire, à ce stade, de préconiser une évolution du périmètre, qui distinguerait explicitement trois cercles au sein de la communauté du renseignement, ou qui reverrait la ligne de partage entre les premier et second cercles. Même s'il est parfois tentant de dessiner un jardin à la française, cette catégorisation nouvelle n'aurait pas de valeur ajoutée opérationnelle certaine, alors même qu'elle susciterait des interrogations dont l'opportunité n'est pas démontrée. Au demeurant, cette question ne relève pas du domaine de la loi et il est souhaitable que le pouvoir exécutif conserve la responsabilité de la définition organique et fonctionnelle des services, puisqu'il a seul la charge d'en assurer la direction opérationnelle.

---

(1) In Retour historique sur les institutions et les pratiques du renseignement français de 1991 à 2015, Le droit du renseignement*, L'Académie du renseignement, Olivier Forcade, p. 26.*

2. La création et la montée en puissance du renseignement pénitentiaire

a. L'intégration de l'administration pénitentiaire parmi les services de renseignement du second cercle

Créé en 2003 à l'initiative de M. Dominique Perben, alors garde des Sceaux, le bureau du renseignement pénitentiaire, initialement dénommé « EMS 3 » avait pour mission de surveiller les détenus difficiles puis, à partir de 2005, de sécuriser les établissements et prévenir les évasions ou mutineries. Ses compétences se sont étendues, en 2015, à la surveillance, « *en liaison avec les autres services compétents de l'État* (…) [de] *l'évolution de certaines formes de criminalité et de radicalisation violente* » (1).

Dès avant les attentats de 2015, dans un avis présenté en octobre 2014 à la commission des Lois (2), le président de votre mission d'information avait plaidé pour *« faire du renseignement pénitentiaire un acteur à part entière de la communauté du renseignemen*t. » La loi de 2015 n'avait malheureusement pas permis de régler ce problème : si un amendement du président de votre mission d'information tendant à créer un service de renseignement pénitentiaire avait été voté en première lecture par l'Assemblée nationale (avec l'avis favorable du rapporteur Jean-Jacques Urvoas et malgré l'avis défavorable de la garde des sceaux Christiane Taubira (3), il n'avait pu prospérer.

Il a fallu attendre la loi du 3 juin 2016 précitée pour renforcer les moyens juridiques à la disposition de l'administration pénitentiaire afin de la doter de capacités de renseignement utiles et efficaces, à des fins administratives et judiciaires : l'article L. 811-4 du code de la sécurité intérieure, sur les services du second cercle, a été amendé pour qu'il puisse concerner des services relevant du ministre de la justice, cette modification ayant pour objet d'autoriser l'administration pénitentiaire à utiliser certaines techniques du renseignement, pour autant que le décret en Conseil d'État le prévoie. C'est le décret n° 2017-36 du 16 janvier 2017, pris sur le rapport du garde des sceaux Jean-Jacques Urvoas, qui a fait naître ce service de renseignement.

Par un arrêté du 29 mai 2019, la garde des sceaux, ministre de la justice a décidé la création d'un service à compétence nationale dénommé « service national du renseignement pénitentiaire » en remplacement du bureau central du renseignement pénitentiaire (4) .

---

(1) Arrêté du 30 juin 2015 fixant l'organisation en bureaux de la direction de l'administration pénitentiaire.

(2) http://www.assemblee-nationale.fr/14/budget/plf2015/a2267-tVI.asp

(3) http://www.assemblee-nationale.fr/14/cri/2014-2015/20150214.asp#P513494

(4) Arrêté du 29 mai 2019 portant création et organisation d'un service à compétence nationale dénommé « Service national du renseignement pénitentiaire ».

b. La création de finalités spécifiques

Deux lois – la loi du 28 février 2017 (1) et la loi du 23 mars 2019 (2) – sont venues renforcer le corpus législatif applicable au renseignement pénitentiaire. Elles ont étendu la mise en œuvre de techniques de renseignement à vocation administrative par l'administration pénitentiaire pour deux finalités :

– la prévention des évasions ;

– la sécurité des établissements pénitentiaires ou des établissements de santé destinés à recevoir des détenus.

Par exception par rapport aux autres services de renseignement, spécialisés ou non, les techniques de renseignement qui peuvent être mises en œuvre par le service national du renseignement pénitentiaire pour ces finalités sont énumérées par l'article L. 855-1 du CSI. Il s'agit des accès aux données de connexion en temps différé, de la géolocalisation en temps réel, du balisage, des *IMSI-catchers*, des interceptions de correspondances (sans usage des *IMSI-catchers*), des écoutes hertziennes, de la sonorisation de lieux et de la fixation d'image, de l'introduction dans un lieu privé.

Les écoutes hertziennes, la captation de paroles prononcées à titre privé, la captation d'images dans un lieu privé et l'introduction dans un lieu privé sont soumises à un contingentement. Chacun de ces trois contingents a été fixé à 20 par une décision du Premier ministre en date du 17 juillet 2019 (3) .

La coexistence de deux régimes juridiques distincts pour la prévention des évasions et le maintien de la sécurité et du bon ordre des établissements pénitentiaires

L'article 727-1 du code de procédure pénale prévoit qu'aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues, le ministre de la justice peut autoriser les agents individuellement désignés et habilités de l'administration pénitentiaire à :

1° Intercepter, enregistrer, transcrire ou interrompre les correspondances de personnes détenues émises par la voie des communications électroniques et autorisées en détention, à l'exception de celles avec leur avocat, et conserver les données de connexion y afférentes ;

2° Accéder aux données stockées dans un équipement terminal ou un système informatique qu'utilise une personne détenue et dont l'utilisation est autorisée en détention, les enregistrer, les conserver et les transmettre.

Les personnes détenues ainsi que leurs correspondants sont informés au préalable des dispositions du présent article.

(1) Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique.

(2) Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

(3) CNCTR, rapport d'activité 2019, p. 37.

L'autorisation est délivrée pour une durée maximale d'un an, renouvelable.

Comme l'a noté la CNCTR, la coexistence de ces deux cadres juridiques s'explique par la différence de nature entre les mesures de surveillance qu'ils régissent. Les techniques prévues à l'article L. 855-1 du code de la sécurité intérieure constituent des moyens de recueillir des renseignements à l'insu des personnes concernées. Aussi sont-elles entourées de toutes les garanties que ce caractère secret rend nécessaires pour s'assurer du respect de la légalité. Les mesures prévues à l'article 727-1 du code de procédure pénale, en revanche, sont mises en œuvre après information des personnes détenues, soit que celles-ci aient été averties que leurs communications licites pourraient être écoutées, soit qu'elles aient reçu notification que les données stockées dans des matériels informatiques illicites ayant été saisis seraient collectées par l'administration pénitentiaire. (1)

Depuis la loi du 23 mars 2019, l'utilisation des techniques de renseignement n'est plus limitée aux seules personnes détenues (2).

Plusieurs garanties destinées à assurer la proportionnalité de ce dispositif ont été apportées, à l'initiative de la présidente de la commission des Lois, Mme Yaël Braun–Pivet (3) :

– la mise en œuvre des techniques de sonorisation ou de captation d'images dans des lieux privés est restreinte aux seules personnes détenues dont il existe des raisons sérieuses de penser que leur comportement constitue une menace d'une particulière gravité pour la sécurité au sein des établissements ;

– aucune technique ne peut être mise en œuvre à l'occasion des communications ou des entretiens entre une personne détenue et son avocat ;

– le nombre de sonorisations ou captations d'images, d'écoutes hertziennes et de dispositifs d'introduction dans des véhicules ou des lieux privés susceptibles d'être mis en œuvre simultanément est contingenté par le Premier ministre ;

– l'usage de ces techniques est soumis au droit commun de la mise en œuvre des techniques de renseignement, en particulier l'exigence d'un avis préalable de la CNCTR.

Le Conseil constitutionnel a jugé conforme à la Constitution les dispositions issues de la loi du 23 mars 2019, estimant que le « *législateur a[vait] assorti les dispositions contestées de garanties propres à assurer une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée, l'inviolabilité du domicile et le secret des correspondances*. » (4)

---

(1) CNCTR, rapport d'activité 2018, p. 32.

(2) Mais seules les personnes détenues peuvent faire l'objet des techniques de captation d'images ou de paroles dans un lieu privé.

(3) Amendement n° 1132.

(4) Décision n° 2019-778 DC du 21 mars 2019, cons.347.

B. L'APPLICATION DU CADRE LÉGAL DE 2015 : UN DÉFI ET UNE CHANCE POUR LES SERVICES DE RENSEIGNEMENT

1. Un cadre juridique qui protège l'action des agents des services de renseignement

La loi du 24 juillet 2015 est aujourd'hui vécue comme un réel atout par les services de renseignement, qui ont tous insisté sur le changement de paradigme que son adoption avait entraîné. Elle a considérablement sécurisé l'action des agents des services de renseignement.

En effet, l'absence d'un corpus juridique encadrant l'activité des services de renseignement exposait la France à méconnaître les stipulations de la Convention européenne de sauvegarde des droits et libertés fondamentales (CEDH). Déjà, la loi de 1991 relative aux interceptions de sécurité avait répondu à la condamnation de la France par l'arrêt *Kruslin* (1) pour non-respect de l'article 8 de la CEDH sur le droit au respect de la vie privée et familiale, appliquant à notre pays la jurisprudence que la Cour avait déjà énoncée depuis la fin des années 1970, s'agissant du champ des atteintes portées au respect de la vie privée en matière d'écoutes téléphoniques, à l'occasion des arrêts *Klass* (2) et *Malone* (3).

Ce cadre juridique morcelé, composé de « rustines » empiriquement posées (4) pour reprendre l'expression du rapporteur du projet de loi relatif au renseignement, constituait également un risque pour les fonctionnaires de ces services qui, hors les techniques reconnues par la loi, étaient dans une situation qui les exposaient.

Comme le soulignait l'ancien président de la commission des Lois, Jean-Jacques Urvoas « *ces services ne doivent pas être considérés comme " spéciaux " ou " secrets ". Certes la presse les qualifie souvent ainsi sans doute parce qu'ils perdent en précision ce qu'ils gagnent en capacité à susciter immédiatement un certain mystère. Mais la direction générale de la sécurité extérieure (DGSE) ou la direction générale de la sécurité intérieure (DGSI) ne sont pas des institutions secrètes : les sites internet de leurs ministères respectifs leur dédient des espaces, leurs directeurs généraux publient parfois des entrevues ou des tribunes. Les services ne sont pas plus spéciaux, sauf peut-être en raison d'un rattachement fonctionnel à l'autorité politique quelque peu original lié à une architecture*

---

(1) CEDH, Kruslin contre France, 24 avril 1990, cf. deuxième partie du rapport.

(2) CEDH, Klass et autres c. Allemagne, 6 septembre 1978.

(3) CEDH, Malone c. Royaume-Uni, 26 avril 1985.

(4) Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques ; loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers ; 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 ; loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme ; loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

découlant de la dyarchie de l'exécutif que l'on doit à la Constitution de la Ve République.

Par contre, à rebours de toute logique, ils continuent d'inscrire leurs activités dans un environnement " para-légal ", " extra-légal " voire " a-légal " (selon les points de vue) qui n'apporte pas de garanties suffisantes pour les citoyens comme les agents des services spécialisés. Vivant au rythme des crises qu'ils suscitent ou subissent, les services qui lui sont dédiés travaillent au profit de la République, mais dans les limbes du droit et des exigences démocratiques. Et, alors qu'il compte parmi les plus anciennes des nations démocratiques, notre pays est également le dernier à ne pas avoir établi un cadre normatif adapté. » (1)

La loi du 24 juillet 2015 en encadrant l'usage d'un certain nombre de techniques, a donc sécurisé l'action des agents de service de renseignement.

En outre, la protection des agents a été renforcée par différentes dispositions de la loi du 24 juillet 2015 :

– anonymat des agents (article L. 861-1 du CSI) ;

– excuse pénale s'agissant de l'usage d'une identité d'emprunt ou d'une fausse qualité (article L. 861-2), des relations avec des personnes susceptibles de porter atteinte aux intérêts fondamentaux de la Nation, de l'extraction de contenus provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie (article L. 863-1) ;

– statut de lanceur d'alerte pour un agent qui a connaissance, dans l'exercice de ses fonctions, de faits susceptibles de constituer une violation manifeste de la loi (article L. 861-3) ;

– procédure particulière s'agissant des actes commis hors du territoire national (article L. 862-1). À l'initiative de M. Philippe Nauche, rapporteur pour avis de la commission de la défense de l'Assemblée nationale, les dispositions de l'article 698-1 du code de procédure pénale, qui impose au procureur de la République de solliciter préalablement un avis du ministre de la défense avant de poursuivre pénalement un militaire, ont été étendues aux personnels civils des services de renseignement ;

– protection juridique des agents qui bénéficient de l'irresponsabilité pénale s'agissant des actes prescrits ou autorisés par des dispositions législatives ou réglementaires (article L. 862-2).

Les différentes auditions menées par les membres de la mission d'information ont permis de faire ressortir que les directeurs de services se félicitaient, de manière générale, des améliorations qu'avait entraînées pour leurs agents l'adoption de la loi du 24 juillet 2015.

---

(1) Assemblée nationale, XIVe législature, rapport n° 2697, p. 16

Un regret a été évoqué lors d'une audition : l'article L. 861-2 subordonne, s'agissant des services du second cercle, le recours à une identité d'emprunt à la publication d'un arrêté du Premier ministre qui n'a jamais été pris. Or, l'anonymisation des déplacements en province des agents devant effectuer des techniques de renseignement, notamment en ce qui concerne les réservations d'hôtels, est largement perfectible.

2. Un changement majeur pour les services de renseignement qui doivent consacrer des moyens humains et techniques à son respect

Tous les services de renseignement qui ont été auditionnés par les membres de la mission d'information ont eu l'occasion de rappeler le changement culturel qu'avait représenté la loi du 24 juillet 2015.

Ce passage de l'ombre à la lumière, même tamisée, a nécessité une réorganisation en profondeur des services pour s'assurer du respect du nouveau cadre légal. Cette culture juridique nouvelle a aujourd'hui « irrigué » les services. Une mobilisation des ressources humaines a été conduite : des personnels ont été spécialisés sur les sujets procéduraux et, de manière générale, les personnels des services de renseignement ont été formés à ces questions. La DGSE estime ainsi que 10 % du temps des agents est alloué à la constitution des dossiers. En outre, des moyens administratifs ont été mis en œuvre de manière à assurer le bon contrôle par la CNCTR. Dans les grands services, il y a entre six et huit niveaux hiérarchiques entre l'enquêteur et l'autorité qui prend la décision.

Mais comme l'a indiqué M. Nicolas Lerner, directeur général de la sécurité intérieure, « *c'est le prix de la sécurisation* » des procédures d'autorisation.

Les membres de la mission d'information ont entendu les contraintes objectives engendrées par la mise en œuvre de la loi relative au renseignement, mais ils soulignent que **jamais cette contrainte n'a été présentée de manière négative.** Tous les services ont souligné l'immense apport de la loi relative au renseignement dans l'exercice quotidien de leurs missions. Comme l'a rappelé le coordonnateur national du renseignement lors de son audition, « *il faut garder à l'esprit que le respect du cadre légal et réglementaire est très coûteux en temps et en ressources humaines mais que si c'est le prix à payer pour rassurer les concitoyens, les services le supportent volontiers car cela leur offre une grande sécurité dans la mise en œuvre des techniques de renseignement*. »

C. LA MISE EN ŒUVRE D'UN DIALOGUE DE QUALITÉ AVEC LA CNCTR

1. La mise en œuvre d'un dialogue avec l'autorité administrative de contrôle

La procédure d'autorisation de mise en œuvre de techniques de renseignement est précisément décrite aux articles L. 821-1 et suivants du code de

la sécurité intérieure (voir *supra*). Si cette procédure fonctionne de manière aussi fluide, de l'avis unanime des acteurs auditionnés par les membres de la mission d'information, c'est grâce à la mise en œuvre d'un dialogue riche, exigeant et de qualité entre les services de renseignement et l'autorité de contrôle.

La CNCTR se voit comme **un tiers de confiance entre les services de renseignement, leur tutelle et le public**.

Le président de la CNCTR, M. Francis Delon, a explicité les différentes manières par lesquelles la commission s'efforce d'être prévisible et d'aider les services et leur autorité de tutelle à déterminer ce qu'ils sont autorisés à faire :

– les **demandes complémentaires** : « *si la motivation* [d'une demande] *parait insuffisante,* [la CNCTR] *peut demander des renseignements complémentaires par tous moyens, y compris par l'audition de représentants du service dans des cas complexes » ;*

– la **motivation des avis** : *« la commission ne se borne pas à donner un avis favorable ou défavorable. Elle assortit souvent ses avis favorables d'observations et de restrictions qui peuvent tenir à la durée de mise en œuvre de la technique, plus courte que celle demandée par le service, voire aux conditions de cette mise en œuvre s'il s'agit d'une technique très intrusive. Elle pourra s'assurer, dans le cadre de l'exercice de son contrôle* a posteriori, *que ces conditions ont effectivement été respectées par le service. Elle motive ses avis défavorables pour permettre au service demandeur d'être informé du raisonnement suivi par la commission et d'en tenir compte pour ses demandes futures » ;*

– l'**élaboration d'une doctrine** *: « à travers ses avis, la commission forge sa doctrine et veille à la porter à la connaissance des services de renseignement, de leurs ministres de tutelle et du Premier ministre*. » (1)

La CNCTR dispose de 24 heures pour se prononcer ou de 72 heures lorsqu'elle doit se prononcer en formation collégiale. Ces délais légaux sont respectés et, au-delà même des délais prévus par la loi, les services de renseignement ont des besoins opérationnels dont la CNCTR sait tenir compte en pratique. Cela la conduit à prendre des décisions dans des délais bien inférieurs à 24 heures. Le format du dialogue s'adapte aux circonstances, de sorte à pouvoir traiter les demandes en quelques heures si c'est nécessaire.

En 2019, la CNCTR a adressé 1 732 demandes de renseignements complémentaires aux services, soit pour environ 2 % des demandes de techniques de renseignement soumises pour avis (2).

---

(1) In La commission nationale de contrôle des techniques de renseignement, Le droit du renseignement, *L'Académie du renseignement, Francis Delon, p. 129.*

(2) CNCTR, rapport d'activité 2019, p. 63.

Depuis 2017, chaque service de renseignement est plus particulièrement suivi par deux ou trois référents attitrés parmi les agents du secrétariat général de la CNCTR. Le rôle de ces référents est de faciliter le dialogue quotidien avec les services afin de prévenir les irrégularités (1) .

2. Un dialogue qui porte ses fruits : la diminution du taux de refus de demandes de techniques de renseignement

L'un des critères qui permet de mesurer la qualité du dialogue établi entre les services de renseignement et la CNCTR est la nette diminution au fil des ans du taux de refus opposé aux demandes de mise en œuvre d'une technique de recueil de renseignement. Il était de 6,9 % la première année, ce qui était important au regard de la pratique de la CNCIS qui émettait moins d'1 % d'avis défavorables. Ce taux est retombé à 3,6 % en 2017, à 2,1 % en 2018 et il est 1,4 % 2019.

De l'avis de la CNCTR, ce recul est imputable au fait que les services de renseignement se conforment mieux à la doctrine de la CNCTR, en présentant des demandes mieux proportionnées aux finalités justifiant le recours aux techniques de renseignement, et « *renoncent à présenter des demandes vouées à la désapprobation de* [la CNCTR] » (2). Dans le même temps, **le nombre de demandes augmente régulièrement. Cela signifie que les services se sont bien adaptés au cadre légal sans pour autant s'autocensurer.**

La CNCTR a en outre rendu, en 2019, 78 avis défavorables sur les demandes d'accès aux données de connexion en temps différé, soit environ 0,2 % du nombre d'avis rendus sur des demandes concernant cette technique. Ce taux était de 0,1 % en 2018.

De manière générale, le président de la CNCTR, lors de son audition par les membres de la mission d'information, a indiqué ne pas avoir décelé de volonté des services de renseignement de contourner la loi, simplement des erreurs et des incompréhensions.

Depuis l'entrée en vigueur de la loi du 24 juillet 2015, le Premier ministre n'a jamais accordé une autorisation après un avis défavorable de la CNCTR (3).

III. DES CONTRÔLES NOMBREUX ET EXIGEANTS

La loi du 24 juillet 2015, en légitimant la politique publique du renseignement, s'est traduite par un renforcement de ses moyens techniques et

(1) CNCTR, op. cit., p. 72.

(2) CNCTR, rapport d'activité 2018, p. 8.

(3) CNCTR, rapport d'activité 2019, p. 53.

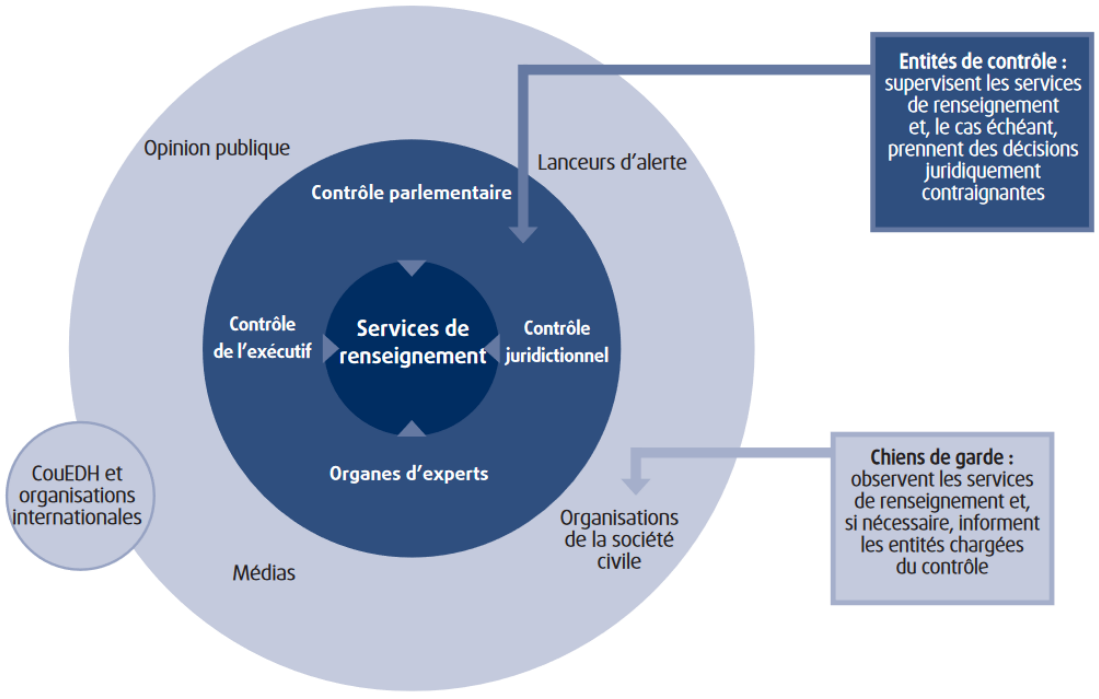
juridiques, renforcement qui s'est accompagné d'une forte logique de contrôle (1), tant interne (**A**) qu'externe (**B**).

En effet, comme l'indiquait récemment le secrétaire d'État auprès du ministère de l'intérieur et ancien directeur de la DGSI, M. Laurent Nuñez, *« **la discrétion comme la clandestinité n'excluent pas la traçabilité et la légalité. C'est même tout le contraire.** (…) Pour respecter une déontologie, un droit, on a besoin du regard d'autrui. Cela revient à considérer que celles et ceux qui exercent leur métier dans la discrétion voire le secret ont besoin d'un cadre juridique et parfois de regards extérieurs.* » (2)

Progressivement, plusieurs niveaux de contrôle, internes et externes, se sont mis en place de manière à vérifier le respect du cadre légal, avec chacun leur légitimité et leur angle d'approche. Les formes du contrôle peuvent porter sur l'efficacité des organismes, y compris dans l'affectation des ressources, ou encore sur la conformité des activités de renseignement avec la loi, voire sur leur régularité déontologique.

SCHÉMA DES RESPONSABILITÉS DANS LE DOMAINE DU RENSEIGNEMENT

Figure 2 : Schémas des responsabilités au sein des services de renseignement



Source : FRA, 2017

Source : Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'UE, office des publications de l'UE, 2017, p. 4

---

(1) In Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement, Le droit du renseignement, *L'Académie du renseignement, Bertrand Warusfel, p. 67.*

(2) In Allocution d'ouverture, Le droit du renseignement, *L'Académie du renseignement, Laurent Nuñez, p. 14.*

A. L'EXISTENCE DE PLUSIEURS NIVEAUX DE CONTRÔLE INTERNE

Les services de renseignement, comme les autres administrations, doivent veiller à l'efficacité de leur action. Toutefois, en raison de la nature particulière des missions qu'ils exercent, il est malaisé de recourir à des avis extérieurs, sous forme d'audits par exemple, afin de déceler des sources éventuelles de dysfonctionnements. Aussi, **la nécessité d'un contrôle interne s'impose-t-elle avec une particulière acuité,** dans la mesure où, par hypothèse, une défaillance pourrait mettre en péril la sécurité de nos concitoyens ou méconnaître l'exigence de respect des libertés.

Le contrôle interne présente une double déclinaison. La première forme consiste en un **contrôle interne exécutif,** mis en œuvre par le Gouvernement afin de s'assurer du bon fonctionnement et de l'efficacité des services placés sous son autorité. La seconde forme correspond au **contrôle interne administratif** exercé par les chefs de service afin de vérifier la régularité des pratiques mises en œuvre et d'impulser des réformes si nécessaire.

1. L'autorisation par le Premier ministre

Aux termes de l'article L. 821-4 du CSI, l'autorisation de mise en œuvre d'une technique de renseignement est délivrée par le Premier ministre. Sur ce point, la loi du 24 juillet 2015 a repris le mécanisme qui existait pour les interceptions de sécurité depuis 1991 (1).

Le simple fait de devoir requérir la signature du Premier ministre réduit *ipso facto* le risque d'une autonomisation opérationnelle des services de renseignement. La technique de renseignement sollicitée ne pourra être en effet autorisée sans que la hiérarchie du service concerné mais aussi le cabinet de son ministre de tutelle et, enfin, celui du Premier ministre aient été sollicités et aient avalisé son emploi (2).

Toutes les techniques de renseignement doivent recevoir l'aval du Premier ministre, puisque même en cas d'urgence absolue, c'est bien le chef du Gouvernement qui délivre l'autorisation – sans avis préalable de la CNCTR. La procédure de l'urgence opérationnelle, qui passait outre ce contrôle hiérarchique, a en effet été censurée par le Conseil constitutionnel (3).

Le Premier ministre peut également demander des précisions, solliciter un complément de motivation, ou ajouter une restriction ou une condition dans la décision d'autorisation.

---

(1) Article 4 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

(2) In Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement, Le droit du renseignement, *L'Académie du renseignement, Bertrand Warusfel, p. 67.*

(3) Conseil constitutionnel, décision n° 2015–713 DC du 23 juillet 2015, Loi relative au renseignement, *cons. 29.*

En outre, un certain nombre de techniques de renseignement font l'objet d'un arrêté de **contingentement** du Premier ministre, pris après avis de la CNCTR [(1)].

En pratique, c'est le préfet, conseiller pour les affaires intérieures au cabinet du Premier ministre, qui signe la plupart des décisions, à l'exception de quelques-unes d'entre elles qui remontent jusqu'à son directeur de cabinet [(2)] .

Cette centralisation, au plus haut niveau du Gouvernement, présente plusieurs avantages, parmi lesquels celui de **pouvoir détecter d'éventuels doublons** et de vérifier la réalité effective de la coopération interservices sur des thématiques communes ou connexes. Lorsque des doublons sont détectés et qu'ils ne constituent pas des cas isolés, parfois sur signalement du GIC ou de la CNCTR, des mécanismes de déconfliction [(3)] ou de renforcement de la coopération interservices peuvent être décidés, en lien avec les cabinets des ministres concernés et du coordonnateur national du renseignement et de la lutte contre le terrorisme [(4)].

Les liens entre le Premier ministre et la CNCTR sont très étroits. Comme l'a indiqué le préfet Renaud Vedel, qui fut conseiller pour les affaires intérieures au cabinet du Premier ministre, « *des réunions fréquentes, quasi hebdomadaires, se tiennent entre le cabinet du Premier ministre et le président de la CNCTR ou ses collaborateurs les plus proches. Elles sont l'occasion d'évoquer en particulier les dossiers difficiles, ainsi que les projets d'organisation technique pouvant impacter la chaîne de contrôle*. » [(5)]

Comme indiqué précédemment, le Premier ministre n'a jamais autorisé une technique de renseignement après avis défavorable de la CNCTR. S'il n'est pas en situation de compétence liée, il apparaît que le Premier ministre fait le choix de se conformer à l'avis de la CNCTR, tout en conservant la faculté de s'en écarter, ainsi que la loi a entendu le permettre. Au plan juridique comme au plan politique, la mission estime qu'il y a là un équilibre qu'il convient de préserver.

2. La centralisation par le groupement interministériel de contrôle (GIC) : une garantie essentielle

La loi du 24 juillet 2015 a appliqué le principe de centralisation à toutes les techniques de renseignement. L'article L. 822–1 du code de la sécurité intérieure dispose que le Premier ministre définit les modalités de la centralisation

---

(1) Accès administratif aux données de connexion en temps réel (article L. 851–2 du CSI), IMSI–catcher *(article L. 851–6), interceptions de sécurité (article L. 852–1), exploitation des mesures de surveillance internationale (article L. 854–2).*

(2) Arrêté du 19 juin 2017 portant délégation de signature.

(3) Résolution des conflits.

(4) In Les contrôles internes, Le droit du renseignement, *L'Académie du renseignement, Renaud Vedel, p. 150.*

(5) Ibid.

des renseignements collectés. Plusieurs autres dispositions du livre III du CSI mentionnent ensuite cette centralisation par un service du Premier ministre (1).

Ces dispositions sont cruciales : « *sans centralisation, aucun contrôle n'est possible en pratique* », comme l'a résumé l'un des interlocuteurs de la mission.

Le principal organe de cette centralisation est **le groupement interministériel de contrôle (GIC)**. Le cœur de ce service a été créé il y a une cinquante ans, par une décision du Premier ministre Michel Debré, en date du 28 mars 1960, afin d'exécuter, pour le compte des services de renseignement, les interceptions téléphoniques administratives. Désormais, il assume cinq missions :

– **il réceptionne les demandes de techniques de renseignement issues des services de renseignement du premier cercle et du second cercle**, par l'entremise de leur ministre de rattachement. Il les soumet à l'avis de la CNCTR, puis à l'autorisation du Premier ministre ;

– **il recueille les données auprès des opérateurs de communications électroniques et des fournisseurs de services sur internet**. Il dispose à cette fin d'un pouvoir de réquisition qui lui est exclusivement réservé. Comme l'a indiqué à la mission un observateur, « *cette intermédiation proscrit toute relation de travail habituelle entre les agents de renseignement et ceux des opérateurs, limite les possibilités de connaissances interpersonnelles et d'habitudes de fréquentation et, par conséquent limite les vulnérabilités potentielles en matière d'actes non tracés qui sortiraient du cadre légal*. » ;

– **il centralise l'exploitation des données recueillies** auprès des opérateurs de communications électroniques et des fournisseurs de services sur internet : les correspondances sont exploitées par les services bénéficiaires au sein du GIC ;

– **il centralise l'exécution des techniques de proximité** : le GIC conduit un programme de centralisation des données recueillies directement par les services à proximité de leurs objectifs afin de garantir l'effectivité du contrôle de la mise en œuvre de ces techniques ;

– **il centralise le traitement des recours contentieux** devant la formation spécialisée du Conseil d'État en matière de techniques de renseignement.

Le GIC dispose aussi d'un département du contrôle en mesure d'effectuer des vérifications.

La loi de 2015 a étendu le champ du renseignement à **des techniques de renseignement dont, par nature, l'exécution est matériellement déconcentrée**.

---

(1) Il s'agit des articles L. 851–1 s'agissant des accès administratifs aux données de connexion, L. 851–4 s'agissant de la géolocalisation en temps réel des équipements terminaux, L. 851–6 s'agissant des IMSI-catchers*, l'article L. 852–1 s'agissant des interceptions de sécurité.*

Leur exécution concrète suppose souvent la survenance d'une opportunité rare, pas toujours prévisible : il en va ainsi de la pose d'une balise sur un véhicule ou d'un dispositif de captation directe, par exemple à l'occasion d'une opération de filature. Dans ces cas-là, ce sont les agents habilités du service de renseignement qui déclenchent opérationnellement la mise en œuvre de la technique de renseignement concernée (1).

Cette atténuation ne signifie pas pour autant absence de contrôle pour ces techniques. Une information immédiate sur l'activation de la mesure doit alors être transmise au GIC et à la CNCTR. En outre, les données collectées doivent faire l'objet d'une centralisation et d'un versement dans des systèmes d'information choisis, développés ou imposés par le GIC.

À cette fin de centralisation et de contrôle, le **GIC tient un registre exhaustif des demandes et des autorisations**, ainsi que des dates d'activation et de désactivation effective des moyens techniques correspondants. Il développe des systèmes d'information et de traçabilité dont l'usage est imposé aux services de renseignement. Pour réaliser leurs surveillances et, souvent, en exploiter le contenu, du moins avant l'extraction des données pertinentes et vérifiées comme correspondant aux finalités définies par l'autorisation, les agents ont l'obligation d'utiliser ces outils. Il s'agit là d'un moyen matériel de contrôle très puissant.

Des échanges nourris ont animé le débat parlementaire en 2015 sur la question de savoir si une **centralisation totale était opportune et nécessaire**. Le Premier ministre Manuel Valls avait indiqué : « *Il faut prendre garde à la vulnérabilité très forte que constituerait la centralisation du produit de l'ensemble du renseignement collecté en un point unique, y compris vis-à-vis de services étrangers*. » (2) Par conséquent, la centralisation recouvre en fait deux dimensions : la dimension géographique – lieux où sont stockées les données – et la dimension juridique – organe chargé de la centralisation. Une centralisation géographique en un lieu unique paraît inappropriée ; la centralisation juridique ayant progressé depuis 2015, il paraîtrait opportun d'inscrire ces avancées dans le marbre de la loi (3).

3. L'inspection des services de renseignement

La création d'une inspection des services de renseignement était l'une des recommandations de la mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement menée en mai 2013 par la commission des Lois de notre assemblée (4).

---

(1) In Les contrôles internes, Le droit du renseignement, *L'Académie du renseignement, Renaud Vedel, p. 150.*

(2) http://www.assemblee-nationale.fr/14/cri/2014-2015/20150212.asp#P511111

(3) Voir troisième partie.

(4) Assemblée nationale, XIVe législature, rapport d'information n° 1022 de MM. Jean–Jacques Urvoas et Patrice Verchère, pp. 54 et 55.

Elle fut mentionnée par la loi du 18 décembre 2013 précitée [1], à l'article 6 *nonies* de l'ordonnance de 1958 relative au fonctionnement des assemblées parlementaires. Son décret de création date du 24 juillet 2014 [2], soit un an avant la loi du 24 juillet 2015.

L'inspection des services de renseignement réalise, sur demande du Premier ministre, des missions de différentes natures – contrôle, audit, étude, conseil et évaluation. Une partie des premiers travaux de cette inspection ont porté sur les conditions concrètes de mise en œuvre de la loi du 24 juillet 2015 [3].

La loi du 24 juillet 2015 n'a pas modifié la structure de l'inspection, qui relève du domaine réglementaire. Son périmètre a été étendu par un décret [4] en date du 19 septembre 2018, qui a intégré l'inspection des services judiciaires, tirant les conséquences de la création d'un service de renseignement pénitentiaire à la suite de la loi de 2016 précitée.

Par conséquent, l'inspection des services de renseignement procède aujourd'hui de **six inspections générales ministérielles**, au sein desquelles plusieurs membres habilités au « très secret-défense » sont désignés par le Premier ministre comme membres de l'inspection des services de renseignement, comme le précise le décret précité :

« *Les membres de l'inspection des services de renseignement sont désignés par le Premier ministre, après avis du coordonnateur national du renseignement et de la lutte contre le terrorisme :*

1° Sur proposition des ministres chargés de la défense, de la sécurité intérieure, de la justice, de l'économie ou du budget, parmi les membres habilités à connaître des informations et supports classifiés au niveau Très Secret-Défense du ***contrôle général des armées****, de* ***l'inspection générale de l'administration****, de* ***l'inspection générale de la justice****, de* ***l'inspection générale des finances*** *et du* ***conseil général de l'économie, de l'industrie, de l'énergie et des technologies****, en activité dans leur corps ou leur service. Ces propositions sont établies après avis des chefs de ces mêmes corps ou services ;*

2° Sur proposition du ministre de la défense, parmi les ***inspecteurs généraux des armées*** *habilités à connaître des informations et supports classifiés au niveau Très Secret-Défense.* »

---

(1) Article 12 de 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.

(2) Décret n° 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement.

(3) In Les contrôles internes, Le droit du renseignement, *L'Académie du renseignement, Renaud Vedel, pp. 157–158.*

(4) Décret n° 2018-798 du 19 septembre 2018 ajoutant l'inspection générale de la justice aux corps et services d'inspection et de contrôle concourant au fonctionnement de l'inspection des services de renseignement.

Ce dispositif vise à diversifier le vivier des compétences des inspecteurs. La permanence et la possibilité d'une programmation de longue durée sont permises par la désignation d'un secrétaire général de l'inspection.

La loi de 2015 a prévu, en outre, une articulation des contrôles de l'inspection avec celui de la CNCTR : la CNCTR a la faculté de solliciter du Premier ministre tout ou partie des rapports de l'inspection des services de renseignement (1).

4. Le contrôle interne aux services de renseignement

Toutes les demandes de mise en œuvre d'une technique de recueil de renseignement doivent être sollicitées auprès du ministre de tutelle du service de renseignement concerné (2). Il existe donc au sein de chacun des ministères, un contrôle interne, relativement méconnu, mais très puissant. Le préfet Renaud Vedel a bien montré le fonctionnement du contrôle interne, qui repose sur une dialectique *« entre la **formalisation précise du besoin opérationnel**, la mise en jeu de la responsabilité de la chaîne hiérarchique purement administrative dans la conformité légale de la surveillance et **l'engagement de la responsabilité de l'autorité politique ministérielle** dans le processus de décision* » (3).

Ainsi, lorsqu'un chef de service de renseignement ou son suppléant qui a reçu délégation de signature signe une demande de technique de renseignement sur une personne d'intérêt, il certifie que cette demande s'inscrit dans le cadre de la loi. Il s'agit de la première des trois signatures d'autorités qui figurent sur l'acte d'autorisation (avec celle du ministre ou de son délégué, et celle du Premier ministre ou de son délégué), en plus de l'avis de la CNCTR.

En outre, la plupart des services de renseignement ont mis en place des cellules de conformité spécialisées en charge de la vérification et de la révision de toutes les demandes de technique de renseignement (4). Habilitées à reformuler, restreindre ou refuser la demande, elles peuvent interagir directement avec l'agent demandeur pour mieux évaluer la nécessité opérationnelle de la demande.

Enfin, le contrôle interne s'exerce par le biais des inspections internes des services. Comme l'a indiqué M. Renaud Vedel, elles « *sont notamment très sourcilleu*[ses] *de la traçabilité interne des responsabilités et l'adéquation des systèmes d'information dans les processus de proposition et de cheminement des surveillances.* » (5)

---

(1) Article 2 de la loi du 24 juillet 2015 précitée.

(2) À l'exception des demandes d'identification de numéros ou d'abonnements, qui sont quasiment considérées comme un préalable à la mise en œuvre d'une technique de renseignement.

(3) In Les contrôles internes, Le droit du renseignement, L'Académie du renseignement, *Renaud Vedel, p. 149.*

(4) Ibid.

(5) Ibid.

5. Un mécanisme de lanceur d'alerte qui n'a encore jamais trouvé à s'appliquer

Les révélations d'Edward Snowden, ancien agent de la CIA et consultant de la NSA progressivement rendues publiques à partir de juin 2013 sur la surveillance mondiale d'internet, mais aussi des téléphones portables et autres moyens de communications, ont eu un énorme impact. Elles ont jeté un trouble durable sur l'ampleur réelle de l'action des services de renseignement.

Il paraissait nécessaire, si des agissements contraires à la loi devaient être constatés par un agent, que ce dernier puisse saisir les autorités compétentes, sans avoir à en subir de conséquences dommageables.

À l'initiative de M. Jean–Jacques Urvoas, la loi du 24 juillet 2015 a donc prévu un mécanisme de « lanceur d'alerte » au bénéfice des agents des services qui estiment que des violations manifestes des dispositions du livre VIII du code de la sécurité intérieure seraient commises au sein du service de renseignement où ils sont affectés.

La procédure établie à l'article L. 861-3 du même code prévoit que l'**agent porte les faits en cause à la connaissance de la seule CNCTR**, qui peut alors saisir le Conseil d'État et en aviser le Premier ministre.

En parallèle, **si la CNCTR estime que les faits rapportés sont constitutifs d'une infraction, elle en avise le procureur de la République** et transmet les documents à la Commission consultative du secret de la défense nationale (CCSDN) afin que celle-ci donne son avis au Premier ministre sur la déclassification de ceux-ci en vue de leur transmission au procureur de la République.

Le **dispositif protège l'agent ayant témoigné de bonne foi** à la CNCTR, en prévoyant qu'aucune sanction, aussi bien disciplinaire que statutaire, ne peut être prise à son égard. Ainsi, la rupture du contrat de travail décidée à la suite de cette dénonciation serait nulle de plein droit. L'administration doit en outre prouver que les mesures statutaires ou les sanctions disciplinaires prises à l'égard d'un agent qui aurait par ailleurs signalé à la CNCTR des faits dans le cadre de ce dispositif sont sans lien avec la dénonciation en la justifiant par des « *éléments objectifs étrangers à la déclaration ou au témoignage de l'agent intéressé* ».

En revanche, les agents qui auraient dénoncé de « *mauvaise foi* » ou « *avec l'intention de nuire* » des faits en réalité inexacts seraient passibles des sanctions prévues au premier alinéa de l'article 226-10 du code pénal, c'est-à-dire des dispositions réprimant la dénonciation calomnieuse.

Ce cadre juridique permettant aux agents des services de dénoncer des pratiques qu'ils estiment illégales, tout en préservant le secret de la défense nationale, est nécessaire. À la connaissance de la mission, **aucune procédure n'a encore été enclenchée sur cette base.**

B. LA MONTÉE EN PUISSANCE DES ORGANES DE CONTRÔLE EXTERNE

Le **contrôle externe de légalité** et de proportionnalité consiste à s'assurer que les demandes déposées par les administrations spécialisées respectent les conditions prévues par la loi et ne portent pas une atteinte disproportionnée aux droits et libertés des citoyens.

Le **contrôle externe de responsabilité** est quant à lui exercé par les parlementaires, qui contrôlent non les services de renseignement eux-mêmes mais leur utilisation par le pouvoir exécutif, conformément à la position exprimée par le Conseil constitutionnel dans sa décision n° 2001-456 DC du 27 décembre 2001. Cette conception suppose néanmoins que les autres formes de contrôle fonctionnent efficacement.

1. La Commission nationale de contrôle des techniques de renseignement (CNCTR)

● L'organisation et les missions de la CNCTR

La première autorité administrative indépendante chargée de contrôler la mise en œuvre d'une technique de renseignement a été créée par l'article 13 de la loi du 10 juillet 1991 précitée. Il s'agissait de la CNCIS, compétente à l'origine uniquement en matière d'interceptions administratives de correspondances. Elle a ensuite vu sa compétence élargie à l'accès administratif aux données de connexion en temps différé (1) et à la géolocalisation en temps réel (2).

L'instauration d'un contrôle externe des écoutes téléphoniques

Comme l'a rappelé la CNCTR dans son premier rapport d'activité, l'instauration d'un contrôle externe de l'activité des services de renseignement avait été lente et limitée (3).

La loi n° 70–643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens inscrivit le droit au respect de la vie privée à l'article 9 du code civil. Les débats précédant l'adoption de cette loi furent l'occasion pour le Parlement de soulever la question de l'existence, de la légitimité de l'encadrement juridique possible des écoutes téléphoniques, qu'elles soient judiciaires ou administratives.

En 1981, le Premier ministre confia au premier président de la Cour de cassation la direction d'une commission d'études chargée de conduire des investigations sur les écoutes téléphoniques, tant judiciaires qu'administratives. Le rapport remis en 1982 recommanda notamment de légiférer afin de concilier les nécessités de l'ordre public et le respect des libertés fondamentales. Cette recommandation ne fut pas davantage suivie d'effet.

Par deux arrêts n° 11105/84 et n° 11801/85 du 24 avril 1990 (affaires *Huvig et Kruslin* c. France), relatifs au régime français des écoutes judiciaires, la Cour européenne des

(1) Article 6 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

(2) Article 20 de 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.

(3) CNCTR, rapport d'activité 2016, pp. 15 et 16.

droits de l'homme condamna la France pour violation de l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, qui protège le droit de toute personne au respect de sa vie privée.

C'est dans ce contexte qu'a été élaborée la loi du 10 juillet 1991 précitée, qui a notamment créé la CNCIS, chargée de veiller au respect des dispositions légales relatives à l'autorisation et à la réalisation des mesures d'interception.

L'article 2 de la loi du 24 juillet 2015 a créé la CNCTR, une nouvelle autorité administrative indépendante, aux missions et pouvoirs étendus par rapport à la CNCIS. Elle a été mise en place le 3 octobre 2015.

La composition de la CNCTR

La CNCTR est composée de neuf membres (1) :

– deux députés et deux sénateurs, désignés de manière à assurer une représentation pluraliste du Parlement ;

– deux membres du Conseil d'État ;

– deux magistrats de la Cour de cassation ;

– une personnalité qualifiée pour sa connaissance en matière de communications électroniques.

Le président de la commission est nommé par décret du président de la République parmi les membres du Conseil d'État et de la Cour de cassation.

Comme le notait le rapport sur le projet de loi relatif au renseignement, le triplement du nombre de membres par rapport à la composition de la CNCIS était motivé par la nécessité de renforcer la capacité d'action de la CNCTR par rapport à celle de la CNCIS étant donné l'élargissement de ses pouvoirs et de lui donner ainsi les moyens d'être un contrepoids efficace au Gouvernement dans l'utilisation des techniques de renseignement (2). De plus, la nomination d'une personnalité qualifiée pour sa connaissance en matière de communications électroniques s'inscrivait dans une certaine filiation de la recommandation n° 41 du Conseil d'État, dans son rapport intitulé « Le numérique et les droits fondamentaux », qui préconisait notamment « *de faire de la CNCIS une autorité de contrôle des services de renseignement dotée 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* ». (3)

(1) La composition de la CNCTR est actuellement la suivante : Francis Delon, Catherine Di Folco, Michel Boutant, Constance Le Grip, Jean–Michel Clément, Martine Jodeau, Gérard Poirotte, Christine Pénichon, Patrick Puges.

(2) Assemblée nationale, XIV^e^ législature, rapport n° 2697 de Jean–Jacques Urvoas sur le projet de loi relatif au renseignement, p. 115.

(3) Rapport public du Conseil d'État, étude annuelle 2014, Le numérique et les droits fondamentaux, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541/0000.pdf

À la fin de l'année 2019, le secrétariat général de la CNCTR se composait d'un secrétaire général, d'un conseiller placé auprès du président de la commission, de 11 chargés de mission et de 4 agents exerçant des missions de soutien (1) .

La CNCTR est chargée d'apprécier la légalité de la mise en œuvre des techniques de renseignement sur le territoire national au regard de l'atteinte portée à la vie privée des personnes concernées. Cette appréciation comprend une double dimension, en amont et en aval de l'autorisation par le Premier ministre :

– toutes les demandes de mise en œuvre d'une technique de renseignement (2) font l'objet d'un **avis de la commission**, qui est ensuite communiqué au Premier ministre (article L. 821-3) ;

– la commission exerce un **contrôle sur les opérations de collecte, de transcription et d'extraction** des renseignements afin de s'assurer du respect des finalités ayant justifié l'autorisation de mise en œuvre de la technique de renseignement (article L. 822-3). De même, elle exerce son contrôle **sur les opérations de destruction** des renseignements collectés (article L. 822-4).

En cas de découverte d'une irrégularité dans la mise en œuvre d'une technique ou lorsque cette mise en œuvre ne paraît plus justifiée au regard des prescriptions légales qui l'ont fondée, la commission peut recommander d'interrompre la technique, voire de détruire les informations déjà collectées (article L. 833-6).

Pour le président de la CNCTR, le contrôle de la légalité *a priori* « *inclut un contrôle de proportionnalité entre l'atteinte à la vie privée qui résulterait de la mise en œuvre de la technique de renseignement sollicitée et la gravité des menaces ou le caractère fondamental des enjeux invoqués par le service de renseignement pour justifier sa demande. Plus la technique sollicitée est intrusive, plus le service devra, pour convaincre la commission, étayer la réalité et l'importance des menaces auxquelles il veut parer. De surcroît, pour les techniques les plus intrusives qui impliquent l'introduction dans un lieu privé, la commission vérifie, à travers l'exercice d'un contrôle de subsidiarité, que les renseignements recherchés ne pourraient être efficacement collectés par d'autres moyens légaux moins attentatoires à la vie privée et au secret des correspondances*. » (3)

● Les contrôles *a posteriori* exercés par la CNCTR ont montré un respect général des obligations légales malgré plusieurs irrégularités

Depuis son installation, en octobre 2015, la CNCTR n'a cessé d'intensifier son contrôle *a posteriori*. Celui-ci s'exerce sur pièces et sur place, plusieurs fois

(1) CNCTR, rapport d'activité 2019, p. 13.

(2) À l'exception des mesures de surveillance sur l'hertzien ouvert, prévues aux articles L. 855–1 A à C.

(3) In La Commission nationale de contrôle des techniques de renseignement, Le droit du renseignement, *L'Académie du renseignement, Francis Delon, p.125 et 129.*

par semaine, au sein des services de renseignement. Ainsi, en 2019, la CNCTR a réalisé une centaine de contrôles sur pièces et sur place [1] , contre 120 en 2018 [2], 130 en 2017 et 60 en 2016 [3]. Le contrôle est également réalisé en ligne depuis les locaux sécurisés de la commission.

En 2019, la CNCTR a constaté que les **services respectent les obligations légales qui leur incombent** mais elle a relevé certaines irrégularités. La plupart d'entre elles ont été signalées aux services concernés au cours des contrôles et rapidement corrigées par ceux-ci.

Les trois catégories d'irrégularités observées en 2019

Les irrégularités les plus couramment observées par la CNCTR et qui ont été corrigées sans formalisation d'une recommandation écrite par la commission se répartissent en trois catégories :

– la première catégorie est liée au **dépassement de la durée légale de conservation** des données brutes recueillies dans la mise en œuvre de mesures de surveillance (huit cas) ou des transcriptions et des extractions. Dans un cas, la CNCTR a constaté que de telles transcriptions ou extractions étaient indûment conservées dans la mesure où leur lien avec la finalité poursuivie était contestable ;

– la deuxième catégorie a trait au **dépassement de la durée d'autorisation de la mesure de surveillance**. La CNCTR en a fait le constat à trois reprises. Dans tous les cas, le dépassement était de très courte durée.

– la troisième catégorie d'irrégularités est liée aux « fiches de traçabilité », c'est-à-dire aux relevés de mise en œuvre, des modalités effectives de réalisation de chaque technique autorisée. Des divergences entre les modalités de mise en œuvre d'une surveillance, indiquées par le service dans sa demande d'autorisation, et celles effectivement employées, ont été constatées dans un dossier. Le service a été invité à en expliquer les raisons qui se sont révélées être d'ordre opérationnel. Dans un autre, les discordances concernaient le matériel précisément utilisé pour exercer la surveillance. Le service a été prié de s'expliquer sur ce qui s'est révélé être une erreur matérielle et de rectifier la fiche de traçabilité.

Dans deux cas, la CNCTR a choisi de saisir formellement le service par un courrier lui recommandant certaines mesures correctrices [4], en application des dispositions de l'article L. 833-6 du code de la sécurité intérieure, que la mise en œuvre d'une technique soit immédiatement interrompue et que les renseignements collectés ainsi que les extractions et transcriptions effectuées soient détruits.

(1) CNCTR, rapport d'activité 2019, p. 67.

(2) CNCTR, rapport d'activité 2018, p. 75.

(3) CNCTR, rapport d'activité 2017, p. 6.

(4) CNCTR, rapport d'activité 2019, p. 68.

Ces deux cas, relevant de deux services différents, concernaient la surveillance de personnes exerçant une profession ou un mandat protégés en application des dispositions de l'article L. 821-7 du code de la sécurité intérieure.

Dans les deux cas, la CNCTR s'est aperçue, à l'occasion de l'instruction de demandes de renouvellement de techniques de renseignement, que la cible exerçait une profession ou un mandat protégés. L'exercice de ces professions ou mandats, ignoré par le service lors de la première demande d'autorisation de surveillance, avait par la suite été révélé par cette surveillance.

La CNCTR a estimé que la surveillance sollicitée ne pouvait être détachée de l'exercice du mandat ou de la profession et elle a, en conséquence, émis un avis défavorable au renouvellement des techniques sollicitées. Elle a, en outre, adressé aux chefs des services demandeurs, à leur ministre de tutelle ainsi qu'au Premier ministre, des recommandations d'interruption immédiate des surveillances en cours et de destruction de tous les renseignements recueillis ainsi que de toutes les transcriptions et extractions éventuellement réalisées. La CNCTR s'est assurée que ces recommandations avaient été intégralement mises en œuvre.

La CNCTR peut saisir le Conseil d'État d'un recours si le Premier ministre ne donne pas suite à ses avis ou recommandations ou que les suites qui y sont données sont estimées insuffisantes. Cette situation ne s'est jamais produite.

La mission considère que la CNCTR remplit l'office qui lui a été fixé par la loi – étant entendu que, comme son nom l'indique, il lui appartient de contrôler « les techniques de renseignement » et non pas les activités de renseignement. En particulier, elle n'est pas chargée d'un contrôle sur l'opportunité de recourir à une technique de renseignement, qui reste du ressort de l'exécutif. La mission ne préconise pas d'évolution du périmètre des missions de la CNCTR.

2. La montée en puissance du contrôle parlementaire

a. La délégation parlementaire au renseignement

● Une institution récente

Le contrôle parlementaire des services de renseignement a longtemps été un « *serpent de mer* » (1) qui s'est nourri de la contradiction entre l'existence du « secret-défense » et l'aspiration de la représentation nationale à pouvoir appliquer l'article 15 de la Déclaration des droits de l'homme et du citoyen : « *la société a le droit de demander compte à tout agent public de son administration.* »

Comme le rappelait la présidente de la commission des Lois, Mme Yaël Braun–Pivet dans un colloque organisé par l'Académie du renseignement, « *la*

(1) Roger Faligot, Jean Guisnel, Rémi Kauffer, Histoire politique des services secrets français, *La Découverte, Paris, 2012, p. 651.*

mise en œuvre d'un contrôle parlementaire du renseignement en France est relativement récente au regard des grandes démocraties qui nous entourent. Alors que les premiers organes parlementaires dédiés au contrôle de la politique publique du renseignement ont été mis en place dès le début des années 1950 aux Pays-Bas et en Allemagne, l'association du Parlement français est nettement plus tardive. » (1)

De 1971 à 2005, ce ne sont pas moins d'une vingtaine d'initiatives parlementaires de création d'un organe de contrôle des services de renseignement qui ont été déposées, sans succès, au Parlement.

M. Nicolas Sarkozy, alors ministre d'État, ministre de l'intérieur, avait souhaité qu'un organe parlementaire chargé de contrôler le renseignement puisse être créé dans le cadre de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme. Il déclarait ainsi à la commission des Lois que : *« « L'idée de constituer une commission parlementaire chargée de contrôler le renseignement apparaît parfaitement normale dans une démocratie moderne. (…) Reste à en mettre au point les modalités, dans un domaine éminemment sensible. Il faut espérer que la sagesse des parlementaires les incitera à ne pas aller trop loin, sous peine de braquer immédiatement les services concernés. Mais on ne peut pas ne pas admettre le principe d'un contrôle parlementaire des activités de renseignement, qui du reste est la norme dans toutes les démocraties. La France ne saurait faire encore longtemps figure d'exception. (…) Il serait du reste souhaitable que les chefs des services de renseignements, tout comme le chef de la police ou des grandes administrations, puissent s'exprimer publiquement. Ce n'est malheureusement pas la tradition dans notre pays. »* (2)

Un projet de loi fut déposé en mars 2006 à l'Assemblée nationale, mais ne put être inscrit à l'ordre du jour du Parlement lors de la présidence de M. Jacques Chirac. Ce n'est qu'après l'élection présidentielle de 2007 que ce projet put enfin aboutir, en débouchant sur l'adoption de **la loi du 9 octobre 2007 créant la délégation parlementaire au renseignement (DPR)** (3).

● Une composition et un fonctionnement originaux

La DPR est une instance commune à l'Assemblée nationale et au Sénat, composée de huit membres : les quatre présidents des commissions des Lois et de la Défense des deux chambres et quatre parlementaires, dont deux d'opposition (4). Ce caractère commun aux deux chambres est une spécificité puisque seul l'office

(1) In « Dix ans de contrôle parlementaire du renseignement : l'exigence démocratique est-elle satisfaite ?», Le droit du renseignement, *L'Académie du renseignement, Yaël Braun-Pivet, p. 139.*

(2) http://www.assemblee-nationale.fr/14/cri/2014-2015/20150212.asp#P511111

(3) Loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

(4) La composition actuelle de la DPR est la suivante : M. Christian Cambon (Président), Mme Françoise Dumas, M. François-Noël Buffet, M. Loïc Kervran, M. Patrice Verchère, M. Michel Boutant, M. Philippe Bas, Mme Yaël Braun-Pivet.

parlementaire d'évaluation des choix scientifiques et technologiques fonctionne sur le même modèle.

La fonction de président de la délégation est assurée alternativement, pour un an, par un député et un sénateur, membres de droit.

La DPR, qui est liée par le secret de la défense nationale, tient ses réunions à huis clos et ne fait aucune publicité de ses activités, ce qui ne doit pas masquer la réalité du travail effectué. Elle contribue à enrichir le débat public sur le renseignement, à travers le rapport annuel qu'elle publie et les communications qu'elle fait.

● Le périmètre du contrôle de la DPR a évolué au fil du temps

Comme l'a noté M. Olivier Forcade, initialement, *« les groupes parlementaires souhaitèrent* (…) *l'établissement d'un contrôle parlementaire sur le renseignement qui ne soit pas intrusif, attentif à la place éminente de l'exécutif en matière de défense et sécurité* ». (1)

Si, à l'origine, la DPR avait des prérogatives limitées au « *suivi* » des activités de renseignement (2), la loi de programmation militaire du 18 décembre 2013 lui a reconnu une mission de « *contrôle et d'évaluation de l'action du Gouvernement en matière de renseignement* », ce qui a constitué une considérable évolution. (3) .

Le champ des activités susceptibles de faire l'objet d'un contrôle a en outre connu une légère extension. Dorénavant, la DPR peut connaître des activités opérationnelles achevées.

Cette loi a également entraîné l'intégration de la commission de vérification des fonds spéciaux – la CVFS – au sein de la DPR, dont elle est devenue une formation spécialisée. La CVFS, composée de quatre des huit membres de la DPR, est l'unique instance chargée du contrôle externe des fonds spéciaux qui répondent à des règles de gestion dérogatoire du droit commun.

---

(1) In « Retour historique sur les institutions et les pratiques du renseignement français de 1991 à 2015 », Le droit du renseignement, *L'Académie du renseignement, Olivier Forcade, pp. 24 à 26.*

(2) Le rapporteur du projet de loi, Bernard Carayon, avait ainsi expliqué que : « Le terme de " contrôle " n'est volontairement pas utilisé dans le projet de loi, celui-ci ayant une connotation trop intrusive. Cette absence pourra être critiquée, mais elle est probablement nécessaire pour permettre la mise en place progressive de l'indispensable climat de confiance mutuelle *», rapport fait au nom de la Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi (n° 13), adopté par le Sénat, portant création d'une délégation parlementaire au renseignement, p. 26.*

(3) 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.

La commission de vérification des fonds spéciaux

Les « fonds secrets » ont longtemps été un attribut de la souveraineté de l'État. Pourtant, comme l'ont rappelé Jacques Buisson et Xavier Cabannes (1), chaque assemblée, sous la Restauration et la Monarchie de Juillet, créait une commission spéciale composée de deux membres auxquels il incombait de réaliser le contrôle de ces masses financières. Lors de l'examen du budget, l'un des deux parlementaires se présentait à la tribune et déclarait sur l'honneur que leur usage avait été convenable.

Le décret n° 47-2234 du 19 novembre 1947 instaura une commission de vérification de l'usage de ces fonds par le SDECE (service de documentation extérieure et de contre-espionnage).

Cet organe fonctionna avec beaucoup de discrétion jusqu'en 2001 et des débats nés lors de la cohabitation entre M. Jacques Chirac et M. Lionel Jospin. La loi de finances pour 2002 créa alors un organe nouveau, la CVFS, composée de quatre députés et de deux magistrats de la Cour des comptes, chargés de vérifier la régularité des fonds utilisés non plus seulement par le service de renseignement extérieur, mais par l'ensemble des services de renseignement. Cet organe mixte, composé de parlementaires et de magistrats, n'a jamais fonctionné sous cette forme : dès le départ, le président de la Cour, Philippe Seguin, refusa que ces derniers y siègent.

Le rééquilibrage entre un contrôle parlementaire mesuré et un contrôle exécutif soucieux de l'efficacité immédiate du dispositif national de renseignement ne peut donc être nié (2).

La loi du 24 juillet 2015 a étendu les pouvoirs d'audition de la DPR, afin de lui permettre de recevoir les plus hauts cadres des services de renseignement, sans que le ministre ou le directeur du service puisse s'y opposer.

Elle a également prévu la possibilité pour la DPR d'entendre le Premier ministre sur son application ainsi que les personnes spécialement déléguées par lui pour délivrer les autorisations de mise en œuvre des techniques de renseignement mentionnées par la loi. La Délégation peut également inviter le président de la CNCTR à lui présenter le rapport d'activité de la commission, tout comme le président de la Commission du secret de la défense nationale.

Depuis la loi du 24 juillet 2015, la DPR n'a pas subi d'évolution majeure (3). Comme l'a souligné le dernier rapport d'activité de la DPR, « *les débats parlementaires sur la loi de programmation militaire 2019–2025 n'ont pas*

(1) Jacques Buisson et Xavier Cabannes, « Les fonds spéciaux et le droit public financier », Petites affiches, *3 août 2001, n° 154, p. 15.*

(2) In Retour historique sur les institutions et les pratiques du renseignement français de 1991 à 2015, Le droit du renseignement, *L'Académie du renseignement, Olivier Forcade, p. 32.*

(3) Elle se fait communiquer, depuis 2017, les observations de la CNCTR sur l'application de l'exception hertzienne en application de l'article 16 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

permis de dégager de consensus sur les évolutions à apporter, à ce stade, au cadre juridique actuel » (1).

● **Les missions de la DPR**

Les missions de la DPR sont strictement bornées par l'article 6 *nonies* de l'ordonnance n° 58–1100 du 17 novembre 1958 relative au fonctionnement des Assemblées parlementaires. Elle exerce le **contrôle parlementaire de l'action du Gouvernement en matière de renseignement et évalue la politique publique en ce domaine**.

À cette fin, elle est destinataire des informations utiles à l'accomplissement de sa mission (2). Ces informations ne peuvent porter ni sur les opérations en cours de ces services, ni sur les instructions données par les pouvoirs publics à cet égard, ni sur les procédures et méthodes opérationnelles, ni sur les échanges avec des services étrangers ou avec des organismes internationaux compétents dans le domaine du renseignement.

Ces exclusions résultent de la jurisprudence du Conseil constitutionnel, qui a jugé, dans sa décision n° 2001–456 DC du 27 décembre 2001 à propos de la commission de vérification des fonds spéciaux que « *s'il appartient au Parlement d'autoriser la déclaration de guerre, de voter les crédits nécessaires à la défense nationale et de contrôle l'usage qui en a été fait, il ne saurait en revanche, en la matière, intervenir dans la réalisation d'opération en cours* » (cons. 45).

La délégation peut saisir pour avis la CNCTR.

Comme l'a précisé la délégation par le passé, elle n'est pas un organe de surveillance de l'administration, mais de contrôle de l'exécutif puisqu'en « *cas d'anomalie avérée, les parlementaires membres de la délégation parlementaire au renseignement peuvent alors en imputer la responsabilité au seul Gouvernement et mettre en œuvre les mécanismes prévus par la Constitution en application de la séparation des pouvoirs* » (3).

---

*(1) Délégation parlementaire au renseignement, rapport n° 1869 (XVI*ème *législature) de Mme Yaël Braun–Pivet relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018, avril 2019, p. 19.*

(2) La loi prévoit notamment la communication d'un certain nombre de documents : la stratégie nationale du renseignement, des éléments d'information issus du plan national d'orientation du renseignement, un rapport annuel de synthèse exhaustif des crédits consacrés au renseignement et le rapport annuel d'activité des services des premier et second cercles, à recourir à certaines techniques de renseignement, des éléments d'appréciation relatifs à l'activité générale et à l'organisation des services des premier et second cercles, les observations que la CNCTR adresse au Premier ministre. En outre, elle peut solliciter du Premier ministre la communication de tout ou partie des rapports de l'inspection des services de renseignement ainsi que des rapports des services d'inspection générale des ministères portant sur les services de renseignement qui relèvent de leur compétence.

(3) Délégation parlementaire au renseignement, rapport n° 2482 de M. Jean–Jacques Urvoas relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014, décembre 2014, pp. 13 et 14.

b. Les perspectives d'évolution

Plusieurs perspectives d'évolution de la DPR ont été esquissées, en particulier par le rapport d'activité de la DPR pour l'année 2018 :

– renforcer les moyens humains affectés au secrétariat de la DPR ;

– communiquer à la DPR la liste des rapports des services d'inspection ministériels et interministériels ainsi que des rapports des organes de contrôle interne des services de renseignement ;

– transmettre à la DPR l'actualisation de la stratégie nationale du renseignement et l'intégralité du plan national d'orientation du renseignement (à l'exclusion des informations que le Gouvernement ne souhaiterait pas communiquer).

Surtout, le rapport d'activité indique que « *le besoin de faire évoluer la DPR fait l'unanimité, aussi bien auprès des parlementaires qu'auprès des services de l'exécutif* ». L'une des recommandations du rapport était d'engager un dialogue entre la DPR et le Gouvernement sur le renforcement des pouvoirs du contrôle du Parlement sur le renseignement, dans la perspective de la loi Renseignement de 2020 (1).

La DPR a donc créé en son sein un groupe de travail dédié à la réflexion sur les évolutions de cet organe bicaméral. Les membres de la mission d'information estiment que ce sera sur la base de ce travail que des modifications législatives pourraient être apportées.

3. Le contrôle de la Cour des comptes

La Cour des comptes contrôle les services de renseignement, à l'instar de l'ensemble des administrations de l'État. Cette intervention est relativement récente puisqu'elle fut promue par Pierre Joxe à partir de 1993, alors qu'il occupait la fonction de Premier président (2).

En application de l'article L. 143–1 du code des juridictions financières, les observations et recommandations d'amélioration ou de réforme portant sur la gestion des services font l'objet de communications de la Cour des comptes aux ministres compétents.

Lorsqu'elles ne sont pas classifiées, elles sont – en même temps que les réponses apportées par le pouvoir exécutif – transmises aux commissions des finances. Elles peuvent également être communiquées aux commissions d'enquête de chacune des assemblées parlementaires qui en formulent la demande.

---

(1) Délégation parlementaire au renseignement, rapport n° 1869 de Mme Yaël Braun–Pivet relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018, avril 2019, p. 26.

(2) Assemblée nationale, XIVe législature, rapport d'information n° 1022 de MM. Jean–Jacques Urvoas et Patrice Verchère, p. 59.

4. Le contrôle juridictionnel

a. Une révolution juridique

Comme l'a montré Bertrand Warusfel, « *la vraie révolution juridique en matière de contrôle des pratiques de renseignement réside en réalité dans la nouvelle compétence spéciale donnée à une formation spécialisée du Conseil d'État pour statuer " sur les recours formés contre les décisions relatives à l'autorisation et à la mise en œuvre de ces techniques et ceux portant sur la conservation des renseignements collectés "* » (1).

Avant la loi du 24 juillet 2015, « *dans les rares cas où le juge administratif avait été saisi dans ce domaine, le secret de la défense nationale* (…) *avait systématiquement été invoqué et bloquait l'office du juge, rendant le contrôle juridictionnel théorique et illusoire en la matière* ». C'est ce blocage, que le Conseil d'État avait consacré dans son arrêt Coulon de 1955, que la loi du 24 juillet 2015 a permis de lever.

À l'inverse de ce qui a été fait dans d'autres pays, par exemple le Royaume-Uni, le législateur français n'a pas décidé de créer une juridiction spécialisée autonome mais, à l'inverse, de spécialiser, au sein de la section du contentieux du Conseil d'État, une formation de jugement dite « *formation spécialisée* » qui traite exclusivement de ces sujets (2).

L'article 773-2 du code de justice administrative indique que les membres des formations spécialisées et leur rapporteur public sont habilités ès qualités au secret de la défense nationale et qu'ils sont *« autorisés à connaître de l'ensemble des pièces en possession de la Commission nationale de contrôle des techniques de renseignement ou des services* » (3).

Cela a permis la mise en œuvre d'un véritable contrôle juridictionnel du renseignement et a consacré le début d'une évolution majeure, celle de l'accès du juge au secret. Comme le note Bertrand Warusfel, « *Ce faisant, la France se prépare progressivement à un changement de paradigme, en privilégiant le contrôle par un juge, tiers impartial qui accède au secret, par rapport à une vision stricte du principe du contradictoire qui aboutissait en réalité à ce que les éléments de preuve secrets restent implicites et ne soient jamais officiellement transmis aux juridictions ni discutées entre les parties.* » (4)

---

(1) In Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement, Le droit du renseignement, L'Académie du renseignement, Bertrand Warusfel, pp. 80 à 82.

(2) In Le contrôle juridictionnel : un contrôle précisément défini par le législateur et confié à une formation spécialisée du Conseil d'État, Le droit du renseignement, *L'Académie du renseignement, Emmanuelle Prada–Bordenave, p.133.*

(3) Article 10 de la loi du 24 juillet 2015 précitée.

(4) In « Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement », Le droit du renseignement, *L'Académie du renseignement, Bertrand Warusfel, pp. 80 à 82.*

Cette évolution a, en outre, permis de mettre le droit français en conformité avec la jurisprudence de Strasbourg qui est assez exigeante s'agissant de l'office du juge par rapport aux pièces et aux preuves secrètes (1).

Le Conseil d'État peut donc être saisi de plusieurs types de recours :

– par des personnes souhaitant vérifier qu'aucune **technique de renseignement** n'est ou n'a été mise irrégulièrement en œuvre à leur encontre (article L. 841-1 du CSI) ;

– par des personnes qui veulent faire vérifier qu'elles ne figurent pas irrégulièrement dans des traitements ou parties de **traitements intéressant la sûreté de l'État** (article L. 841-2) (2) ;

– par des personnes souhaitant vérifier qu'elles n'ont pas fait l'objet d'une surveillance irrégulière dans le cadre de l'exploitation de communications ou de données de connexion d'identifiants techniques rattachables au territoire national dont l'utilisateur communique depuis ce territoire (article L. 854-9).

Par ailleurs, la formation spécialisée peut être saisie dans deux autres cas :

– par la CNCTR, si elle estime que le Premier ministre ne donne pas suite à ses avis ou de manière insuffisante (articles L. 841-1 et L. 854-9) ;

– dans le cadre d'une question préjudicielle, toute juridiction ayant à connaître « *d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité d'une ou de plusieurs techniques de recueil de renseignement* » pouvant saisir le Conseil d'État afin que sa formation spécialisée puisse, après examen des données classifiées, se prononcer sur la légalité de la collecte du renseignement (article L. 841-1). Elle doit statuer dans le délai d'un mois.

Les traitements ou parties de traitements automatisés de données à caractère personnel intéressant la sûreté de l'État (article R. 841–2)

1° Décret portant création au profit de la direction générale de la sécurité intérieure d'un traitement automatisé de données à caractère personnel dénommé CRISTINA ;

2° Décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers d'informations nominatives mis en œuvre par la direction générale de la sécurité extérieure ;

3° Décret autorisant la mise en œuvre par la direction du renseignement et de la sécurité de la défense d'un traitement automatisé de données à caractère personnel dénommé SIREX ;

4° Décret autorisant la mise en œuvre par la direction du renseignement militaire d'un traitement automatisé de données à caractère personnel dénommé DOREMI ;

(1) CEDH, 19 septembre 2017, requête no 35289/11.

(2) Voir annexe n° 9.

5° Décret portant création d'un traitement automatisé de données à caractère personnel dénommé FSPRT ;

6° Décret n° 2010-569 du 28 mai 2010 portant création du fichier des personnes recherchées, pour les seules données intéressant la sûreté de l'État mentionnées au 8° du III de l'article 2 de ce décret ;

7° Le 1° de l'article R. 231-3 du code de la sécurité intérieure, pour les seules données mentionnées au 3° de l'article R. 231-8 du même code ;

8° Arrêté relatif à la création d'un système de traitement automatisé de données à caractère personnel dénommé STARTRAC mis en œuvre par le service à compétence nationale TRACFIN, pour les seules données intéressant la sûreté de l'État ;

9° Décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé BCR-DNRED ;

10° Décret portant création d'un traitement automatisé de données à caractère personnel dénommé GESTEREXT ;

11° Décret autorisant la mise en œuvre par la direction du renseignement militaire d'un traitement automatisé de données à caractère personnel dénommé BIOPEX ;

12° Décret autorisant la mise en œuvre par le commandement de la Légion étrangère d'un traitement automatisé de données à caractère personnel dénommé LEGATO ;

13° Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données (ACCReD), pour les seules données intéressant la sûreté de l'État ».

b. L'organisation de la formation spécialisée

La formation spécialisée est composée de cinq membres : le président et quatre membres exerçant les fonctions de rapporteur. Elle siège dans une formation composée de trois juges : le président et deux de ses membres, dont le rapporteur. Deux rapporteurs publics sont affectés auprès d'elle [(1)]. Aucun des membres de la formation n'exerce exclusivement ses fonctions auprès de celle-ci. La formation est assistée d'un greffe spécialisé.

La section ou l'assemblée du contentieux du Conseil d'État peuvent également connaître d'affaires concernant la mise en œuvre de techniques de renseignement ou de fichiers intéressant la sûreté de l'État, dans leur formation ordinaire si la formation spécialisée leur soumet une pure question de droit, dans

(1) Le président est nommé pour une période de 4 ans par arrêté du Premier ministre après avis du garde des sceaux et sur présentation du vice-président du Conseil d'État, après avis du président de la section du contentieux. Son mandat peut être renouvelé une fois, à sa demande, pour une période de 4 ans par arrêté du vice-président du Conseil d'État. Les membres sont, quant à eux, désignés par arrêté du président de la section du contentieux, après avis des présidents adjoints. Les rapporteurs publics sont désignés par arrêté du vice-président, pris sur proposition du président de la section du contentieux après avis du président de la formation spécialisée.

une formation restreinte si l'affaire est renvoyée devant ces formations pour qu'elles statuent. Ces formations n'ont pas été réunies à cette fin, à ce jour.

c. Les spécificités de la procédure devant la formation spécialisée

Le principe du caractère contradictoire de la procédure devant le juge administratif, rappelé à l'article L. 5 du code de justice administrative, a été aménagé pour tenir compte des exigences particulières du secret de la défense nationale.

Aussi les **données couvertes par le secret de la défense nationale ne sont-elles connues que du juge et non des parties requérantes.**

Les administrations défenderesses (1) ainsi que les autorités administratives indépendantes (CNIL et CNCTR), sont tenues de verser au dossier tous les éléments nécessaires au contrôle de la formation. La formation dispose également des actes réglementaires, pour la plupart non publiés, relatifs aux fichiers concernés.

Les administrations et autorités concernées produisent, sous le contrôle de la formation, deux versions de leurs mémoires : une version confidentielle, qui n'est pas communiquée à la partie requérante, et une version non confidentielle, qui est communiquée à cette dernière.

La formation spécialisée tient des audiences à huis clos, sauf exception (par exemple, lorsqu'elle statue sur une question prioritaire de constitutionnalité). Le rapporteur public conclut alors hors la présence des parties, devant la seule formation spécialisée. Ses conclusions ne sont pas communicables, sauf à l'administration après la séance.

Les décisions notifiées aux requérants ne peuvent comporter aucune indication confidentielle et ne doivent révéler ni directement, ni indirectement si le requérant a fait l'objet d'une technique de renseignement ou d'une inscription dans un fichier et, s'il a fait l'objet d'une telle technique ou d'une telle inscription, les informations qu'elle comporte.

C'est uniquement lorsqu'une technique de renseignement a été mise en œuvre dans des conditions qui apparaissent entachées d'illégalité, ou lorsqu'un fichage a été réalisé ou maintenu illégalement que la formation spécialisée en informe le requérant, sans toutefois pouvoir faire état d'aucun élément protégé par le secret de la défense nationale. Dans une telle hypothèse, par une décision distincte dont seule l'administration compétente (et la CNCTR s'il s'agit de techniques de renseignement) sont destinataires, la formation spécialisée annule le cas échéant l'autorisation et ordonne la destruction des renseignements irrégulièrement collectés.

---

(1) Services du Premier ministre pour les techniques de renseignement ; ministères gestionnaires des fichiers – intérieur, défense et économie – pour l'accès aux fichiers.

Comme l’a indiqué le président de la formation spécialisée, M. Edmond Honorat, **la formation respecte très scrupuleusement cette contrainte imposée par la loi, même si elle conduit, en pratique, à des motifs de rejet non détaillés voire stéréotypés**, souvent décevants pour les requérants. Il est vrai que le caractère asymétrique de la procédure est fortement contesté par les parties et leurs avocats, qui estiment ne pas être en mesure de se défendre utilement.

La formation spécialisée a ainsi jugé que la procédure suivie ne méconnaît ni les droits de la défense constitutionnellement garantis, ni les droits fondamentaux consacrés par la Convention européenne de sauvegarde des droits de l’homme et des libertés fondamentales (notamment ses articles 6 et 13) ou la Charte des droits fondamentaux de l’Union européenne voire d’autres conventions internationales.

Pour compenser les contraintes liées au caractère asymétrique de la procédure et assurer un contrôle effectif par le juge, **la formation spécialisée dispose de larges pouvoirs d’investigation à l’égard de l’administration** : suppléments d’instruction écrits, ce qui est fréquent dans la pratique ; auditions séparées des parties ; contrôles et visites sur place, ce qu’elle a déjà fait dans plusieurs cas, bien que le droit de visite ne soit pas explicitement prévu par le code de justice administrative.

Lors des audiences à huis clos, le requérant est invité systématiquement à prendre la parole pour présenter ses observations et compléter les éléments qu’il a pu apporter par écrit. Les membres de la formation spécialisée posent des questions afin d’apprécier le bien-fondé du recours au regard des éléments confidentiels portés à leur connaissance.

La formation spécialisée est, enfin, habilitée à soulever de sa propre initiative tout moyen, donc toute question de légalité ou de régularité, indépendamment de l’argumentation des parties.

d. Un premier bilan satisfaisant même si des améliorations sont souhaitables

● Un usage modéré des recours

Le contentieux porté devant la formation spécialisée a été, **dans sa quasi-totalité, un contentieux de l'accès aux fichiers intéressant la sûreté de l'État**. Il a porté, dans une large mesure, sur les fichiers du ministère de l'intérieur (1) et, dans une moindre mesure, sur les fichiers du ministère des armées – DGSE notamment.

DONNÉES GÉNÉRALES

Nombre de recours enregistrés depuis le 1er janvier 2016	**382**	**%**
Dont transmissions du TA de Paris	111	29,1 %
Dont saisines directes	271	70,9%

Source : Conseil d'État.

	2016	**2017**	**2018**	**2019**
Recours enregistrés	124	99	73	86
Dont transmissions du TA de Paris	77	27	3	4
Dont saisines directes	44	72	70	82

Source : Conseil d'État.

DONNÉES PAR TYPE DE SAISINE

1° du L. 841-1 (TR)	**32**
2° du L. 841-1 (CNCTR)	0
L. 841-2 (fichiers de sûreté)	329
III du L. 853-3 (ILP)	0
L. 854-9 (identifiant rattachable France)	0

Source : Conseil d'État.

(1) Fichier des personnes recherchées – FPR ; fichier Schengen – N-SIS II ; fichier CRISTINA de la DGSI.

DONNÉES PAR FICHIERS INTERROGÉS (1)

CRISTINA (DGSI)	83
DGSE	70
SIREX (DRSD)	33
DOREMI (DRM)	25
FSPRT	3
FPR	95
NSIS Schengen	72
STRATRAC (TRACFIN)	7
TAJ	2
Demande générale sans fichier identifié	5
Technique de renseignement	34

Les contrôles effectués par la formation spécialisée n'ont révélé aucune irrégularité dans le traitement des données des personnes figurant dans les fichiers soumis à son contrôle, à l'exception de **quelques anomalies** (péremption de données, protection de données rendues publiques par ailleurs, …) qu'elle a ordonné aux responsables de traitements de corriger.

Les **demandes de contrôle des techniques de renseignement demeurent marginales**, de l'ordre de quelques unités chaque année.

Aucun recours n'a été introduit par le président de la CNCTR ou trois des membres de cette commission.

La formation spécialisée du Conseil d'État n'a pas été saisie à ce jour de recours portant sur la surveillance de communications électroniques internationales, à l'exception du recours d'une parlementaire européenne de nationalité néerlandaise, introduit à l'époque où seule la CNCTR était habilitée à saisir le Conseil d'État. La formation spécialisée avait, en conséquence, rejeté ce recours en raison de son irrecevabilité.

● L'ouverture du recours

La CNCTR, dans son rapport d'activité pour l'année 2018, a indiqué que les conditions posées par la loi pour l'introduction de recours par des particuliers sont de nature à susciter des difficultés d'application et des interrogations quant à leur pertinence au regard du droit à un recours effectif. Interrogé sur ce point, le président de la formation spécialisée du Conseil d'État, M. Edmond Honorat, a estimé qu'« *une ouverture du recours à toute personne concernée supprimerait ces difficultés. Néanmoins, en l'état actuel des choses, il est difficile d'apprécier le*

(1) Une même requête peut porter sur plusieurs fichiers.

volume de contentieux qu'une telle ouverture pourrait susciter et les modifications que cela pourrait induire sur le fonctionnement de la formation spécialisée, dont les moyens sont limités. »

● Portée de l'obligation faite au juge de ne révéler ni directement ni indirectement si le requérant est inscrit ou non dans un fichier.

Cette contrainte limite les pouvoirs d'instruction du juge. Notamment, il est très difficile sinon impossible de discuter de l'exactitude de mentions figurant dans un fichier sans porter atteinte à cette obligation. Il s'agit de l'un des points faibles du contrôle, que ne manquent pas de soulever régulièrement les avocats.

Elle limite aussi la possibilité de motiver les décisions, qui sont dès lors, en grande partie, stéréotypées et présentent un caractère très elliptique.

Comme l'a noté le président de la formation spécialisée du Conseil d'État, M. Edmond Honorat, dans une note transmise aux membres de la mission d'information, la situation actuelle est paradoxale puisque « *selon le type de recours formé par un requérant, celui-ci peut avoir accès à plus ou moins d'informations pourtant protégées de la même façon. Ainsi, si le requérant conteste un refus ou un retrait d'autorisation professionnelle, l'administration sera obligée de justifier sa décision devant le juge administratif dans le cadre d'un débat contradictoire alors que s'il conteste le refus de lui donner accès aux fichiers consultés avant de prendre la décision, il n'obtiendra aucune information*. »

DEUXIÈME PARTIE : DES ENJEUX TECHNOLOGIQUES ET JURISPRUDENTIELS MAJEURS POUR L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT

Si les services de renseignement se sont bien approprié le cadre légal de la loi du 24 juillet 2015, ils sont néanmoins confrontés à deux types d'enjeux.

Le premier enjeu est de nature technologique **(I)**. En effet, si la loi a été rédigée de façon à éviter son « obsolescence programmée », le texte reste indéniablement axé sur l'usage de techniques et de ce fait, les évolutions technologiques en cours – explosion de la quantité de données à traiter, déploiement de la 5G, développement du chiffrement des communications, développement des techniques de reconnaissance biométrique – ont sans conteste un impact sur les méthodes de travail des services de renseignement que le législateur ne peut s'abstenir de prendre en compte dans le cadre d'un bilan législatif.

Parallèlement à ces enjeux d'ordre technologique, les services de renseignement français opèrent dans un cadre juridique marqué non seulement par l'évolution du droit national mais également par celle du droit international, et en particulier de la jurisprudence européenne (**II**). Cet enjeu jurisprudentiel a une double origine. D'une part, la Cour européenne des droits de l'homme a élaboré depuis une quarantaine d'années une jurisprudence sur la surveillance qui, comme dans d'autres domaines du droit, a des effets majeurs sur les législations nationales. D'autre part, et le fait est beaucoup plus récent mais aussi beaucoup plus préoccupant pour l'efficacité de l'action des services de renseignement, la Cour de justice de l'Union européenne (CJUE) a choisi, à la fin de l'année 2016, de se prononcer contre la conservation généralisée et indifférenciée des données par les opérateurs de télécommunications. Cette décision de la CJUE pourrait conduire à une remise en cause majeure de l'usage de nombreuses techniques de renseignement par les services non seulement français mais de tous les États membres de l'Union européenne.

I. PLUSIEURS ÉVOLUTIONS TECHNOLOGIQUES ONT DES INCIDENCES SUR LE CADRE D'INTERVENTION DES SERVICES DE RENSEIGNEMENT

Lors de ses auditions, la mission d'information a entendu plusieurs directeurs de service insister sur le fait que la loi du 24 juillet 2015 était très techno-centrée tandis que d'autres insistaient au contraire sur la plasticité d'un texte technologiquement neutre.

Comme on l'a vu en première partie du rapport, la loi du 24 juillet 2015 est **une loi de principe**. Il existe cependant **un débat sur son degré de techno-dépendance**. Plusieurs interlocuteurs de la mission ont insisté sur la nécessité de maintenir une neutralité technologique de la loi. D'après M. Floran Vadillo [(1)], la loi du 24 juillet 2015 est préservée de tout risque d'obsolescence programmée car dans ce texte, « *la modalité technique importe moins que la nature de l'ingérence (violation du secret des correspondances, violation du domicile,* etc.*), ou du renseignement recueilli (données, paroles, images, position géographique). Et lorsqu'un dispositif technique est évoqué, la loi veille à ne rien figer grâce à l'emploi de termes génériques et au renvoi à des actes réglementaires. En substance, la loi de 2015 a été rédigée pour ne pas vieillir, à l'instar de celle de 1991 qui, votée avant internet et le téléphone mobile, n'a pas nécessité de modifications pour prendre en charge les avancées technologiques*. *Par conséquent, les évolutions technologiques ne peuvent avoir d'incidence sur la rédaction lorsque leur principe figure dans la loi.* (…) *Si les services de renseignement devaient utiliser des drones,* (…) *il leur suffirait,* selon le chercheur, *d'énumérer les capacités du drone : collecte de données techniques (L. 851-6), interceptions (L. 852-1 II), captation de données informatiques (L. 853-2), captation d'images ou de son (L. 853-1), pénétration domiciliaire (L. 853-3).* »

De fait, on l'a vu en première partie de ce rapport, les articles 5 et 6 de la loi de 2015, qui sont codifiés au titre V du livre VIII du code de la sécurité intérieure, et qui ont trait aux techniques de recueil de renseignement, ne visent pas explicitement de technologies mais les « accès administratifs aux données de connexion », les « interceptions de sécurité », la « sonorisation de certains lieux et véhicules », la « captation d'images et de données informatiques », « les mesures de surveillance des communications électroniques internationales » et « les mesures de surveillance de certaines communications hertziennes ».

Les membres de la mission d'information souscrivent entièrement à l'idée qu'il importe d'assurer la stabilité du cadre juridique instauré par la loi du 24 juillet 2015 – un texte dont ils ont voulu montrer en première partie de ce rapport qu'il était équilibré et qu'il avait fait l'objet d'un important travail d'appropriation par les services de renseignement. Ils se félicitent également de cette plasticité du texte et donc de la clairvoyance du législateur de 2015. Par conséquent, la mission d'information ne peut que plaider contre des modifications par trop fréquentes de la loi.

Néanmoins, la question technologique a été soulevée lors de nombreuses auditions de la mission d'information, c'est pourquoi il importe à ses membres d'aborder cet enjeu.

---

(1) In L'Hétairie, Une seconde loi renseignement ? Pour une main tremblante mais des idées claires, *note du 9 mars 2020, pp. 8 et sq*

Le professeur Bertrand Warusfel, dans une intervention qu'il a présentée devant l'Académie du renseignement [(1)], revient sur la raison pour laquelle la loi est essentiellement tournée vers les moyens de renseignement de nature technologique. La loi de 2015, nous dit-il, « *a pris le parti de ne viser et encadrer que des moyens de renseignement de nature technologique.* (…) *Ce primat des sources techniques a plusieurs origines. D'une part, on assiste dans le domaine spécifique du renseignement au même phénomène de " numérisation " que dans tous les autres secteurs d'activité publique ou privée.* (…) *Mais à cette révolution numérique en marche tout autour de nous, s'ajoute une incitation particulière à numériser le renseignement qui découle, à notre sens, du primat de la lutte antiterroriste qui s'est imposée dans la dernière décennie comme la mission prioritaire de l'actuelle communauté du renseignement. C'est en effet l'antiterrorisme qui, en accroissant très fortement le nombre de cibles potentielles à surveiller, a poussé les services intérieurs (et non plus seulement extérieurs) à vouloir recourir massivement aux moyens de surveillance électronique, alors que traditionnellement le renseignement humain était la pratique dominante des services tels que la DST ou les RG.* »

Si la loi a été rédigée de manière à pouvoir s'adapter aux évolutions technologiques, il est indéniable que plusieurs d'entre elles ont ou auront des incidences sur le cadre d'intervention des services de renseignement.

Le premier enjeu technologique est celui de l'explosion de la quantité de données captées, défi auquel devrait permettre de répondre ce qu'il est convenu d'appeler « **l'intelligence artificielle** » (IA), outil indispensable à l'ensemble des ministères régaliens, et en particulier aux services de renseignement. Le recours à la multiplicité des outils de l'intelligence artificielle suppose « d'entraîner les machines », ce qui soulève la question des modalités de conservation des données nécessaires, en masse, pour permettre cet entraînement (**A**).

Le deuxième enjeu concerne l'évolution des télécommunications. D'une part, **le déploiement en cours et progressif de la cinquième génération de standards de télécommunications mobiles, la 5G**, est de nature à remettre en cause l'usage de techniques de renseignement telles que l'*IMSI-catcher*. D'autre part, on assiste à un développement du **chiffrement** des communications qui complique l'activité des services de renseignement (**B**).

Troisième enjeu d'ordre technologique, celui de **la reconnaissance biométrique** qui connaît un essor important depuis une dizaine d'années et qui soulève de nombreuses questions de libertés publiques. Cet outil, déjà utilisé dans certains domaines, nécessiterait un certain encadrement juridique mais aussi des ajustements techniques avant de pouvoir, le cas échéant, être exploité par les services de renseignement (**C**).

---

(1) In « Entre légitimation et contrôle : les logiques de l'encadrement juridique du renseignement », Le droit du renseignement*, L'Académie du renseignement, pp. 75 sq.*

Enfin, le quatrième enjeu concerne **l'utilisation des fichiers** par les services de renseignement (**D**).

A. L'IA PERMET DE FAIRE FACE À L'EXPLOSION DE LA QUANTITÉ DE DONNÉES MAIS SON USAGE SUPPOSE LA DÉFINITION DE MODALITÉS PARTICULIÈRES DE CONSERVATION DE CES DONNÉES À DES FINS DE RECHERCHE-DÉVELOPPEMENT

Le premier enjeu de portée technologique évoqué lors des auditions de la mission d'information est celui de l'explosion de la quantité de données captées. Cette effervescence quantitative s'explique aussi bien par le déploiement de capteurs de plus en plus performants que par la démultiplication des objectifs à surveiller, dans un contexte de numérisation croissante de la société.

Ce qu'il est convenu d'appeler l'intelligence artificielle devrait permettre de relever ce défi et, ainsi, éviter aux services de renseignement d'être submergés d'informations. Le développement de cet outil technologique par les services se heurte néanmoins aux règles juridiques qui encadrent très strictement – et à très juste titre, lorsqu'il s'agit de préserver les libertés et la vie privée des individus – les modalités de conservation des données collectées.

1. Le recours à l'intelligence artificielle permet de relever le défi de l'explosion de la quantité de données et offre une multiplicité d'usages possibles

a. Une solution au problème de l'explosion de la quantité de données

Certains chefs de service de renseignement auditionnés par la mission d'information ont souligné que l'un des principaux défis qui se présentaient à eux pour l'avenir était **l'exploitation des données, dont la quantité a explosé avec la numérisation croissante**. Les services doivent traiter, analyser et exploiter un flux exponentiel de données provenant de capteurs toujours plus performants. Ils doivent être capables de fournir la bonne information au bon moment en évitant de « se noyer » dans le flot d'informations. Lors de son audition du 8 mars 2018 devant la commission de la Défense nationale et des forces armées, le général Ferlet, directeur du renseignement militaire, avait déjà soulevé la question et avait même évoqué un « *tsunami de données* ».

Les services de renseignement peuvent certes bénéficier d'un renfort en ressources humaines pour assurer l'analyse et l'exploitation de données [(1)]. Cela représente d'ailleurs un défi de gestion de ces ressources humaines car le domaine est très attractif dans le secteur privé – en particulier dans certaines spécialités comme celles des interprétateurs image – et que compte tenu des niveaux de rémunération proposés, le secteur public n'est pas toujours le plus compétitif. Pour attirer des agents spécialisés en ce domaine, les services de renseignement

(1) Notamment dans le cadre de la loi de programmation militaire pour 2019-2025, s'agissant des services de renseignement sous tutelle du ministère des armées.

jouissent bien sûr d'un certain prestige mais certains d'entre eux peuvent avoir du mal à fidéliser leurs agents. Il faut donc que les services fassent un effort de formation et qu'ils se dotent d'outils en la matière.

Il n'en reste pas moins que **le traitement du *big data* nécessite le recours à des outils d'intelligence artificielle**. Comme l'a expliqué le général Ferlet le 8 mars 2018 dans les circonstances précitées, « *il ne saurait être question de faire face [à la croissance exponentielle de la masse de données à exploiter] en se contentant de demander des moyens supplémentaires en exploitants ou en analystes*. » Le général a insisté sur la nécessité de « *trouver des solutions plus innovantes, à base d'outils d'intelligence artificielle*. (…) *Il ne sert à rien,* a-t-il affirmé, *de collecter toujours plus de données et de renseignements si nous n'arrivons pas à les exploiter en tirant de nos bases de données les informations pertinentes au moment utile.* »

Cette préoccupation est largement partagée par les directeurs des autres services et administrations interrogés par la mission.

b. *Une multiplicité d'usages possibles*

Comme l'a souligné le coordonnateur ministériel en matière d'intelligence artificielle du ministère de l'intérieur (1), M. Renaud Vedel, lors de son audition par la mission d'information, l'intelligence artificielle recouvre de nombreux domaines techniques intéressant les services de renseignement : le traitement de l'image, de la parole, du texte mais aussi d'autres types de données plus hétérogènes. L'IA doit permettre aux agents des services d'avoir un meilleur accès à l'information, de développer la traduction et la transcription automatiques, de détecter une langue ou de reconnaître un locuteur, d'extraire des informations telles que des entités nommées, d'accélérer le traitement de la vidéo par élimination ou sélection de scènes sur requête sémantique, de détecter des schémas de communication ou encore de masquer des passages, extraits ou parties de documents à des fins de protection de la vie privée.

Il importe en effet de souligner que l'intelligence artificielle est un **moyen de discerner** et non pas de faire plus de surveillance ni de décupler les capacités d'intervention des services dans la vie privée des individus. L'intelligence artificielle n'est pas un outil de surveillance des personnes mais elle **favorisera la productivité des services de renseignement.**

2. L'apprentissage de l'intelligence artificielle suppose une adaptation du cadre juridique applicable à la conservation des données nécessaires à la recherche-développement

Comme l'a rappelé le coordonnateur ministériel précité lors de son audition par la mission d'information, « *les ministères régaliens ont besoin d'un*

(1) Entre-temps devenu le coordonnateur de la Stratégie nationale pour l'intelligence artificielle, rattaché à la direction générale des entreprises du ministère de l'économie et des finances.

cadre juridique permettant le développement d'outils incorporant des algorithmes d'intelligence artificielle, même à titre expérimental, pour leurs propres besoins ou pour l'écosystème dans lequel ils agissent. » C'est d'ailleurs l'un des objets du livre blanc de la sécurité intérieure en cours d'élaboration.

Ce besoin d'encadrement juridique a également été souligné par la secrétaire générale de la défense et de la sécurité nationale (SGDSN), Mme Claire Landais, qui a indiqué que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) menait elle aussi une réflexion sur le sujet.

a. La modélisation par les données suppose leur conservation pendant une longue durée dans la phase d'entraînement des outils d'IA

L'automatisation par l'intelligence artificielle suppose de recourir à la modélisation par les données. Cette modélisation s'opère en deux phases bien distinctes :

– la phase d'apprentissage, d'entraînement et de test, d'une part ;

– la phase opérationnelle, dite de production, d'autre part.

● La phase d'entraînement

Lors de la phase d'entraînement, des **données personnelles réalistes, tirées d'exemples opérationnels**, **sont utiles**, voire indispensables, pour construire un algorithme (1) performant. À l'issue du processus d'entraînement, l'algorithme ne conserve plus de données personnelles. « *Il s'agit* », a expliqué M. Renaud Vedel, *« d'un objet mathématique dont toute la valeur économique et opérationnelle réside dans la convergence réussie des paramètres* ». Les données d'entraînement étant coûteuses à produire, à annoter et à stocker, il est très souhaitable de **les conserver pendant une longue durée** : cela permet de tester ou de ré-entraîner les algorithmes régulièrement, de comparer la performance relative de plusieurs algorithmes différents applicables à une tâche donnée et de ne pas dupliquer les coûts lorsqu'un nouvel algorithme étalonné comme plus performant est disponible pour remplacer le précédent. Il importe d'insister sur le fait que les données personnelles utilisées dans la phase d'entraînement n'ont **aucune conséquence opérationnelle sur les personnes concernées**.

● La phase opérationnelle

Lors de la phase opérationnelle, ce sont des **données nouvelles**, totalement indépendantes des données d'apprentissage, que l'on utilise. Ces données sont tirées des missions de recherche et d'investigation en cours. Comme l'a indiqué le coordonnateur ministériel précité, « *le traitement peut légitimement entraîner des*

(1) On entend par là une série d'instructions d'exécution d'un calcul ou de résolution d'un problème, en particulier à l'aide d'un ordinateur. Ces instructions forment le fondement de toutes les opérations réalisables par un ordinateur et, par conséquent, constituent un aspect fondamental de tous les systèmes d'IA.

conséquences défavorables pour les personnes visées si celles-ci représentent une menace et il convient donc d'appliquer aux données opérationnelles le droit commun des données : principe de finalité et de proportionnalité, durées strictes de conservation et contrôle » d'une autorité administrative indépendante.

● La nécessité de pouvoir discriminer entre une situation de menace et une situation non porteuse de menace

L'intérêt recherché lorsqu'on recourt à l'intelligence artificielle est de pouvoir discriminer entre une situation représentant une menace et une situation non porteuse de menace. Pour **entraîner un algorithme à faire la distinction** entre ces deux types de situations, il est nécessaire d'avoir à disposition des exemples de chacun de ces deux types de situations et, par conséquent, de données « *n'ayant rien à voir avec la menace* ». Or, comme le souligne le coordonnateur ministériel précité, tout le droit habituel des fichiers de police ou de renseignement est construit sur le principe de finalité qui dispose que seules les données relatives aux personnes en lien avec un acte de délinquance ou une menace peuvent faire l'objet d'un traitement. Ainsi, seules des données relatives aux auteurs d'infraction peuvent être conservées. Dans de nombreux cas, ce principe est trop strict pour l'intelligence artificielle. Dans d'autres cas, l'algorithme à construire n'est pas un discriminateur mais nécessite quand même de recourir à des données variées. Par exemple, pour construire un traducteur automatique dans une paire de langues peu fréquente, ce qui compte est d'avoir le plus possible d'échantillons traduits, peu importe qu'ils aient ou non un lien avec des actes de délinquance ou des menaces.

b. Prévoir une exception à la durée légale de conservation des données pour faire de la recherche-développement et l'assortir des garanties adéquates

Lors de leurs auditions, plusieurs services de renseignement ont exprimé le souhait que la loi prévoie la possibilité d'accorder une dérogation aux durées de conservation en vigueur, leur permettant de faire de la recherche-développement avec des données existantes, afin d'assurer l'entraînement des outils d'intelligence artificielle. Il ne s'agit pas de prévoir une finalité spécifique dédiée à la recherche-développement mais simplement de leur assurer la capacité à faire des tests.

● La loi prévoit déjà l'utilisation de données par la direction générale de l'armement (DGA) à des fins de recherche-développement

Prévoir dans la loi des dispositions spécifiques relatives à l'utilisation de données à des fins de recherche-développement n'est pas inédit. Il existe en effet déjà des dispositions législatives en matière de tests réalisés par la direction générale de l'armement du ministère des armées : l'article L. 2371-2 du code de la défense, qui a été modifié par l'article 36 de la loi de programmation militaire (LPM) pour 2019-2025, prévoit en effet des règles applicables aux essais de matériels réalisés par ce service. Il est d'ailleurs prévu par ce dispositif que ces tests sont soumis à une déclaration préalable auprès de la CNCTR. Pour mémoire,

la version initiale de l'article L. 2371-2 du code de la défense, issue de l'article 18 de la loi du 30 octobre 2017 précitée, autorisait la DGA à appliquer des mesures d'interception aux fins d'effectuer des essais sur le territoire. Puis la LPM a complété cette disposition afin de prévoir, préalablement à ces tests, un régime de déclaration à la CNCTR.

L'article L. 2371-2 du code de la défense

Dans sa rédaction issue de l'article 36 de la loi n° 2018-607 du 13 juillet 2018 de programmation militaire, l'article L. 2371-2 du code de la défense définit les conditions dans lesquelles les personnels de la direction générale de l'armement ainsi que les militaires de certaines unités des forces armées peuvent procéder aux essais de qualification des matériels permettant la mise en œuvre de techniques de renseignement.

Cet article permet la réalisation d'essais de qualification pour les matériels nécessaires à la mise en œuvre de l'ensemble des techniques et mesures de renseignement concernées par de tels essais, à savoir les appareils et dispositifs permettant :

– le recueil de données techniques de connexion et les données relatives à la localisation d'équipements terminaux ;

– l'interception de sécurité ;

– l'interception de correspondances échangées au sein d'un réseau fermé de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque le réseau est conçu pour une utilisation privative (hertzien « privatif ») ;

– la surveillance des communications électroniques internationales ;

– l'interception de communications empruntant exclusivement une voie hertzienne ouverte.

En effet, bien que des moyens de communication « plastrons » soient utilisés pour mener les essais de qualification, des communications privées peuvent néanmoins être interceptées de manière résiduelle à l'occasion de tels tests. Quand bien même les données ainsi recueillies ne sont pas exploitées, il convient de sécuriser juridiquement ces campagnes de qualification et les personnels qui les réalisent, en écartant tout risque de poursuite pénale dès lors que les essais seraient menés conformément à la loi.

La loi interdit expressément l'exploitation des données recueillies aux fins de tests et prévoit par ailleurs :

– que chaque campagne d'essais doit faire l'objet d'une déclaration préalable auprès de la CNCTR ;

– que de tels essais ne peuvent être réalisés que par des personnels individuellement désignés et habilités ;

– que les données recueillies dans le cadre de ces essais ne peuvent être conservées que pour la durée de ceux-ci et qu'elles doivent être détruites à l'issue de la campagne de tests ;

– que la CNCTR est informée du champ et de la nature des essais effectués et qu'un registre recensant les opérations réalisées dans le cadre de ces campagnes de qualification lui est communiqué à sa demande.

● La loi prévoit déjà une dérogation aux durées de conservation de droit commun s'agissant des données cryptées

Si la loi prévoit déjà la possibilité d'utiliser des données personnelles à des fins de recherche-développement, le législateur a également déjà prévu la possibilité de déroger aux durées de conservation des données de droit commun, dès lors que ces dernières sont cryptées. Comme on l'a vu en première partie, l'article L. 822-2 du code de la sécurité intérieure prévoit que :

– la durée maximale de conservation est de six ans à compter du recueil pour les **renseignements chiffrés** ;

– **dans une mesure strictement nécessaire aux besoins de l'analyse technique et à l'exclusion de toute utilisation pour la surveillance des personnes concernées**, les renseignements collectés qui contiennent des éléments de **cyberattaque** ou qui sont chiffrés, ainsi que les renseignements déchiffrés associés à ces derniers, peuvent être conservés au-delà des durées de droit commun fixées au I de l'article L. 822-2.

● La définition d'un régime dérogatoire à des fins d'apprentissage des outils d'IA doit être impérativement assortie de garanties spécifiques.

Tout d'abord, comme nous l'avons souligné plus haut, si le législateur décidait d'établir un régime dérogatoire aux durées légales de conservation des données à des fins d'apprentissage des outils d'intelligence artificielle, il lui faudrait impérativement bien distinguer entre le régime juridique applicable aux données nécessaires en phase d'apprentissage de l'intelligence artificielle et le régime juridique actuellement applicable au traitement de données.

Ensuite, en contrepartie de la définition d'un régime juridique assoupli en matière de conservation des données en phase d'apprentissage, il conviendrait de prévoir des garanties spécifiques telles que :

– l'exclusion de tout usage opérationnel des données d'entraînement ;

– la conservation de ces données par un tiers de confiance indépendant des services investigateurs ;

– la pseudonymisation des données – pour autant qu'elle soit compatible avec la finalité d'apprentissage.

Le coordonnateur ministériel en matière d'intelligence artificielle a indiqué à la mission que « *dans la plupart des cas, le principe d'anonymisation n'est pas pertinent : il aboutit en pratique à appauvrir ou à détruire au préalable l'information précisément utile à l'opération de modélisation par apprentissage.*

C'est tout particulièrement le cas pour certains traitements d'images, de la voix humaine ou de données hétérogènes relatives à des personnes ».

Pseudonymisation et anonymisation des données personnelles (1)

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible.

La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires. En pratique la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, *etc.*) d'un jeu de données par des données indirectement identifiantes (alias, numéro dans un classement, *etc*.). La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. En pratique, il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces. C'est pourquoi des données pseudonymisées demeurent des données personnelles. L'opération de pseudonymisation est réversible, contrairement à l'anonymisation.

Enfin, le coordonnateur ministériel en matière d'intelligence artificielle a indiqué aux membres de la mission d'information que les services de renseignement devraient mener une politique renouvelée de gestion des données, selon une approche ternaire :

– les données sont d'abord collectées, raffinées et sélectionnées pour produire un renseignement particulier sur une thématique et dans un dossier donné ;

– les données relatives aux menaces avérées mériteront d'être capitalisées : données brutes, données recoupées, produits finis de renseignement ;

– des échantillons de données pertinents correspondant au cas d'usages de logiciels de modélisation par les données mériteront d'être spécifiquement extraits, mis en qualité et insérés dans des jeux d'apprentissage à des fins de constitution non pas d'un capital informationnel mais d'un capital technologique métier.

La mission d'information formule une proposition en ce sens au VI de la troisième partie de rapport.

B. LES MODALITÉS DE COMMUNICATION ÉVOLUENT AVEC LE CHIFFREMENT ET LE DÉPLOIEMENT À VENIR DE LA 5G

Le deuxième défi technologique évoqué par les services de renseignement lors des auditions de la mission d'information concerne les évolutions en cours des modalités de télécommunications. Deux évolutions ont été abordées :

(1) *Source : Commission nationale de l'informatique et des libertés, https://www.cnil.fr/fr/lanonymisation-des-donnees-un-traitement-cle-pour-lopen-data*

– d'une part, le déploiement de la 5G qui remettra en cause l'usage, par les services de renseignement, des *IMSI-catchers* ;

– d'autre part, le chiffrement des communications.

1. La remise en cause de l'usage des *IMSI-catchers* par le déploiement à venir de la 5G

L'arrivée de la 5G en France est prévue à partir de l'année 2020. La procédure de sélection pour l'attribution des fréquences de la 5G, conduite par l'Autorité de régulation des communications électroniques et des postes (ARCEP) a été lancée le 31 décembre 2019. Les autorisations d'utilisation de fréquences seront délivrées aux opérateurs mobiles au cours du deuxième trimestre 2020 et les fréquences devraient être disponibles pour une utilisation par les opérateurs mobiles soit au 1er juillet 2020, soit au 1er janvier 2021, selon les départements.

a. Une rupture technologique

La 5G, cinquième génération de standards de télécommunications mobiles, va entraîner une véritable rupture technologique.

Le réseau 5G (1) se caractérise par **une architecture décentralisée**, un cœur de réseau local étant placé sur chacune des antennes. Il repose sur les principes de l'informatique en périphérie (*edge computing*) qui consiste à traiter les données en périphérie du réseau, près de la source, plutôt que vers les centres de données (*data center*) et repose sur plusieurs nouvelles technologies : un réseau par tranches (*network slicing*) (2), avec un accès multiple en périphérie (MEC) (*multi-access edge computing*), une virtualisation des fonctions du réseau (*network functions vitualization*) et une virtualisation des ressources réseaux (*software defined network*) avec un chiffrement de bout en bout (*end-to-end encryption* – E2E) et la détection des fausses stations (*false-base detection*).

Ses caractéristiques lui permettront notamment de scinder des réseaux physiques en plusieurs réseaux virtuels afin d'y relier l'ensemble des objets connectés (3) tels que les véhicules, smartphones, ordinateurs, assistants vocaux, capteurs variés, *etc*. En 2025, le nombre d'objets connectés à internet devrait atteindre 25 milliards pour un marché d'une valeur de 1 000 milliards d'euros. Ces nouvelles technologies offrent plusieurs avantages à l'utilisateur : un débit plus rapide – 100 fois supérieur au réseau 4G –, une latence (4) très faible, des

---

(1) Source : Réseau 5G et cybersécurité, Observatoire national des sciences et technologies de la sécurité, ressources documentaires du pôle judiciaire de la gendarmerie nationale et https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security .

(2) Le slicing *rend possible la séparation de l'utilisation du réseau en fonction des demandes de l'utilisateur, selon ses usages. Cette capacité permettra de déployer les applications de* cloud computing *(fonctionnalités assurées via le* cloud *et donc indépendantes de la performance du terminal – téléphone, ordinateur* etc.*) tout en maintenant une utilisation régulière du réseau pour des fonctions de base.*

(3) Internet of things *ou IoT.*

(4) La latence correspond au temps nécessaire à deux appareils pour communiquer entre eux.

connexions plus stables et moins énergivores ainsi qu'une sécurité des communications renforcées.

b. *Une technologie remettant en cause l'usage des* IMSI-catchers

Si la 5G présente de nombreux avantages pour ses utilisateurs, elle constitue un défi pour les services de renseignement, comme d'ailleurs pour les forces de l'ordre.

Lors de leurs auditions, les responsables des différents services de renseignement n'ont pas manqué d'alerter les membres de la mission d'information sur le fait que le développement de la 5G pourrait compliquer, voire rendre impossibles, les actuels repérages de communications, écoutes et localisations. Le déploiement de la 5G va avoir trois conséquences.

Tout d'abord, il va rendre complexes voire impossibles le recueil de données de connexion et donc l'identification et la localisation d'appareils mobiles. Le chiffrement empêchera la lecture de l'IMSI (*International Mobile Subscriber Identity*), c'est-à-dire du numéro de code unique qui permet à un réseau de téléphonie mobile d'identifier un usager lors de chaque appel. Ce code se trouve stocké sur la carte SIM de l'appareil – la puce qui enregistre les données pour l'abonné – et est inconnu de l'utilisateur de cet appareil. Avec la 5G, les identifiants numériques échangés entre les terminaux et les antennes du réseau mobile changeront à des fréquences élevées. Si l'on ne peut pas établir de lien entre les identifiants éphémères et les identifiants pérennes, l'exploitation des données recueillies sera pratiquement impossible. La 5G va ainsi « réduire à néant » ce qu'Europol décrit comme le plus important des outils opérationnels et tactiques d'investigation [(1)].

La 5G va également rendre difficile l'analyse des données captées : le chiffrement de bout en bout de l'ensemble du trafic sur le réseau 5G compliquera les opérations de criminalistique [(2)] informatique en ralentissant le travail d'enquête puisqu'il rendra nécessaire le déchiffrement ou décryptage des données.

Enfin, la technologie du réseau par tranches va répartir l'ensemble des communications sur l'ensemble des réseaux virtuels. Chaque réseau virtuel étant géré par une société différente, cela va contraindre à collaborer avec plusieurs prestataires de services, parfois à l'international, afin de pouvoir récupérer auprès de chacun d'eux des fragments de l'information recherchée. Avec la norme MEC les objets seront capables de communiquer directement entre eux sans transiter par le réseau d'un opérateur téléphonique, rendant l'information recherchée potentiellement inaccessible pour les forces de l'ordre.

---

(1) Propos rapportés par Jean-Pierre Stroobants in Le Monde *du 12 juin 2019, « La 5G provoque un vent de panique au sein des services de sécurité européens ».*

(2) La criminalistique consiste en l'ensemble des techniques mises en œuvre par la justice, la police et la gendarmerie pour établir la preuve d'un délit ou d'un crime et en identifier son auteur.

c. Imposer de nouvelles obligations aux opérateurs ?

Il pourrait être **nécessaire que les opérateurs de télécommunications fournissent en temps réel un accès à un annuaire permettant de relier identifiants éphémères et identifiants pérennes**. On pourrait aussi demander à l'opérateur les identifiants électroniques qui se sont connectés à telle ou telle antenne, à tel instant.

En l'état actuel du droit, la loi n'a pas prévu que les opérateurs apportent leur concours à la mise en œuvre de l'article L. 851-6 du code de la sécurité intérieure, relative à l'utilisation d'*IMSI-catchers* pour le recueil de données de connexion ni pour celle du II de l'article L. 852-1, relatif à l'utilisation d'*IMSI-catchers* pour le recueil des correspondances.

2. La remise en cause des interceptions de sécurité par le chiffrement de bout en bout des communications

Indépendamment du déploiement à venir de la 5G, **nombre de logiciels ou applications – tels que Whatsapp, Telegram, Signal ou Wire – proposent déjà un chiffrement des échanges « de bout en bout ».** Ce procédé, qui vise à rendre illisibles les échanges qui se déroulent sur ces plateformes à l'aide de techniques de cryptographie, consiste à transformer une donnée pouvant être lue par n'importe qui – donnée dite « claire » – en donnée ne pouvant être lue que par son émetteur et son destinataire grâce à l'utilisation d'une clef de chiffrement. Il n'est possible de récupérer la donnée claire à partir de la donnée chiffrée qu'à condition de disposer de la clef de déchiffrement, clef qui est entre les seules mains de l'entreprise proposant son logiciel ou son application. Les données chiffrées sont codées à l'aide d'un algorithme. Comme l'explique François Paget, expert en cybercriminalité et secrétaire général adjoint du Club de la sécurité de l'information français (Clusif) (1), une clef de déchiffrement est généralement une suite de chiffres ou une séquence hexadécimale incompréhensible, en fonction du système utilisé pour le chiffrement.

Si le chiffrement vise à garantir la confidentialité des échanges et à protéger la vie privée des utilisateurs de ces logiciels ou applications, il représente évidemment un **obstacle pour les services de renseignement souhaitant procéder à des interceptions de sécurité**. Le travail des services de renseignement s'en trouve d'autant plus compliqué que les entreprises proposant ces logiciels ou applications rechignent très souvent à partager les données dont elles disposent au nom de respect la vie privée des utilisateurs. Les États-Unis, entre autres, sont allés jusqu'à accuser les entreprises (2) qui refusent de coopérer de complicité avec les personnes utilisant ces plateformes chiffrées pour fomenter des actes délictueux sans crainte de représailles. Le directeur de l'Agence

(1) In Les Échos, *https://www.lesechos.fr/2016/02/le-chiffrement-des-donnees-comment-ca-marche-197164*.

(2) Voir notamment cet article, relatif au contentieux opposant le FBI à Apple : https://www.lesechos.fr/2016/02/chiffrement-apple-et-google-contre-la-nsa-le-fbi-et-donald-trump-197166 .

nationale de sécurité américaine, la NSA, a même déclaré que le chiffrement avait empêché de déjouer les attentats du 13 novembre 2015 à Paris (1) .

S'il est indéniable que le chiffrement des communications se développe, le directeur du GIC, lors de son audition, a néanmoins fait état d'un paradoxe : alors qu'internet est très majoritairement chiffré et de plus en plus impénétrable, les interceptions de sécurité – non seulement de voix mais aussi de flux internet – ne se sont jamais aussi bien portées puisqu'elles connaissent une croissance à deux chiffres.

3. La position de la mission d'information

Qu'il s'agisse de la remise en cause de l'usage des *IMSI-catchers* par le déploiement de la 5G ou des interceptions de sécurité par le chiffrement des communications, la mission d'information estime que ces mutations technologiques n'appellent pas, à ce stade, une réponse juridique certaine. Elle tenait cependant à souligner l'importance de ces défis technologiques pour les services de renseignement.

C. LA RECONNAISSANCE BIOMÉTRIQUE, UNE TECHNOLOGIE DONT L'UTILISATION DOIT ÊTRE ENCADRÉE

1. Une technologie d'authentification et d'identification

La reconnaissance faciale est **une technologie biométrique d'identification et de contrôle de l'identité des personnes**. Informatique et probabiliste, cette technologie permet de reconnaître automatiquement une personne sur la base de son visage pour l'authentifier ou l'identifier. Il s'agit, à partir d'une image numérique ou d'un support vidéo présentant un visage, de comparer et d'analyser ses caractéristiques en fonction des lignes faciales. Authentifier une personne grâce à la reconnaissance faciale consiste à comparer son visage avec une image de celui-ci enregistrée préalablement et censée le caractériser. Identifier une personne nécessite de comparer la même caractéristique avec une base de données de personnes connues. La reconnaissance faciale permet également de réidentifier une personne mais aussi de rechercher une personne parmi une foule de personnes inconnues, afin de vérifier si y figure une personne dont on dispose des caractéristiques biométriques du visage. Tous les dispositifs de reconnaissance faciale reposent sur une action de comparaison avec un attribut présenté par une base de données ou un support physique détenu par la personne.

Selon la Commission nationale de l'informatique et des libertés (CNIL) (2), la reconnaissance faciale peut être associée à d'autres dispositifs : *« À la différence par exemple des systèmes de captation et de traitement vidéo, qui nécessitent la*

(1) Source : Les Échos, *ibid.*

(2) In Reconnaissance faciale : pour un débat à la hauteur des enjeux, *15 novembre 2019, pp. 3 sq.*

mise en place de dispositifs physiques, la reconnaissance faciale est une fonctionnalité logicielle qui peut être mise en œuvre au sein de systèmes existants (caméras, bases de données de photos, etc.*). Cette fonctionnalité peut donc être connectée, branchée sur une multitude de systèmes, et combinée avec d'autres fonctionnalités*. »

Cette technologie a nettement progressé puisqu'alors que les systèmes de reconnaissance biométrique les plus performants atteignaient un taux de 72 % de précision en 2010, ils dépassent parfois les 95 % aujourd'hui (1).

2. Des usages et des finalités multiples

La CNIL rappelle que la reconnaissance faciale peut poursuivre des finalités très diverses, aussi bien commerciales que liées à la sécurité publique. « *Si l'on parcourt le champ des usages potentiels, une gradation peut être envisagée, en fonction du degré de contrôle des personnes sur leurs données personnelles, de leur marge d'initiative dans le recours à cette technologie, des conséquences qui en découlent pour elles et de l'ampleur des traitements mis en œuvre* ». Compte tenu de l'objet de ce rapport d'information, nous ne nous étendrons pas sur la question de l'authentification par la reconnaissance faciale, préférant nous concentrer sur l'usage de cette technologie à des fins d'identification.

L'identification par la reconnaissance biométrique peut donner lieu à une multiplicité d'usages, rappelés par la CNIL dans son étude du 15 novembre 2019 et dont nous retenons, en particulier les suivants :

– **la recherche, dans une base de données comportant des photographies, de l'état civil** d'une personne (victime, suspecte, *etc*.) non identifiée, ainsi que le permet par exemple en France le traitement des antécédents judiciaires (TAJ (2)) ;

– **le suivi des déplacements d'une personne dans l'espace public**, par comparaison entre son visage et les gabarits biométriques des personnes circulant ou ayant circulé dans la zone surveillée, par exemple en cas d'oubli d'un bagage ou à la suite de la commission d'un délit ;

– **la reconstitution du parcours d'une personne et de ses interactions successives** avec des personnes tierces, par une comparaison des mêmes éléments mais réalisée en différé, pour identifier ses contacts par exemple ;

---

(1) Si l'on en croit le Forum économique mondial, qui travaille actuellement sur le sujet et qui a produit en février dernier un Livre blanc intitulé Cadre d'action pour un usage responsable de la reconnaissance faciale (page 4).

(2) Le traitement d'antécédents judiciaires (TAJ) est pour l'instant le seul fichier comportant une photographie dont l'usage est autorisé à des fins de reconnaissance faciale.

– **l'identification sur la voie publique de personnes recherchées**, par confrontation en temps réel de tous les visages captés à la volée par des caméras de vidéoprotection et une base de données détenue par les forces de l'ordre.

Comme l'indiquent les auteurs du rapport sur la *Reconnaissance faciale : entre exigence de contrôle et respect de la vie privée* [(1)], « ***la reconnaissance faciale connaît au niveau international un développement nettement plus important et abouti qu'en France.*** *De nombreux pays connaissent des déploiements à grande échelle et l'utilisation sur la voie publique s'illustre également à travers plusieurs exemples, non limités à la question sécuritaire* [(2)]. » Le rapport cite plusieurs cas, notamment aux États-Unis et en Europe : l'utilisation à des fins d'enquête par Europol ; la sécurisation des villes (New York, Chicago, Moscou) et des sites sensibles (tels que la Maison blanche à Washington DC) ; certaines expérimentations sur le continent européen (l'aéroport d'Heathrow à Londres, la gare routière de Madrid et la gare Südkreuz de Berlin).

4. Une technologie présentant des risques potentiels importants et nécessitant un encadrement juridique

a. Des risques potentiels très importants pour les libertés publiques

La reconnaissance faciale présente bien évidemment des risques pour les libertés publiques. La CNIL en identifie quatre principaux :

– cette technologie concerne des **données sensibles** ;

– elle est « sans contact » et **potentiellement omniprésente** ;

– elle représente, selon la CNIL, un « **potentiel de surveillance inédit** » ;

– enfin, c'est une **technologie encore faillible**.

Premier type de risque inhérent à la technologie de reconnaissance faciale, celle-ci concerne des données « sensibles » c'est-à-dire des **données relatives à l'intimité de la vie privée** des personnes. Ces données *« présentent la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir* [(3)]. »

Deuxièmement, la CNIL rappelle que les données de reconnaissance faciale sont **potentiellement disponibles partout** puisque les visages des personnes sont collectés et enregistrés dans une multiplicité de bases de données et puisque toute photographie peut potentiellement devenir une donnée biométrique.

---

(1) Reconnaissance faciale : entre exigence de contrôle et respect de la vie privée – Quels outils, quels enjeux, quelles garanties, *Institut national des hautes études de la Sécurité et de la justice (INHESJ) 30ème session nationale « Sécurité et Justice » 2018-2019 Groupe de diagnostic stratégique (GDS) n° 8.*

(2) Page 14 du rapport précité

(3) CNIL, ibid.

La CNIL parle ainsi d'une véritable « *dissémination de données* » dans un « *contexte d'exposition permanente de soi sur les réseaux sociaux* ». La Commission nationale de l'informatique et des libertés fait remarquer que cette technologie permet le traitement de données à distance et à l'insu des personnes et le suivi en temps réel des déplacements de chacun, sans interaction avec la personne et donc sans qu'elle en ait même conscience : *« Techniquement, la reconnaissance faciale permet ce que nulle autre technologie ne permet actuellement ni n'a jamais permis, à savoir reconnaître une personne n'ayant entrepris aucune démarche particulière, ni à l'occasion d'un enrôlement ni à l'occasion de la comparaison, voire identifier nominativement une telle personne, sans que le porteur du dispositif ait jamais entretenu la moindre relation avec elle*. »

Dans le cadre de sa réflexion précitée, le Forum économique mondial se fait l'écho de ces préoccupations, soulignant lui aussi que l'un des risques de la reconnaissance faciale « *serait qu'une technique devienne un outil de surveillance active des personnes en temps réel. L'usage de cette technologie inquiète à juste titre l'opinion publique d'autant qu'il se fait parfois à l'insu et sans le consentement des personnes concernées.* (…) *Il est régulièrement fait état d'atteintes à l'intégrité des données biométriques et d'utilisation des données personnelles en vue de développer des systèmes de reconnaissance faciale sans en informer les utilisateurs.* »

Troisièmement, la reconnaissance faciale représente, selon la CNIL, un potentiel de surveillance inédit. Nombreux sont les dispositifs de vidéosurveillance, de vidéoprotection mais aussi les *smartphones* et les écrans publicitaires pouvant devenir des supports de surveillance. La CNIL souligne qu'« *on ne peut exclure que ces dispositifs de captation d'images, supports potentiels de tout système de reconnaissance faciale, soient en outre couplés à d'autres types de technologies, par exemple la captation du son, amplifiant encore davantage le degré de surveillance des personnes et des lieux. Ce tournant technologique se double d'un changement de paradigme de la surveillance, déjà constaté en de nombreux domaines : **le passage d'une surveillance ciblée de certains individus à la possibilité d'une surveillance de tous aux fins d'en identifier certains.** Le remplacement des contrôles humains de vérification de l'identité des personnes par des contrôles réalisés par des traitements algorithmiques, modifie, par lui-même, le potentiel de surveillance.* »

La Commission nationale de l'informatique et des libertés parle ainsi d'un véritable changement de nature de la surveillance dès lors que celle-ci devient indifférenciée. Les cas d'usages les plus poussés de la reconnaissance faciale présentent un risque évident d'atteinte à l'anonymat dans l'espace public. L'espace public, physique ou numérique, est un lieu où s'exercent de nombreuses libertés individuelles et publiques : droit à la vie privée et à la protection des données personnelles, mais également liberté d'expression et de réunion, droit de manifester, liberté de conscience, libre exercice des cultes, *etc*. Cet anonymat est protégé par le droit en vigueur.

Le Forum économique mondial note lui aussi que certains usages de la reconnaissance faciale « *représentent une menace potentielle pour les droits humains et les libertés individuelles, notamment la liberté d'expression, la liberté de réunion et d'association ainsi que pour le droit au respect de la vie privée* ».

Enfin, quatrième point, la CNIL souligne à quel point cette technologie reste faillible : comme tout traitement biométrique, la reconnaissance faciale repose sur des estimations statistiques de correspondance entre les éléments comparés. La variation des performances peut ainsi avoir des conséquences très importantes pour les personnes mal reconnues par le dispositif. En outre, cette technologie comporte actuellement des biais importants : des expérimentations menées en France et dans le monde ont par exemple démontré que les taux d'erreur commis par les algorithmes de reconnaissance faciale pouvaient varier avec le sexe ou la couleur de peau.

b. Le droit applicable

Comme le rappellent les auteurs du rapport de l'INHESJ précité, « *au nombre des biométries disponibles (empreintes digitales, iris, voix,* etc.*), la reconnaissance faciale est particulière, basée sur la capture d'une photographie du visage d'une personne, à laquelle est appliqué un procédé technique permettant d'extraire des caractéristiques, le " gabarit ". C'est à partir de cette représentation mathématique du visage que la comparaison faciale est effectuée. L'usage qui peut être fait de cette catégorie de données est strictement encadré par les dispositions relatives à la protection des données*. »

Plusieurs dispositions encadrent la technique de reconnaissance faciale dans le droit en vigueur.

● Le droit applicable en cas d'utilisation de la reconnaissance biométrique par l'État dans le cadre de ses prérogatives de puissance publique

Les dispositifs d'analyse automatisée du flux vidéo, pouvant embarquer des modalités de reconnaissance biométrique, reposent généralement sur des systèmes de vidéoprotection. En droit français, les traitements de données biométriques pour le compte de l'État dans le cadre de ses prérogatives de puissance publique sont encadrés par l'article 32 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et par l'article 10 de la directive européenne n° 2016/68022. **L'article 32 de la loi de 1978** prévoit que **sont autorisés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés**, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

● En cas d'utilisation par les acteurs privés, le RGPD s'applique

Dans l'Union européenne, depuis le 25 mai 2018, la mise en place de traitements mobilisant des données personnelles est encadrée par le Règlement général sur la protection des données (RGPD). L'utilisation de dispositifs de reconnaissance faciale, faisant intervenir des données biométriques, particulièrement sensibles parce qu'elles permettent d'identifier de façon unique un individu, doit donc se conformer aux dispositions introduites par ce règlement. En particulier, le responsable d'un traitement doit effectuer une analyse d'impact relative à la protection des données et la transmettre à la CNIL, pour consultation préalable, en cas de détection de risques résiduels élevés. Dès lors, la CNIL n'est plus systématiquement informée de la mise en place de ces dispositifs et n'a plus à donner son accord *a priori*. En contrepartie, ce nouveau système vise à la responsabilisation de l'auteur du traitement et de son sous-traitant, qui est considéré comme coresponsable. Pour ce type d'utilisation, le consentement est une des bases légales possibles. Le RGPD permet de déroger à certaines règles lorsque le traitement est effectué à des fins de recherche scientifique. Les responsables de traitement sont désormais assujettis à de nouvelles obligations : notification à l'autorité de contrôle de toute violation de données personnelles, tenue d'un registre, désignation le cas échéant d'un délégué à la protection des données. Au surplus, dans de très nombreux cas, une analyse d'impact sur la protection des données doit être réalisée. Les responsables de traitement doivent également veiller à ce que les personnes qui souhaitent exercer les droits qui leur sont reconnus (droits d'information, d'accès, à l'effacement des données) obtiennent satisfaction.

● Le droit applicable aux fichiers en matière de reconnaissance biométrique

Le fichier des personnes recherchées (FPR) [(1)] comporte des photographies mais l'article 3 du décret du 28 mai 2010 créant ce fichier précise qu'elles ne peuvent faire l'objet d'un dispositif de reconnaissance faciale.

Quant au traitement des antécédents judiciaires (TAJ), sur lequel nous reviendrons *infra*, il est utilisé dans le cadre d'enquêtes judiciaires, pour la recherche des auteurs d'infractions, et d'enquêtes administratives, notamment les enquêtes préalables à certains emplois publics ou sensibles. Il comprend des informations concernant des personnes mises en cause, des victimes, ou des personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition au sens des articles 74 et 74-1 du code de procédure pénale. Au nombre des données enregistrées, figure

(1) Ce fichier a pour objet de recenser toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification et de faciliter l'action des services de police et de gendarmerie, des autorités judiciaires, militaires ou administratives. L'inscription au FPR intervient notamment pour des motifs d'ordre public, tels que la prévention de menaces contre la sécurité publique ou la sûreté de l'État.

la photographie, qui comporte des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale [(1)].

Enfin, s'agissant du fichier des titres électroniques sécurisés (TES) [(2)], la CNIL a relevé dans sa délibération n° 2016-292 du 29 septembre 2016 portant avis sur le projet de décret, que « *le II de l'article 3* (…) *prévoit que le traitement TES ne comportera pas de dispositif de recherche permettant l'identification à partir de l'image numérisée du visage ou des empreintes digitales. Les données biométriques ne seront accessibles qu'à partir des données d'identité, ce qui permettra de vérifier l'identité avancée par le demandeur, mais non de rechercher l'identité d'une personne à partir de ses empreintes ou de sa photographie* ». Elle a par ailleurs souligné « *que l'effectivité de cette exclusion, qui suppose la mise en œuvre de mesures de sécurité strictes et un contrôle permanent des accès aux données ainsi que de leur utilisation, doit impérativement être assurée* ».

5. L'usage éventuel de la reconnaissance biométrique par les services de renseignement : quels principes ?

● Plusieurs acteurs du renseignement envisagent d'utiliser la reconnaissance biométrique

Plusieurs interlocuteurs de la mission d'information estiment que l'utilisation de la reconnaissance biométrique par les services de renseignement sera inéluctable et envisagent d'y recourir. L'un d'entre eux a ainsi souligné que la reconnaissance biométrique était une technologie particulièrement utile pour repérer les personnels civils étrangers ayant servi à l'étranger, qui se font renvoyer de leur base et qui se font employer sur une autre base en changeant de nom, grâce à de faux papiers : la reconnaissance biométrique permet alors de vérifier que la personne ne porte pas son vrai nom.

On peut distinguer trois sources d'approvisionnement en images pour l'usage de la reconnaissance biométrique par les services de renseignement. Tout d'abord, les images **collectées par les services**. Ensuite, **internet** avec la possibilité, dans le futur, de recourir à des moteurs de recherche utilisant la reconnaissance biométrique. Il s'agirait alors de surveiller internet en y ciblant certaines personnes. Enfin, la troisième source serait **l'espace public**, domaine qui n'a pas encore été expérimenté par les services, compte tenu de la sensibilité du sujet mais aussi d'une insuffisante maîtrise technologique.

---

(1) Article R. 40-26 du code de procédure pénale.

(2) Le fichier TES regroupe les traitements de données à caractère personnel relatifs aux passeports et aux cartes nationales d'identité. Il vise, d'une part, à faciliter l'établissement, la délivrance, le renouvellement, l'invalidation et le retrait des titres concernés et, d'autre part, à prévenir et détecter leur falsification et contrefaçon. In fine*, il centralise notamment, dans une base de données, l'image numérisée du visage de l'ensemble des demandeurs de carte nationale d'identité et de passeport, et réunit ainsi les données biométriques relatives à la quasi-totalité de la population française.*

● L'usage de la reconnaissance biométrique à des fins de renseignement n'est pas mûr et nécessitera des adaptations technologiques

Certaines personnalités auditionnées par la mission estiment que l'usage de la reconnaissance biométrique à des fins de renseignement ne sera pas possible avant cinq à dix ans. Cette technologie reste pour l'heure au **stade expérimental**. Elle impose en effet des **contraintes techniques de flux d'information**. La vidéoprotection est communale sauf à Paris et le renvoi de flux étant de plus en plus lourd, il **nécessite des moyens très importants**.

● Si la reconnaissance biométrique devait être utilisée par les services de renseignement, il conviendrait d'en faire une technique de renseignement en soi

Si la reconnaissance faciale devait être intégrée aux techniques de renseignement, il conviendrait qu'elle fasse l'objet des mêmes modalités d'encadrement que ces techniques, notamment en termes de **finalités, de durée et de limitation à certains lieux publics**. Il pourrait notamment être envisagé de constituer un fichier permanent de données biométriques qui ne serait activé que lors de périodes déterminées, dans des contextes prévus ou dans des zones particulièrement exposées.

● Compte tenu des risques que présente cette technologie pour les libertés publiques, la mission d'information ne préconise aucune évolution législative en la matière, même à titre expérimental

Comme nous l'avons expliqué plus haut, la reconnaissance biométrique soulève de nombreux problèmes de libertés publiques puisqu'elle **concerne des données sensibles, qu'elle est « sans contact » et potentiellement omniprésente, qu'elle représente un « potentiel de surveillance inédit » et qu'elle reste faillible**. Pour toutes ces raisons, la mission ne préconise aucune évolution législative en matière d'usage de la reconnaissance biométrique par les services de renseignement, même à titre expérimental.

D. LES FICHIERS : UN OUTIL STRATÉGIQUE DONT IL FAUT CLARIFIER LE RÉGIME JURIDIQUE

Les fichiers représentent un outil stratégique pour les services de renseignement puisqu'ils **permettent aux services de n'utiliser les techniques de renseignement qu'à titre subsidiaire et d'effectuer, en amont, un travail très utile aux enquêteurs**. Si chaque service de renseignement dispose de ses propres fichiers, il a bien sûr également la possibilité d'accéder à de très nombreux autres fichiers administratifs [(1)].

(1) Le foisonnement des fichiers est d'ailleurs assez problématique et peut parfois nuire à l'efficacité des services.

La loi du 24 juillet 2015 comporte plusieurs dispositions en matière d'utilisation des fichiers :

– le dernier alinéa de l'article 2, relatif au contentieux du droit d'accès aux traitements de données intéressant la sûreté de l'État ;

– l'article 16, sur le droit d'obtention d'informations de Tracfin auprès des entreprises de transport et des opérateurs de voyage ou de séjour ;

– l'article 19, qui crée un fichier judiciaire national automatisé des auteurs d'infractions terroristes ;

– l'article 20, relatif à la consultation du traitement d'antécédents judiciaires.

En outre, plusieurs questions relatives aux fichiers ont été soulevées dans le cadre des travaux de la mission d'information. Il s'agit en particulier des difficultés d'accès des services de renseignement à certains fichiers et de l'interconnexion des fichiers. Ces questions sont loin d'être neuves : elles ont déjà été abordées par MM. Jean-Jacques Urvoas et Patrice Verchère en 2013 (1) et plus récemment, par MM. Didier Paris et Pierre Morel-À-L'Huissier dans leur rapport du 17 octobre 2018 sur les fichiers mis à la disposition des forces de sécurité (2).

1. Le régime dérogatoire applicable aux fichiers des services de renseignement

a. Les fichiers de renseignement sont régis par des dispositions spécifiques de la loi du 6 janvier 1978 et font l'objet d'un droit d'accès indirect

● Un régime juridique dérogatoire défini au titre IV de la loi de 1978

Tous les services spécialisés de renseignement, au sens des articles L. 811-2 et R. 811-1 du code de la sécurité intérieure, mettent légalement en œuvre un ou plusieurs traitements de données aux fins de l'exercice de leurs activités. Tous ces traitements sont mentionnés à l'article 1er du décret n° 2007-914 du 15 mai 2007 modifié (3). Plusieurs services dits du second cercle, au sens des articles L. 811-4 et R. 811-2 du CSI, mettent également en œuvre des fichiers mentionnés au même article 1er du décret précité. Certains de ces services disposent par ailleurs de fichiers non mentionnés dans ce décret, qui leur permettent d'exercer leurs

---

(1) Rapport d'information n° 1022 du 14 mai 2013 sur l'évaluation du cadre juridique applicable aux services de renseignement.

(2) Cf. infra.

(3) Il s'agit du décret n° 2007-914 du 15 mai 2007 modifié 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. Le I de l'article 30 de la loi n° 78-17 correspond aujourd'hui au I de l'article 33 de la même loi. Ce décret cite également le fichier LEGATO de la Légion étrangère, le fichier des personnes recherchées (FPR) pour certaines fiches seulement, le fichier national de sécurité Schengen SNIS, avec les mêmes restrictions, et le traitement ACCReD pour les seules données intéressant la sûreté de l'État.

missions et qui poursuivent dès lors des finalités bien plus larges que le renseignement (1). Enfin, les services des premier et second cercles peuvent également être autorisés à accéder à certains autres fichiers, que d'autres services mettent en œuvre, notamment aux fins de défense et de la promotion des intérêts fondamentaux de la nation. C'est le cas, par exemple, de tous les services spécialisés de renseignement mais également des services du renseignement territorial ou de services de la direction des opérations et de l'emploi de la gendarmerie nationale, qui peuvent accéder aux données enregistrées dans le traitement des antécédents judiciaires (2).

Les fichiers exclusivement consacrés au renseignement ne relèvent pas du droit européen (3) – ni du Règlement général sur la protection des données, qui concerne uniquement le premier pilier du droit européen, ni de la directive « Police-Justice », qui concerne la matière pénale (4). Ils **relèvent d'une catégorie plus large, celle des fichiers intéressant la sûreté de l'État** et la défense régis par le **titre IV de la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978**. À ce titre, ils bénéficient de règles dérogatoires au cadre général applicable (cf. annexe n° 9). Ainsi, si la CNIL exerce un contrôle préalablement à l'adoption des textes portant création de ces fichiers – que ces textes créateurs soient publiés ou non –, elle n'exerce aucun contrôle *a posteriori* quant au respect de la légalité par les services qui gèrent ces fichiers.

● Un droit d'accès indirect par l'intermédiaire de la CNIL

Les administrés disposent d'un droit d'accès indirect à ces fichiers de renseignement, par l'intermédiaire de la CNIL (5). Ce droit indirect n'ouvre pas aux demandeurs un droit systématique à communication des données. Ces

---

(1) On peut par exemple citer le service central des courses et jeux (cf. arrêté du 8 novembre 2010) ou encore les traitements mis en œuvre par la direction centrale de la police aux frontières (par exemple, le traitement SETRADER).

(2) Cf. les articles L. 234-1 et suivants et R. 234-1 et suivants du code de la sécurité intérieure. L'article R. 234-2 prévoit ainsi que les services spécialisés de renseignement dont les agents peuvent accéder aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6 du code de procédure pénale sont la DGSE, la DRSD, la DRM, la DGSI, la DNRED et Tracfin.

(3) RGPD (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE) et Directive « Police-Justice » (Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil).

(4) La loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 comporte quatre titres bien distincts : le premier, consacré aux dispositions générales, le deuxième, qui transpose le RGPD, le troisième qui transpose la directive « Police-Justice » et le quatrième, consacré aux « fichiers intéressant la sûreté de l'État et la défense ». Cependant, certains fichiers sont mixtes et peuvent donc être régis par le titre III de la loi de 1978 (cf. annexe n° 9).

(5) Les personnels de la CNIL disposent déjà, lorsque l'exercice de leurs missions le justifie (en particulier en matière de droit d'accès indirect aux traitements de sécurité publique et de sûreté de l'État et en matière d'avis sur les projets de texte réglementaire relatifs à de tels traitements), des habilitations au secret de la défense nationale qui les autorisent à accéder aux informations nécessaires à cet exercice.

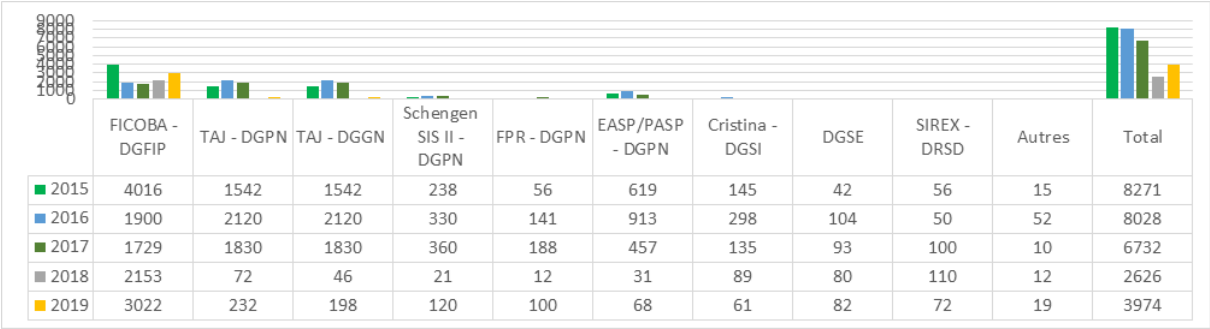
dernières ne peuvent être communiquées à la personne concernée qu'avec l'accord du responsable du fichier qui peut s'y opposer pour des motifs liés à la finalité du fichier – sûreté de l'État, défense. En cas de refus de communication, la CNIL indique à la personne concernée les voies de recours qui lui sont ouvertes pour contester cette décision.

L'exercice du droit d'accès indirect

L'article 118 de la loi du 6 janvier 1978 prévoit que, s'agissant des fichiers intéressant la sûreté de l'État et la défense, les demandes tendant à l'exercice du droit d'accès, de rectification et d'effacement sont adressées à la CNIL qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. La commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel.

L'article 119 de la loi de 1978 prévoit que par dérogation à l'article 118, lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire autorisant le traitement peut prévoir que les droits d'accès, de rectification et d'effacement peuvent être exercés par la personne concernée auprès du responsable de traitement directement saisi.

Le tableau ci-dessous, fourni à la mission d'information par la CNIL, présente les statistiques, par année et par fichier, relatives à l'exercice du droit d'accès indirect par les administrés. Il fait clairement apparaître que **l'essentiel des requêtes concerne le fichier national des comptes bancaires (FICOBA), très loin devant les fichiers des services de renseignement**.



	FICOBA - DGFIP	TAJ - DGPN	TAJ - DGGN	Schengen SIS II - DGPN	FPR - DGPN	EASP/PASP - DGPN	Cristina - DGSI	DGSE	SIREX - DRSD	Autres	Total
2015	4016	1542	1542	238	56	619	145	42	56	15	8271
2016	1900	2120	2120	330	141	913	298	104	50	52	8028
2017	1729	1830	1830	360	188	457	135	93	100	10	6732
2018	2153	72	46	21	12	31	89	80	110	12	2626
2019	3022	232	198	120	100	68	61	82	72	19	3974

En pratique, le système du droit d'accès indirect est évidemment indispensable à la préservation de l'efficacité des fichiers des services de renseignement.

b. Certains fichiers mixtes sont soumis au régime du droit d'accès direct mais ce droit peut faire l'objet de restrictions

Le refus de communication de données, par le ministère de l'intérieur par exemple, à une personne exerçant ses droits n'est pas limité aux cas où ces données intéresseraient la sûreté de l'État : **l'article 107 de la loi « Informatique**

et Libertés » prévoit la possibilité pour les responsables de traitement de **restreindre le droit d'accès direct, dès lors qu'une telle restriction « *constitue une mesure nécessaire et proportionnée dans une société démocratique* ».** Cet article énumère les motifs pouvant justifier un refus de communication de données : éviter de gêner des enquêtes ou de nuire à la prévention ou à la détection d'infractions pénales, protéger la sécurité publique ou la sécurité nationale, protéger les droits et libertés d'autrui. Ces restrictions d'accès doivent être prévues par l'acte instaurant le traitement. Un responsable de fichier peut ainsi limiter la communication des données contenues dans ledit fichier, voire ne pas communiquer ces informations. Il peut aussi refuser ou limiter le droit d'accès des administrés. Dans ce cas, les administrés ont la possibilité d'exercer leurs droits d'accès de manière indirecte, par l'intermédiaire de la CNIL, ou de former un recours juridictionnel.

Ces restrictions, prévues au titre III de la loi de 1978 (qui transpose la directive « police-justice »), **concernent les fichiers de sécurité publique** (notamment de prévention des infractions pénales) **mais aussi certains fichiers « mixtes »**, comportant à la fois des dispositions intéressant la sécurité publique et des dispositions relevant de missions de renseignement.

Dans la mesure où les responsables de certains fichiers, tels que le traitement PASP de la police nationale ou le traitement GIPASP de la gendarmerie, opposent systématiquement un refus d'accès direct – à raison, puisqu'il s'agit d'éviter la compromission des informations que contiennent ces fichiers –, la mission estime qu'il serait opportun que le pouvoir réglementaire prévoie explicitement, pour ces traitements, un régime d'accès indirect. Cela éviterait aux administrés de ne se tourner que dans un second temps vers la CNIL, une fois qu'ils se sont vu opposer un refus de communication. Selon les informations transmises à la mission, un projet de décret, en cours d'étude par la CNIL, devrait traiter ce problème.

c. La complexité du contentieux du droit d'accès aux fichiers intéressant la sûreté de l'État

● La problématique du contentieux des fichiers « partagés »

Comme on l'a vu dans la première partie, le dernier alinéa de l'article 2 de la loi du 24 juillet 2015, codifié à l'article L. 841-2 du code de la sécurité intérieure, définit les règles afférentes au contentieux du droit d'accès aux fichiers intéressant la sûreté de l'État. Interrogé par la mission d'information quant au bilan qu'il tirait de l'application de l'article L. 841-2 du code de la sécurité intérieure, le président de la formation spécialisée du Conseil d'État, M. Edmond Honorat, a présenté plusieurs observations.

Il a indiqué que dans sa rédaction actuelle, l'article L. 841-2 du code de la sécurité intérieure, qui définit la compétence de la formation spécialisée du Conseil d'État en matière de fichiers, **se réfère au contrôle de la mise en œuvre**

du seul article 118 (1) de la loi du 6 janvier 1978 relative à l'informatique et aux libertés. Or, cet article ne concerne que les fichiers, « intéressant la sûreté de l'État (2) et la défense », régis par le titre IV de la loi et soumis à un droit d'accès indirect via la CNIL.

L'article L. 841-2 exclut, en théorie, les **fichiers « partagés », qui relèvent désormais d'un droit d'accès direct** auprès du responsable du traitement avec recours facultatif devant la CNIL et, pour l'essentiel, du titre III de la loi – traitements à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Ces fichiers, qui sont en pratique ceux auxquels l'accès est le plus fréquemment demandé, sont réputés **comporter deux parties** : celle comprenant les données intéressant la sûreté de l'État ; celles comprenant les données d'un autre type. « *Ce découpage,* a priori *simple et logique, soulève pourtant plusieurs difficultés* » a souligné le président de la formation spécialisée. « *Et la pratique fait apparaître que le contrôle de l'accès à ce type de fichiers n'a pas été véritablement pensé et ne l'est peut-être toujours pas*. »

D'une part, le président de la formation spécialisée du Conseil d'État a indiqué qu'il n'était **pas toujours aisé de déterminer si des données intéressent ou non la sûreté de l'État**. Tracfin soutient notamment qu'il lui est très difficile en pratique de procéder à une telle détermination, les déclarations de soupçons que ce service enregistre et doit exploiter pouvant révéler de simples comportements délinquants comme des comportements susceptibles de porter atteinte à la sûreté de l'État. Ce service de renseignement réclame, en conséquence, que le contrôle de l'accès à la totalité du fichier STARTRAC soit soumis à la formation spécialisée du Conseil d'État.

D'autre part, **certaines des données de ces fichiers peuvent ne pas être communiquées en raison de leur sensibilité sans pour autant relever de la sûreté de l'État**. Il semble aussi que certains services refusent, en pratique, l'accès à toute donnée de manière à ne donner aucune indication, même indirecte, sur la nature de ces données. Or, le contrôle des refus ainsi opposés relève de juges différents : Conseil d'État, tribunal administratif de Paris, voire juge judiciaire pour tout ce qui a trait, par exemple, aux condamnations pénales. **Il en résulte parfois pour les demandeurs de grandes difficultés à déterminer le juge compétent et, pour les juridictions, des saisines concurrentes ou des saisines erronées qui compliquent la bonne gestion des dossiers.** Le Conseil d'État et le tribunal administratif ont mis au point des procédures d'information réciproque afin de permettre, si nécessaire, un ré-aiguillage des requêtes, mais cela ne suffit pas toujours à éliminer les requêtes inutiles.

---

(1) Cf. supra *le a) du 1 du D du présent I.*

(2) Cf. annexe n° 10.

● **La position de la mission d'information**

La mission d'information estime qu'il conviendrait de simplifier le droit applicable sur deux points et de :

– prévoir un **accès indirect aux fichiers auxquels une restriction au droit d'accès est systématiquement appliquée** (1), de sorte que les administrés saisissent la CNIL en premier, sans s'adresser d'abord au ministère de tutelle d'un responsable de fichier ;

– réviser les textes réglementaires applicables aux différents fichiers afin que ces textes **précisent systématiquement, pour chaque fichier, de quel titre de la loi de 1978 « Informatique et libertés » le fichier relève, comment s'exerce le droit d'accès des administrés et quelle juridiction est compétente** en cas de contentieux.

2. Le droit d'obtention d'informations de Tracfin auprès des entreprises de transport et des opérateurs de voyage ou de séjour

Autre disposition de la loi de 2015 intéressant les fichiers, l'article 16 (2) confie à Tracfin un **droit d'obtention d'informations auprès des entreprises de transport et des opérateurs de voyage ou de séjour** (identification des personnes, dates, heures et lieux de départ et d'arrivée, bagages et marchandises). En outre, il impose aux entreprises de transport public routier de personnes de recueillir l'identité des passagers des voyages internationaux dont la distance est supérieure à 250 kilomètres et de conserver cette information pendant un an. Enfin, cet article organise les **échanges d'information entre Tracfin et les autres services de renseignement**.

Lors de son audition par la mission d'information, la directrice de Tracfin, Mme Maryvonne Le Brignonen, a indiqué que Tracfin avait **utilisé son droit de communication, de la part de transporteurs aériens, des dossiers passagers (PNR) à 165 reprises en 2019**. Cette **disposition est très utile, selon elle, pour détecter des signaux faibles de radicalisation**, notamment lorsque quelqu'un se met à acheter beaucoup de billets d'avion et à beaucoup voyager.

La directrice de Tracfin a indiqué à la mission que son service n'utilisait pas la disposition lui permettant d'obtenir des informations de la part des opérateurs de voyage. En effet, à chaque fois qu'un nouvel acteur entre en jeu, un important travail de pédagogie doit être fait afin de garantir le respect de la confidentialité. En outre, Tracfin dispose déjà d'une importante matière première grâce au PNR.

---

(1) Tels que le PASP et le GIPASP.

(2) Codifié à l'article L1631-4 du code des transports et aux articles L. 561-26 et L. 561-29 du code monétaire et financier.

3. Le fichier judiciaire national automatisé des auteurs d'infractions terroristes : un nouvel outil utile et précis

a. Un nouvel instrument visant à prévenir la récidive et à faciliter la recherche d'auteurs d'infractions en lien avec le terrorisme

L'article 19 de la loi du 24 juillet 2015 crée, au sein d'une nouvelle section du titre XV du livre IV du code de procédure pénale, un fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT) dans le but de doter les services chargés de la lutte contre le terrorisme d'un outil permettant de **prévenir la récidive et de faciliter la recherche d'auteurs d'infractions en lien avec le terrorisme**. Ces dispositions sont inspirées de celles applicables au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV).

Le FIJAIT **recense les personnes majeures ou mineures condamnées pour certaines infractions terroristes**. Il peut s'agir d'actes de terrorisme directs : atteinte à la vie en relation avec un projet terroriste, enlèvement et séquestration en relation avec un projet terroriste, détournement de moyen de transport en relation avec un projet terroriste. Il peut aussi s'agir d'infractions visant à préparer ou à financer un acte terroriste : faux et usage de faux documents publics en relation avec un projet terroriste, recel de malfaiteur terroriste, blanchiment en relation avec un projet terroriste. Il peut enfin s'agir d'infractions sanctionnant un comportement qui laisse penser que l'individu est susceptible de commettre un acte terroriste : association de malfaiteurs terroristes, entreprise terroriste individuelle, sortie du territoire malgré une interdiction quand il existe des raisons sérieuses de penser que ce voyage vise à participer à des activités terroristes.

Pour être inscrit au FIJAIT, il faut avoir **fait l'objet soit d'une condamnation**, même non définitive, y compris en cas de dispense de peine ou d'ajournement de la peine ; soit d'une **décision d'irresponsabilité pénale pour cause de trouble mental** ; soit d'une **mise en examen**, lorsque le juge d'instruction a ordonné l'inscription de la décision dans le fichier.

La personne inscrite au FIJAIT est informée de son inscription, soit en personne, soit par courrier recommandé à la dernière adresse déclarée, soit avec l'intervention de la police ou de la gendarmerie. Si la personne concernée est un majeur protégé, son représentant légal est informé.

L'inscription est automatique en cas de condamnation. Le tribunal peut toutefois décider de ne pas inscrire le condamné au FIJAIT en motivant spécialement sa décision. Dans tous les autres cas, elle n'est pas automatique : elle doit être indiquée dans la décision.

Toute personne inscrite au FIJAIT est soumise aux obligations suivantes :

– **justifier son adresse**, une première fois après avoir été informée de son inscription au fichier, puis **tous les trois mois** ;

– **déclarer tout changement d'adresse, dans un délai de quinze jours** au plus tard après ce changement ;

– **déclarer tout déplacement à l'étranger quinze jours à l'avance au plus tard** et **tout déplacement en France quinze jours à l'avance** pour les personnes résidant à l'étranger.

Ces obligations s'appliquent pour une **durée de dix ans** si la personne est majeure et cinq ans si elle est mineure.

Les données enregistrées dans le fichier sont :

– l'identité de la personne (nom, prénom, sexe, date et lieu de naissance, nationalité, filiation, adresses successives et dates correspondantes) ;

– la nature et la date de la décision ayant conduit à l'inscription (tribunal, nature de l'infraction, date et lieu des faits, peine prononcée etc.) ;

– des informations telles que les dates de justification d'adresse, la périodicité de l'obligation de présentation *etc*.

Le fait pour les personnes tenues à ces obligations de ne pas les respecter est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Le FIJAIT peut être consulté par les autorités judiciaires, les officiers de police judiciaire, les préfets et certaines administrations de l'État pour le recrutement, l'agrément ou l'habilitation de personnels intervenant dans certaines activités ou exerçant des professions sensibles ou exposées. Les préfets peuvent également transmettre les informations contenues dans ce fichier aux maires et aux présidents d'intercommunalités, de conseils départementaux et de conseils régionaux pour les mêmes besoins en matière de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation.

Les informations inscrites au FIJAIT sont **conservées pendant vingt ans**. Si l'inscription concerne une violation d'une interdiction de sortie du territoire ou du contrôle administratif suite à un retour en France, elles sont conservées cinq ans. Ce délai court à compter du prononcé de la décision. Si la personne est emprisonnée au moment du prononcé de la décision, le délai ne commence à courir qu'à partir de sa libération. Les informations peuvent aussi être retirées plus tôt si la personne inscrite décède ou n'est finalement pas déclarée coupable ou si le procureur de la République ordonne l'effacement.

L'article 706-25-14 du code de procédure pénale renvoie à un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des

libertés, la détermination des modalités d'application du FIJAIT. Le décret n° 2015-1840 du 29 décembre 2015 modifiant le code de procédure pénale et relatif au fichier judiciaire national automatisé des auteurs d'infractions terroristes précise la nature et les modalités d'enregistrement des données qui sont inscrites au FIJAIT et les autorités compétentes à cette fin. Il détaille les conditions dans lesquelles il est procédé à la notification de l'inscription au FIJAIT et décrit précisément les modalités d'exécution des obligations imposées aux personnes inscrites au fichier. Il dresse la liste des autorités, agents ou services qui peuvent interroger le fichier. Il précise la procédure applicable pour l'effacement des données, en particulier les délais dans lesquels les instances judiciaires saisies doivent répondre aux demandes.

b. ***Un outil réactif, précis et fiable***

Les interlocuteurs de la mission d'information ont qualifié ce fichier d'« *outil réactif, précis et fiable* » pour la prévention de la récidive car il **permet une localisation rapide des individus inscrits au fichier**.

Ce fichier a été ouvert depuis le 1er juillet 2016 et les enregistrements y ont crû lentement, certes, mais régulièrement. Au 31 janvier 2020, 1 230 personnes étaient inscrites au fichier, au titre de 1 405 décisions, une même personne pouvant faire l'objet de plusieurs décisions d'inscription. Le FIJAIT est beaucoup consulté, par de nombreuses administrations : il a en effet donné lieu à **565 000 consultations, dont la moitié provient de l'administration pénitentiaire**. Le fichier est également consulté par **l'éducation nationale – à hauteur de 150 000 consultations** –, par le renseignement intérieur et par les préfectures, notamment préalablement à certains recrutements dans la fonction publique, dans des structures classées Seveso d'importance vitale ou dans les transports.

En cas de violation des obligations imposées aux personnes inscrites au FIJAIT, une **alerte automatisée se déclenche**. Il revient au ministère de la justice de gérer toutes ces alertes. À titre d'illustration, 140 alertes ont été déclenchées en janvier 2020, dont quarante-six pour défaut de justification d'adresse dans les délais. Vingt-deux alertes ont fait l'objet d'une régularisation dans le même mois.

Le FIJAIT étant un fichier de surveillance, il permet la localisation rapide des personnes qui y sont inscrites et de contrôler que ces personnes respectent leurs obligations de signalement de leur localisation et de signalement de déplacement. **Le FIJAIT s'articule ainsi avec le fichier des personnes recherchées (FPR)**, une interconnexion des deux fichiers étant prévue.

4. La consultation du traitement d'antécédents judiciaires

En application de l'article 20 [(1)] de la loi du 24 juillet 2015, les agents individuellement désignés et habilités des services du premier et du second cercles déterminés par décret, dans la stricte limite de leurs attributions et pour les **seuls besoins liés à la protection des intérêts mentionnés aux 1° (indépendance nationale, intégrité du territoire et défense nationale), 4° (prévention du terrorisme) et 5° (prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique)** de l'article L. 811-3 du code de la sécurité intérieure, peuvent avoir accès aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6 du code de procédure pénale (fichier TAJ), 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**.

Le traitement d'antécédents judiciaires (TAJ)

Le traitement d'antécédents judiciaires (TAJ) est utilisé, en application des articles 230-6 à 230-11 du code de procédure pénale, dans le cadre des enquêtes judiciaires afin de faciliter la constatation des infractions, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il est également utilisé dans le cadre d'enquêtes administratives (comme les enquêtes préalables à l'exercice de certains emplois relevant du domaine de la sécurité ou de la défense). Il est alimenté par la police et la gendarmerie. Le TAJ est géré par la direction centrale de la police judiciaire.

Sont enregistrées dans le TAJ les informations relatives :

– aux personnes mises en cause, c'est-à-dire à l'encontre desquelles il y a des indices graves et concordants d'avoir participé soit à un crime, soit à un délit, soit à certaines contraventions limitativement énumérées par la loi ;

– aux victimes de ces infractions ;

– aux personnes faisant l'objet d'une enquête pour recherche des causes de la mort ou de la disparition. En application de l'article R. 40-26 du code de procédure pénale, les données concernant l'état civil des personnes mises en cause, leur signalement et leur photographie, ainsi que les données relatives aux faits qui font l'objet de l'enquête, sont enregistrés dans le traitement.

Selon les informations recueillies par la mission d'information lors de ses auditions, cette disposition constitue un atout pour les services de renseignement : ainsi, par exemple, la directrice de Tracfin a indiqué que ce service utilisait le traitement d'antécédents judiciaires dans le cadre d'enquêtes financières et que le fait de **connaître le profil pénal d'une personne permettait de « colorer » une enquête qui était d'abord financière**. De son côté, la direction générale de la police nationale a indiqué que les agents du SCRT accédaient au TAJ principalement dans le cadre des finalités 4 (prévention du terrorisme) et 5

(1) Qui a créé un article L. 234-4 au sein du code de la sécurité intérieure.

(prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, des violences collectives de nature à porter gravement atteinte à la paix publique). La mission d'information juge donc cette disposition très utile.

Dans leur rapport d'information précité, MM. Didier Paris et Pierre Morel-À-L'Huissier (1) considèrent qu'il pourrait être pertinent d'étendre l'accès des services de renseignement aux données du TAJ relatives aux victimes. **La mission d'information ne partage pas ce point de vue.** En effet, plusieurs dizaines de millions de personnes sont inscrites au TAJ (2) en tant que victimes et il n'est pas démontré, à ce stade, qu'un accès des services de renseignement à ces informations soit nécessaire.

5. L'inaccessibilité de certains fichiers pourtant nécessaires aux services

En dehors des dispositions précitées, qui relèvent de la loi du 24 juillet 2015, deux questions relatives aux fichiers ont été abordées lors des travaux de la mission d'information : d'une part, le problème du manque d'accès de certains services à des fichiers dont ils ont pourtant besoin ; d'autre part, la question de l'interconnexion des fichiers.

Ainsi que le soulignent MM. Didier Paris et Pierre Morel-À-L'Huissier dans leur rapport d'information précité (3), « *les nouvelles menaces pesant sur la sécurité publique engendrent pour les services de nouveaux besoins en termes d'accès aux fichiers, d'interconnexions et de fiabilisation des identités des personnes inscrites. Il convient d'y répondre, tout comme à la montée en puissance des enquêtes administratives préalables à l'exercice de certains emplois sensibles.* » La mission d'information souscrit à ce constat, la question ayant été abordée à plusieurs reprises par les services dans le cadre de ses travaux.

Le problème du manque d'accès aux fichiers a notamment été abordé par le directeur du renseignement et de la sécurité de la défense, le général Éric Bucquet. La **direction du renseignement et de la sécurité de la défense** (DRSD) est particulièrement **sensible à la question de l'accès aux fichiers** dans la mesure où elle est notamment chargée de mener des **enquêtes administratives à des fins de protection du secret de la défense nationale** et d'émettre des avis concernant les **habilitations « confidentiel défense », « secret défense » et « très secret défense »**. Le général Bucquet a indiqué à la mission d'information que le **fichier ACCReD** (4) ne lui était pas accessible pour l'instant alors qu'il lui serait fort utile puisque le travail d'analyse de la DRSD consiste à aller interroger des fichiers pour savoir si tel nom y est enregistré ou pas. Le directeur de la DRSD a expliqué

---

(1) Dans leur rapport d'information n° 15 n° 1335 enregistré à la présidence de l'Assemblée nationale le 17 octobre 2018, sur les fichiers mis à la disposition des forces de sécurité, p. 40.

(2) Sur son site, la CNIL indique que 87 millions d'affaires sont répertoriées dans le TAJ et que le TAJ comporte plus de 18,9 millions de fiches de personnes mises en cause.

(3) Ibid.*, p. 8.*

(4) Cf. annexe n° 8.

que 50 % des dossiers traités par sa direction étaient « propres » et que leur traitement ne devrait donc prendre qu'une semaine maximum au lieu des quatre mois actuellement observés. Le général Bucquet a toutefois indiqué qu'à la suite d'un rapport de l'inspection des services de renseignement faisant état de ce problème, le Premier ministre avait demandé que tous les services de renseignement puissent accéder à ACCReD, ce qui suppose une évolution d'ordre réglementaire. Dans un souci d'efficacité de la DRSD et donc de sécurité nationale, la mission d'information souscrit pleinement à la demande d'évolution formulée par le général Bucquet.

À la suite de ses travaux, la mission suggère également que le fichier national des détenus, qui est une extraction du traitement GENESIS de l'administration pénitentiaire et qui permet aux officiers de police judiciaire de la police et de la gendarmerie d'avoir accès à certaines catégories de données collectées dans ce traitement, soit utilisable par les services de renseignement de la direction générale de la police nationale.

La mission d'information rappelle enfin que MM. Didier Paris et Pierre Morel-À-L'Huissier préconisent, dans leur rapport d'information précité (1), un accès des services de renseignement au PASP et au GIPASP du ministère de l'intérieur. Ils insistent (2) en effet sur la nécessité d'« *élargir le champ des données auxquelles les services de renseignement spécialisés ont accès, notamment dans le cadre de leurs missions de prévention du terrorisme.* » Les membres de la mission d'information souscrivent entièrement à la proposition de leurs collègues s'agissant des fichiers du ministère de l'intérieur. **Il est en effet assez étonnant que des services tels que la DGSI n'aient pas, en droit, accès aux fichiers de la police et de la gendarmerie alors même que ces services du ministère de l'intérieur contribuent aux mêmes missions. Il conviendrait donc de faire évoluer l'état du droit en modifiant les articles R. 236-16 et R. 236-26 du code de la sécurité intérieure, relatifs, respectivement, au PASP et au GIPASP.**

Plus généralement, les membres de la mission d'information sont ouverts à un élargissement de l'accès des services de renseignement aux fichiers existants, compte tenu à la fois du caractère stratégique de ces fichiers pour ces services et de la persistance, à un haut niveau, des menaces qui pèsent sur la sécurité nationale, à commencer par la menace terroriste.

6. L'interconnexion des fichiers

La question de l'interconnexion des fichiers **n'est pas neuve**. En 2013 déjà, les rapporteurs Jean-Jacques Urvoas et Patrice Verchère, dans leur rapport d'information précité, soulignaient l'importance capitale de permettre et de favoriser cette interconnexion : les auteurs du rapport ont estimé que si le

(1) P. 40

(2) P. 68 du rapport précité.

recoupement manuel des informations était « *aussi légal que précieux* », il était aussi très fastidieux et très prenant. Ils ont rappelé à quel point une telle interconnexion pouvait s'avérer indispensable pour **détecter les « signaux faibles »** (1). Ils ont également souligné l'intérêt que pourrait présenter le croisement des fichiers policiers et financiers. « *À l'heure où les nouvelles technologies facilitent grandement les entreprises terroristes,* estimèrent MM. Jean-Jacques Urvoas et Patrice Verchère, *il semble contre-productif de se priver d'un tel outil dont l'exploitation peut aisément s'effectuer si des précautions sont prises en matière de contrôle de l'accès et de l'utilisation de ces fichiers, dans le respect des droits et libertés.* » Les membres de la mission d'information ne peuvent que souscrire à ces propos, compte tenu de l'intérêt stratégique des fichiers dans un contexte sécuritaire qui s'est fortement aggravé depuis 2015.

De la même manière, MM. Didier Paris et Pierre Morel-À-L'Huissier soulignent dans leur rapport d'information précité (2) qu'« *il est nécessaire de développer les interconnexions entre fichiers pour remédier à leur cloisonnement* ».

a. ***L'interconnexion : définition et objectifs***

La notion d'interconnexion recouvre une **large palette de fonctionnalités techniques**. La CNIL la définit comme « *la mise en œuvre de moyens techniques permettant la* ***mise en relation automatisée d'informations*** *provenant de fichiers ou de traitements qui étaient au préalable distincts, soit d'un point de vue technique, soit d'un point de vue organisationnel* ». Le Conseil d'État a jugé qu'une « *interconnexion doit être regardée comme l'objet même d'un traitement qui permet d'accéder à, d'exploiter et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu* ». Au sens strict, l'interconnexion est ainsi un sous-ensemble des mises en relation de fichiers.

Comme le soulignent MM. Didier Paris et Pierre Morel-À-L'Huissier (3), « *les objectifs des interconnexions sont multiples :*

– ***l'échange d'informations automatique*** *entre différents services ;*

– *la* ***mutualisation*** *de l'alimentation de différents fichiers, ce qui permet des gains d'efficacité et renforce la fiabilité des données ;*

– *la* ***mise à jour*** *automatique des données ;*

– *la* ***consultation simultanée*** *de plusieurs fichiers, avec un champ plus ou moins large des informations consultées ;*

---

(1) Individus dont les agissements, pris séparément, ne révèlent pas de danger potentiel.

(2) P. 68.

(3) Rapport précité, p. 42.

– le ***recoupement*** *des informations sur une même personne issue de différents fichiers.* »

Les deux députés indiquaient en 2018 que « *le développement des interconnexions est une demande forte des services pour renforcer la cohérence des fichiers et remédier à leur cloisonnement* ». En 2020, la mission d'information confirme ce constat.

Dans le droit en vigueur, plusieurs fichiers sont déjà interconnectés, tels que le système d'information Schengen (SIS), qui est interconnecté pour alimentation ou consultation à une douzaine de fichiers nationaux.

b. ***La nécessité d'assortir les interconnexions de fichiers de certaines garanties***

Interrogée par la mission d'information, la CNIL a souligné qu'elle n'était aucunement défavorable par principe à la mise en application d'interconnexions, « *dès lors que celles-ci sont* ***justifiées par la finalité poursuivie*** *et qu'elles interviennent dans des conditions de nature à assurer une* ***protection suffisante des données à caractère personnel*** ». Dans la sphère policière, judiciaire ou de sécurité, la CNIL s'est ainsi prononcée favorablement à la mise en œuvre de nombreuses interconnexions de fichiers nécessaires aux besoins des responsables de traitement.

● L'absence de formalité nécessaire à chaque opération d'interconnexion

Selon la CNIL, « *si une interconnexion peut être considérée comme un traitement à part entière, qui doit dès lors respecter l'ensemble des conditions prévues par les textes, cela ne signifie pas qu'une formalité particulière doit être effectuée pour chaque opération concrète d'interconnexion de fichiers : les* ***interconnexions peuvent être prévues à titre général*** *dans les textes réglementaires qui encadrent les traitements en cause. Elles ne doivent en tout état de cause pas faire l'objet d'une autorisation de la CNIL* ». Dans sa version en vigueur avant l'adoption du « paquet européen » en matière de protection des données [(1)] et sa transposition en droit national [(2)], la loi du 6 janvier 1978 modifiée prévoyait en effet une autorisation de la CNIL pour certaines

(1) RGPD (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE) et directive « Police-Justice » (directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil).

(2) Par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

interconnexions, mais cette formalité n'est plus applicable depuis juin 2018. Surtout, dans l'état du droit antérieur comme actuel, une interconnexion ne doit pas nécessairement faire l'objet d'une autorisation de la CNIL [(1)] dès lors que les traitements concernés sont régis par des arrêtés ou des décrets en Conseil d'État, pris après avis de la CNIL, qui sont par nature des textes normatifs supérieurs, et que ces textes en autorisent la mise en œuvre. En revanche, la CNIL s'est prononcée, dans le cadre de son avis sur le projet de texte qui lui était soumis, sur le principe comme sur les modalités de chacune d'entre elles.

● Plusieurs conditions formelles à remplir en cas d'interconnexion

Pour qu'une interconnexion entre fichiers de services de renseignement soit effectuée, les conditions formelles suivantes doivent être remplies :

– les **agents des autres services que ceux qui mettent en œuvre le traitement concerné doivent être mentionnés** dans les dispositions relatives aux destinataires du traitement (personnes habilitées à accéder ou à prendre connaissance des données qui y sont enregistrées) ;

– **l'interconnexion doit également être mentionnée**, dès lors qu'il s'agit de l'un des objets mêmes du traitement en cause, dans le texte réglementaire qui régit ledit traitement ;

– l'interconnexion et ses modalités exactes de mise en œuvre (finalités, données concernées, mesures de sécurité appliquées *etc*.) doivent être **portées à la connaissance de la CNIL** dans le cadre du dossier de saisine relative à la modification de l'arrêté ou du décret en Conseil d'État concerné afin que la commission puisse rendre un avis éclairé sur la modification envisagée.

● Des conditions de fond à respecter

Des conditions de fond doivent également être respectées, comme pour tout traitement mis en œuvre :

– l'interconnexion doit être **justifiée au regard des besoins spécifiques** des services ou de circonstances particulières ;

– elle ne doit **pas conduire à détourner les finalités** des traitements concernés ;

– elle doit être **limitée**, s'agissant des données concernées ou des destinataires de celles-ci, **à ce qui est nécessaire à l'atteinte des objectifs** poursuivis ;

---

(1) Ainsi, par exemple, n'ont pas fait l'objet d'une autorisation de la CNIL, les interconnexions des logiciels de rédaction des procédures de police et de gendarmerie (LRPPN et LRPGN) avec Cassiopée, du traitement iGAV (gestion des gardes à vues) avec le traitement LRPPN, du FOVeS avec le traitement API-PNR France, du FIJAIT et du FAED avec CASSIOPEE, du traitement SETRADER avec le FPR et le système d'information Schengen (SIS).

– enfin, elle doit être entourée de toutes les **mesures de sécurité nécessaires**.

La CNIL considère donc qu'il serait possible d'**encadrer l'interconnexion par voie réglementaire**, en modifiant les textes régissant les fichiers de renseignement, **tout en maintenant le cadre législatif actuel**. Elle ajoute que « *sous réserve d'une appréciation par la CNIL des cas d'espèce qui lui seraient soumis, l'élargissement des interconnexions actuellement mises en œuvre à de nouveaux fichiers ou de nouveaux services ne soulève pas de difficultés de principe, dès lors qu'on exclut toute interconnexion généralisée de tous les fichiers de renseignement* ».

● Les conditions nécessaires à la mise en œuvre d'interfaces « hit/no hit »

La création d'**interfaces** permettant la consultation automatique et simultanée de plusieurs fichiers de renseignement aux seules fins **de vérifier si l'identité de la personne concernée y est enregistrée** (1) – interfaces qui **fonctionneraient comme des moteurs de recherche** à partir de la saisie d'une identité ou d'un identifiant technique commun – peut constituer une **réponse adaptée à la nécessité d'assurer une meilleure mutualisation des renseignements** à la disposition des services.

Une telle interface existe déjà, depuis 2017, dans le cadre des enquêtes administratives et permet notamment la consultation automatique ou l'interrogation de nombreux fichiers mis en œuvre dans le cadre du renseignement. Comme nous le rappelons en annexe n° 8, le **traitement ACCReD** permet l'interrogation du FSPRT, de CRISTINA, de GESTEREXT, de SIREX et du fichier de la DGSE. Dans son avis sur le texte portant création du traitement, la CNIL a indiqué : « *Cette consultation automatique, qui constitue l'objet même dudit traitement et doit dès lors être regardée comme une interconnexion, apparaît justifiée à la commission au regard de la nécessité de prendre en charge un volume important d'enquêtes et de procéder à la consultation simultanée de multiples traitements* ». En outre, les **modalités d'accès aux informations enregistrées** ou issues des traitements que le dispositif ACCReD permet « d'interfacer » sont **fortement dégradées** s'agissant des fichiers relevant des services de renseignement : si le dispositif permet ainsi d'accéder directement aux autres traitements, aux fins de vérifier si l'identité de la personne concernée y est enregistrée, il permet **uniquement d'adresser automatiquement une liste de personnes aux services concernés qui vérifient ensuite manuellement** si elles figurent dans les traitements qu'ils gèrent. La CNIL estime que « *l'absence de mutualisation ou d'accès direct à certaines informations détenues par les services spécialisés de renseignement résulte donc*

(1) Comme le suggèrent Didier Paris et Pierre Morel-À-L'Huissier, une étape supplémentaire pourrait consister à instaurer un système d'alerte de présence au sein d'autres fichiers. À la différence des interfaces hit/no hit qui nécessitent d'introduire une requête, un système d'alerte se déclencherait automatiquement à chaque fois qu'une inscription sur un fichier trouve écho sur un autre fichier.

en l'espèce uniquement de la volonté du pouvoir réglementaire et des services eux-mêmes, et aucunement d'un quelconque obstacle juridique ou lié au positionnement de la CNIL ».

Cette **fonctionnalité de criblage** est déjà utilisée aussi dans le cadre du système API-PNR (1) mis en œuvre depuis 2014. Un tel dispositif présente des intérêts opérationnels évidents et importants : l'**automatisation des consultations et interconnexions facilite et accélère les échanges d'informations nécessaires** à l'exercice de certaines missions des services de renseignement.

Le criblage permet en outre la **minimisation des données transmises**, réduites à la seule existence ou non des personnes concernées dans les traitements consultés et, le cas échéant, aux motifs pour lesquels ces personnes y sont recensées. Il contribue également au respect du **principe d'exactitude des données** : il peut permettre de ne pas conserver dans un dispositif certaines données, issues d'autres traitements, qui peuvent être mises à jour dans ces fichiers « sources » et se révéler dès lors inexactes ou périmées si elles étaient maintenues dans le dispositif sans bénéficier de cette mise à jour. Le criblage peut enfin permettre de limiter la conservation de données à la seule durée nécessaire à l'atteinte de l'objectif poursuivi par de telles interconnexions.

Ces fonctionnalités doivent néanmoins s'accompagner d'au moins trois garanties.

Premièrement, ces dispositifs doivent être **circonscrits dans leur périmètre, aux fins de respecter les exigences de finalité, de nécessité et de proportionnalité** (2) : seuls les croisements automatiques de fichiers nécessaires

---

(1) Il s'agit d'un fichier de contrôle des déplacements aériens. Utilisé notamment pour la lutte contre le terrorisme ou le trafic de drogues, il contient deux types d'informations : d'une part, les données API (Advanced passenger informations ou renseignements préalables sur les voyageurs), liées à l'enregistrement des passagers provenant du passeport ou d'un autre document de voyage et des informations générales concernant le vol ; d'autre part, les données PNR (Passenger Name Record ou dossier passager), liées à la réservation et contenues dans les dossiers créés par les compagnies aériennes pour chaque vol. Elles permettent d'identifier chaque passager et d'avoir accès à tous les renseignements concernant son voyage : vols d'aller et de retour, correspondances éventuelles, moyens de paiement utilisés, services particuliers souhaités à bord, etc. Le système API-PNR est géré par un service spécifique, l'Unité Information Passagers (UIP), rattachée au ministère chargé des douanes. Il peut être consulté par les services de police, de gendarmerie et des douanes, ainsi que par les services de sécurité et de renseignement spécialisés. Le système API et PNR s'applique aux vols à destination et en provenance de pays étrangers. Il ne concerne pas les vols reliant deux aéroports de France métropolitaine.

(2) Par exemple, dans le cadre du traitement ACCReD, la CNIL avait souligné que le dispositif était utilisé aux fins d'enquêtes particulièrement nombreuses, très diverses et ne présentant pas toutes le même degré de sensibilité (nombreuses décisions de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation) et que les traitements FSPRT, GESTEREXT et CRISTINA, particulièrement sensibles et intéressant la sûreté de l'État, ne devaient dès lors pas pouvoir être systématiquement consultés, cette consultation devant être réservée aux seules enquêtes soulevant des enjeux en matière de sûreté de l'État. De même, s'agissant par exemple du FPR, divisé en sous-fichiers regroupant les personnes inscrites en fonction du fondement juridique de la recherche (motifs judiciaires et administratifs très divers), elle a estimé que la consultation effectuée devait être limitée, dans le cadre du dispositif relatif aux grands événements, aux seuls sous-fichiers susceptibles de contenir des informations pertinentes au regard de l'objectif de prévention des atteintes à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'État.

doivent être mis en œuvre, au regard de finalités précisément définies. Les **accès** qu'ils permettent doivent être limités aux **seuls services concourant à cette finalité**. Ces interfaces doivent enfin permettre la consultation automatique des seuls fichiers pertinents au regard de la finalité précisément poursuivie et, au sein de ces fichiers, des seules données pertinentes.

Deuxièmement, **aucune décision juridique ou affectant sensiblement les personnes ne doit être exclusivement fondée sur un tel dispositif**. Il est impératif qu'aucune décision ne soit prise sur le fondement de la seule inscription dans un des fichiers ainsi automatiquement consultés et que des vérifications complémentaires soient réalisées avant d'en tirer des conséquences affectant les personnes concernées, vérifications qui ne sauraient se réduire à la connaissance des motifs de cette inscription et des données précisément enregistrées dans le traitement en cause. En effet, les données enregistrées dans les traitements consultés automatiquement précités sont susceptibles, pour certaines, de résulter d'éléments déclaratifs et pourraient en tout état de cause être erronées ou ne pas avoir fait l'objet d'une mise à jour récente (1).

Troisièmement, **des mesures de sécurité rigoureuses doivent encadrer ces mises en relations et interconnexions**. La sécurité des dispositifs reposant sur une interface « *hit*/*no hit* » (2) doit faire l'objet d'une attention toute particulière, du simple fait de la **mise en place de liaisons informatiques qui augmentent notamment le risque d'interceptions ou d'attaques des données** lors des transmissions. Ces mesures doivent en particulier concerner la confidentialité des transmissions (chiffrement des transferts de données), la traçabilité des consultations automatiques, l'habilitation des personnels autorisés à accéder aux données, *etc*.

Dès lors que tels dispositifs d'interfaces « *hit*/*no hit* » respectent les exigences élémentaires précitées – de nécessité et de proportionnalité – et que de telles garanties adaptées sont prévues, leur élargissement à de nouvelles fins, de nouveaux fichiers ou de nouveaux services, relevant de la politique publique de renseignement, ne soulève pas de difficulté de principe, pour la CNIL, au regard du cadre juridique fixé par la loi relative à l'informatique et aux libertés.

● La possibilité d'aller au-delà des fonctions de criblage à condition de prévoir des garanties spécifiques

De telles interconnexions pourraient tout à fait, sous les mêmes réserves et notamment la prévision de garanties spécifiques adaptées, être élargies à d'autres fonctionnalités et ne pas se réduire au criblage, sans pour autant aboutir à l'interconnexion généralisée de tous les fichiers de renseignement, qui serait par

---

(1) La CNIL a également rappelé ces exigences dans le cadre du traitement ACCReD, compte tenu à la fois de la nature des fichiers automatiquement consultés (par exemple, le FSPRT ou le TAJ) et des préjudices importants qui peuvent découler de l'adoption d'un avis ou d'une décision défavorable infondés.

(2) C'est-à-dire une interface permettant la consultation automatique et simultanée de plusieurs fichiers de renseignement aux seules fins de vérifier si l'identité de la personne concernée y est enregistrée.

nature disproportionnée en l'absence des garanties précitées. **Sous réserve d'une appréciation par la CNIL des cas d'espèce qui lui seraient soumis et si les réticences des services de renseignement eux-mêmes sont levées à l'égard du partage des informations dont ils disposent, des interconnexions plus approfondies peuvent être envisagées**. Le partage d'informations permis par de telles interconnexions pourrait ainsi **couvrir plus de données que la seule existence ou non d'une ou plusieurs personnes dans les traitements consultés, voire l'ensemble des données** qui leur sont relatives et qui sont enregistrées dans ces traitements. Dans un tel cas, des garanties devraient être apportées : **caractère ponctuel des opérations d'interconnexions réalisées, motivation expresse, suppression des éléments non pertinents, durées de conservation limitées**, *etc*.

La mission d'information formule une proposition relative à l'interconnexion des fichiers au V de la troisième partie du rapport.

II. LA JURISPRUDENCE EUROPÉENNE A UNE PORTÉE MAJEURE SUR LES LÉGISLATIONS NATIONALES ET SUR L'ACTIVITÉ DES SERVICES DE RENSEIGNEMENT

Parallèlement à l'enjeu que représentent, pour les services de renseignement, les évolutions technologiques décrites *supra*, le droit français du renseignement doit tenir compte d'un second enjeu : celui de la jurisprudence européenne. Il convient de distinguer, au sein de cet ensemble, la jurisprudence de la Cour européenne des droits de l'homme (CEDH) de celle de la Cour de justice de l'Union européenne (CJUE), tant leurs effets sur le droit du renseignement diffèrent.

De fait, s'il est indéniable que la jurisprudence de la CEDH fait évoluer au fur et à mesure le droit des États européens dans un sens protecteur du droit au respect de la vie privée, cette jurisprudence sur la « surveillance de masse », élaborée par étapes au cours d'une quarantaine d'années, semble prendre en compte, par-delà les différences d'organisation nationales, les contraintes opérationnelles qui pèsent sur les autorités étatiques, et en particulier sur leurs services de renseignement. C'est le sentiment qu'ont eu les membres de la mission d'information lors des auditions qu'ils ont menées auprès des différents chefs de service impliqués dans la politique publique du renseignement (**A**).

En revanche, la jurisprudence récente de la Cour de justice de l'Union européenne – juridiction dont la protection des droits de l'homme ne semble pas être le « cœur de métier » – inquiète bien davantage les membres de la mission d'information. Nous n'hésiterons pas, et nous expliquerons pourquoi plus avant, à qualifier la décision *Tele2 Sverige AB* rendue par la CJUE le 21 décembre 2016 de véritable *hold-up* jurisprudentiel et ses conséquences possibles en droit interne, d'épée de Damoclès pour les services de renseignement. De fait, cette décision, si elle devait être appliquée à la lettre par les autorités nationales, entraînerait une remise en cause de l'usage de toutes les techniques de recueil de renseignement qui ne sont pas mises en œuvre en temps réel. C'est dire l'impact de ce droit

supranational sur notre droit français du renseignement, dont nous avons pourtant montré le caractère équilibré en première partie de ce rapport (**B**).

A. LA JURISPRUDENCE DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME EN MATIÈRE DE SURVEILLANCE DE MASSE, CADRE CONVENTIONNEL DU DROIT FRANÇAIS DU RENSEIGNEMENT

La jurisprudence de la CEDH a joué un rôle d'aiguillon dans l'émergence, en France comme sur l'ensemble du continent européen, d'un droit encadrant l'activité des services de renseignement. M. Olivier Forcade, professeur des universités [(1)], le souligne : alors que le renseignement était un domaine traditionnellement resté dans le secret et par conséquent à l'écart de toute institutionnalisation, à partir des années 1989-1990, « *s'opère un tournant par l'affirmation d'un encadrement des activités secrètes des États occidentaux* (…). *Par ses arrêts, la Cour européenne des droits de l'homme a conduit les États européens à ajuster le droit à certaines de leurs pratiques secrètes, toujours justifiées par la sécurité nationale, la lutte contre les ingérences étrangères et les atteintes à la sûreté de l'État. C'est pourquoi l'encadrement juridique des activités secrètes touchant à la sécurité des États et des citoyens a progressé rapidement, avec des rythmes, certes variables, selon les États et leur histoire contemporaine, en France par des textes réglementaires avant que la question n'entre dans le domaine de la loi.* (…) *À ce titre,* poursuit M. Olivier Forcade, *la loi du 24 juillet 2015 sur le renseignement est le fruit d'une maturation et d'une évolution précise de l'encadrement juridique des pratiques de renseignement en France, dans un environnement international attentif.* »

Dès avant 2015, la condamnation de la France par la CEDH le 24 avril 1990 dans une affaire *Kruslin et Huvig* – qui concernait des écoutes judiciaires – fut le prélude à la loi du 10 juillet 1991 précitée.

La jurisprudence de la Cour de Strasbourg, qui a eu et qui continue à avoir une influence sur le droit français du renseignement, s'est établie progressivement au cours des quarante dernières années, sur le fondement de l'article 8 de la Convention européenne des droits de l'homme, relatif au droit au respect de la vie privée.

(1) In Le droit du renseignement, ibid., introduction page 19.

L'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales relatif au droit au respect de la vie privée : la règle et l'exception

La Convention de sauvegarde des droits de l'homme et des libertés fondamentales, plus couramment appelée Convention européenne des droits de l'homme, prévoit en son article 8 une règle générale, le droit au respect de la vie privée, et une exception, l'ingérence d'une autorité publique dans cette vie privée, conditionnée au caractère prévisible de la loi et au caractère nécessaire à de la sécurité nationale. Cet article stipule que :

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

Dans le champ du renseignement, l'article 8 de la Convention européenne des droits de l'homme énonce ainsi deux exigences, précisées par la Cour européenne des droits de l'homme dans sa jurisprudence :

– l'ingérence dans la vie privée doit être prévue par la loi ;

– cette ingérence doit être nécessaire à la sécurité nationale : la Cour européenne des droits de l'homme reconnaît aux États une marge d'appréciation nationale pour déterminer le type de système de surveillance dont ils ont besoin pour protéger la sécurité nationale mais elle soumet un tel système à des garanties minimales. L'atteinte aux droits et libertés, si elle est envisageable, doit donc être légitime, nécessaire et proportionnée au but poursuivi.

1. Une jurisprudence ayant directement entraîné l'adoption de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques

a. L'arrêt fondateur Klass c. Allemagne *du 6 septembre 1978 : la reconnaissance par la CEDH de la nécessité pour les États démocratiques de se doter d'outils de surveillance*

Sur le fondement de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, la Cour européenne des droits de l'homme a traité la question de la surveillance secrète dans plusieurs affaires, remontant à l'arrêt *Klass c. Allemagne* du 6 septembre 1978. Dans cette affaire, la CEDH a considéré que **le pouvoir de surveiller en secret les citoyens n'était conforme à l'article 8 de la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques**. Constatant que les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments

subversifs opérant sur son territoire, la Cour européenne des droits de l'homme a estimé que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications était, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale, à la défense de l'ordre et à la prévention des infractions pénales.

En d'autres termes, et selon une jurisprudence constante, depuis l'arrêt *Klass c. Allemagne,* la CEDH estime qu'un régime d'interception n'emporte pas, en lui-même, violation de la Convention, les États disposant, par ailleurs, d'une importante marge d'appréciation dans le choix des moyens permettant de protéger la sécurité nationale. Le pouvoir de surveiller en secret les citoyens n'est, toutefois, tolérable que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques.

La Cour européenne de Strasbourg précise aussi dans l'arrêt *Klass* que le respect de la Convention européenne des droits de l'homme implique, entre autres, qu'une ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace que doit normalement assurer, au moins en dernier ressort, une autorité juridictionnelle car il offre les meilleures garanties d'indépendance, d'impartialité et de régularité procédurale.

b. Les exigences de clarté, d'accessibilité et de prévisibilité de la loi

À la suite de cet arrêt fondateur, la Cour européenne des droits de l'homme a été amenée à préciser le sens des exigences posées à l'article 8 de la Convention, et notamment celle que les ingérences éventuelles des pouvoirs publics dans la vie privée des individus soient « *prévues par la loi* ». Au demeurant, la CEDH considère la loi non dans sa dimension formelle de texte législatif mais au sens général de norme, ce qui inclut notamment les actes réglementaires et la jurisprudence. Ce sont la clarté, l'accessibilité et la prévisibilité de la norme qui importent, pas sa forme matérielle.

● L'exigence de prévisibilité de la loi : l'arrêt *Malone c. Royaume-Uni*

Non seulement la surveillance secrète doit être encadrée par la loi mais la CEDH exige en outre que cette loi soit prévisible et précise. Dans l'arrêt *Malone c. Royaume-Uni* du 2 août 1984, la CEDH précise que la prévisibilité « *ne saurait signifier qu'il faille permettre à quelqu'un de prévoir si et quand ses communications risquent d'être interceptées par les autorités, afin qu'il puisse régler son comportement en conséquence. Néanmoins, la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions, elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance.* »

La loi doit être d'autant plus prévisible et précise que les atteintes au droit au respect de la vie privée sont importantes. La CEDH considère en effet dans

l'arrêt *Malone* que « *puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la loi irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire.* » Ainsi, selon la CEDH, une norme est prévisible lorsqu'elle est rédigée avec assez de précision pour permettre à toute personne de régler sa conduite.

● L'exigence de clarté de la loi : l'arrêt *Kruslin et Huvig c. France*

C'est en 1990 que la France a été condamnée pour la première fois par la CEDH dans une affaire d'écoutes. Cette condamnation a eu un effet majeur sur notre droit puisqu'elle a conduit le gouvernement de l'époque à présenter devant le Parlement ce qui allait devenir la loi de 1991 sur les interceptions de sécurité.

Dans l'arrêt *Kruslin c. France* du 24 avril 1990, qui concernait des écoutes judiciaires, la CEDH a notamment précisé le sens de l'exigence de clarté de la loi posée par l'article 8 de la Convention. La Cour a considéré, en l'espèce, que le droit français, écrit et non écrit, n'indiquait pas avec assez de clarté, en matière d'écoutes judiciaires, l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités. Ainsi que le précise la CEDH dans son arrêt, l'exigence que l'ingérence au droit au respect de la vie privée soit « prévue par la loi » veut que la mesure incriminée ait une base en droit interne mais a aussi trait à la qualité de la loi en cause : les mots « prévue par la loi » exigent l'accessibilité de la loi à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle.

Les trois exigences posées par la CEDH

Pour être conforme à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, toute ingérence dans la vie privée doit répondre à trois exigences :

– être prévue « par la loi », soit par une norme accessible, prévisible et précise ;

– avoir pour fondement l'un des objectifs limitativement énumérés par l'article 8 paragraphe 2 de la Convention ;

– être, « nécessaire, dans une société démocratique », à la poursuite d'un tel objectif, à savoir répondre à un besoin social impérieux et respecter le principe de proportionnalité.

c. Les conséquences de l'arrêt* Kruslin *en droit interne : le vote de la loi du 10 juillet 1991 relative au secret des correspondances par la voie des communications électroniques

Ainsi que l'ont rappelé MM. Jean-Jacques Urvoas et Patrice Verchère dans leur rapport d'information sur l'évaluation du cadre juridique applicable aux

services de renseignement [1], « *c'est cette condamnation qui avait incité le gouvernement de Michel Rocard à préparer une loi relative aux interceptions de sécurité, adoptée en juillet 1991. Le droit alors en vigueur manquait singulièrement de précision puisque la légalité de ces interceptions de sécurité reposait sur une simple interprétation très large de l'article 81 du code de procédure pénale, autorisant le juge d'instruction à procéder à tous les actes d'instruction qu'il estime utiles à la manifestation de la vérité. La Cour de cassation y avait vu à plusieurs reprises la base légale d'une faculté laissée au juge d'ordonner une écoute téléphonique et le droit interne s'en était alors contenté. Mais, comme l'indiquait la CEDH, " les écoutes et autres formes d'interceptions des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. Partant, elles doivent se fonder sur une loi d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner ".* »

Dans son rapport législatif d'avril 2015, M. Jean-Jacques Urvoas, alors rapporteur de ce qui allait devenir la loi du 24 juillet 2015, est à nouveau revenu sur l'influence de la jurisprudence de la CEDH sur la législation française, considérant que celle-ci « *dessina[it] peu à peu le cadre juridique des conversations téléphoniques, de fait incluses dans les notions de correspondance et de vie privée contenues à l'article 8 de la Convention. Dès lors, leur interception comme leur enregistrement par l'autorité publique constituaient une ingérence dans l'exercice du droit garanti par ledit article* ». Et le président Urvoas d'ajouter : « *La leçon dispensée sur les bords du Rhin fut vite entendue sur les rives de la Seine* » puisque le processus législatif conduisant à l'adoption de la loi de 1991 s'ensuivit et que la presse fut même – grande première ! – invitée à visiter les locaux du GIC quelques jours avant le début des débats législatifs à l'Assemblée nationale.

M. Olivier Forcade [2] conforte cette analyse, soulignant que « *sous les injonctions d'arrêts de la Cour européenne des droits de l'homme, en 1990, le premier défi pour l'État fut de faire entrer le secret dans le droit, sans définition publiquement assumée du cadre et des applications concrètes de cette évolution initiale.* (…) *En plaçant le Groupement interministériel de contrôle (GIC) sous contrôle externe d'une Commission nationale de contrôle des interceptions de sécurité (CNCIS), la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par les voies des télécommunications touchait à l'autonomie de " l'État secret ", entendu au sens des activités publiques secrètes. Celle-ci fut fortement portée par le Premier ministre Michel Rocard au sortir d'une décennie 1980 qui avait connu le dévoilement d'activités de renseignement dans une publicité, devant l'opinion publique nationale ou internationale, qui n'avait pas nécessairement été recherchée* ».

---

(1) Rapport d'information du 14 mai 2013, en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, page 31.

(2) Le droit du renseignement, ibid.*, page 22.*

2. L’évolution de la jurisprudence de la CEDH et son influence sur l’élaboration de la loi de 2015

La jurisprudence de la CEDH en matière de surveillance de masse a évolué au fil de l’évolution des techniques, se saisissant successivement des différentes techniques de surveillance pouvant être utilisées. Ainsi et tout d’abord, la Cour a eu à connaître de la surveillance de la correspondance postale et des communications téléphoniques (*Klass et autres c. Allemagne*, 6 septembre 1978 (1) ; *Weber et Saravia c. Allemagne*, 29 juin 2006 (2)), nationales et internationales. La Cour a ensuite eu à connaître de l’interception massive de télécopies et courriels (*Liberty et autres c. Royaume-Uni*, 1er juillet 2008) ou encore des communications par téléphonie mobile (*Roman Zakharov c. Russie [GC]*, 4 décembre 2015) puis plus largement de toute donnée de communication et notamment des métadonnées (*Big Brother Watch et autres c. Royaume-Uni* (3), 13 septembre 2018) et l’ingérence dans les systèmes ou « hacking » (*Privacy International et autres c. Royaume-Uni*, affaire actuellement pendante).

a. Les six garanties posées par la CEDH dans l’affaire Weber et Saravia *en matière d’ingérence dans la vie privée*

Dans sa décision de principe *Weber et Saravia c. Allemagne* du 29 juin 2006, la CEDH dégage six garanties minimales en matière d’ingérence dans la vie privée, que le droit interne doit indiquer clairement :

– la nature des infractions susceptibles de donner lieu à un mandat d’interception ;

– la définition des catégories de personnes susceptibles d’être mises sur écoute ;

– la fixation d’une limite à la durée d’exécution de la mesure ;

– la procédure à suivre pour l’examen, l’utilisation et la conservation des données recueillies ;

– les précautions à prendre pour la communication des données à d’autres parties ;

– les circonstances dans lesquelles peut ou doit s’opérer l’effacement ou la destruction des données interceptées.

En avril 2007, dans l’arrêt *Popescu c. Roumanie*, la CEDH a estimé que la procédure roumaine d’interceptions de sécurité présentait des garanties insuffisantes : ces interceptions pouvaient être effectuées sur simple autorisation d’une instance non indépendante du pouvoir exécutif, sans aucune limitation dans

---

(1) Cf. supra.

(2) Cf. infra.

(3) Cf. infra.

le temps ni contrôle *a priori* d'un juge ou d'une autorité administrative indépendante. Aucun contrôle *a posteriori* n'était prévu non plus ni même de modalités de conservation et de destruction des enregistrements effectués.

La Cour européenne des droits de l'homme a par la suite confirmé sa jurisprudence *Weber et Saravia* dans les arrêts *Liberty et autres c. Royaume-Uni* du 1er juillet 2008), *Roman Zakharov c. Russie* du 4 décembre 2015, *Centrum för Rättvisa c. Suède* du 19 juin 2018 et *Big Brother Watch et autres c. Royaume-Uni* (1)du 13 septembre 2018.

Deux critères additionnels ont d'ailleurs été appliqués par la Cour à compter de son arrêt *Roman Zakharov c. Russie*. Sont désormais également pris en compte les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne. Selon la Cour, il est en souhaitable que le contrôle soit effectué par un juge, dans la mesure où un tel contrôle présente les meilleures garanties d'indépendance et d'impartialité. Cependant, une autorisation préalable n'est pas nécessaire dès lors qu'il existe un organe de contrôle indépendant (*Big Brother Watch et autres c. Royaume-Uni* (2)). Dans ce dernier arrêt, la CEDH a refusé la demande des requérants d'actualiser ces critères à la lumière de l'avancée des technologies de surveillance.

Selon les informations fournies à la mission d'information par la direction des affaires juridiques du ministère de l'Europe et des affaires étrangères, (DAJ-MEAE), dans chaque espèce, la Cour tient compte de toutes les circonstances de la cause, par exemple la nature, la portée et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit interne (Roman Zakharov c. Russie). Par ailleurs, la Cour a jugé que lorsqu'un État instaure une surveillance secrète dont les personnes contrôlées ignorent l'existence et qui demeure dès lors inattaquable, il se peut qu'un individu soit traité d'une façon contraire à l'article 8 de la Convention, voire privé du droit garanti par cet article, sans le savoir et partant sans être à même d'exercer un recours au niveau national ou devant les organes de la Convention (*Klass et autres c. Allemagne*). Tel est particulièrement le cas dans un contexte où les progrès techniques ont fait évoluer les moyens d'espionnage et de surveillance et où les États peuvent avoir des intérêts légitimes à prévenir des troubles, des infractions ou des actes de terrorisme. Certaines conditions doivent être remplies pour qu'un requérant puisse se prétendre victime d'une violation entraînée par la simple existence de mesures de surveillance secrète ou d'une législation permettant de telles mesures (*Roman Zakharov c. Russie*). Selon les informations fournies par la DAJ-MEAE, la jurisprudence de la Cour européenne des droits de l'homme révèle une adaptation constante à l'évolution des techniques de surveillance et du contexte dans

(1) *Cf.* infra.

(2) *Cf.* infra.

lesquelles elles sont mises en œuvre. Le contrôle qu'elle effectue sur les régimes nationaux de mise en œuvre de ces techniques apparaît de plus en plus strict.

b. La jurisprudence de la CEDH, cadre conventionnel de l'élaboration de la loi du 24 juillet 2015

Si l'arrêt *Kruslin* de 1990 a directement inspiré l'adoption de la loi du 10 juillet 1991 sur les interceptions de sécurité, la jurisprudence ultérieure de la Cour européenne des droits de l'homme a également pu peser sur la volonté du législateur d'adopter, en 2015, un texte régissant l'activité des services de renseignement, afin d'éviter toute condamnation par le juge européen.

Dans leur rapport d'information de 2013 précité (1), M. Jean-Jacques Urvoas – qui allait devenir le rapporteur à l'Assemblée nationale de la loi de 2015 – et M. Patrice Verchère ont appelé l'attention sur le risque de condamnation par la CEDH pesant sur la France en l'absence de loi encadrant l'activité des services de renseignement : « *La France*, soulignaient-ils, *risque en permanence de se voir condamnée par la Cour européenne des droits de l'homme pour violation des dispositions de la Convention européenne des droits de l'homme et des libertés fondamentales. Si aucun recours n'a, pour l'heure, été formé pour des faits relevant d'une activité de renseignement, le risque d'une condamnation est constant*. (…) *Il apparaît que le recours aux moyens spéciaux d'investigation mis en œuvre par les services de renseignement en dehors du cadre judiciaire, comme les sonorisations de lieux privés ou la pose de balises sur un véhicule, peuvent sans aucun doute conduire à une condamnation de la France par la CEDH, en l'absence d'une base juridique précise.* » Les deux rapporteurs de l'époque incitaient alors le législateur à définir une telle base juridique en lui suggérant « *de prendre notamment pour base l'analyse de la jurisprudence de la CEDH qui définit, en creux mais assez nettement, le contour d'une future loi sur le renseignement*. » Ils allaient même jusqu'à préconiser de s'appuyer sur la jurisprudence de la CEDH en matière de géolocalisation en temps réel (2) ou encore de renforcement de la protection afférente à la procédure de témoignage des agents des services de renseignement (3).

Dans son rapport législatif de 2015, le rapporteur, M. Jean-Jacques Urvoas, a à nouveau insisté sur le fait que la jurisprudence de la Cour européenne des droits de l'homme constitue le cadre conventionnel dans lequel s'inscrit le projet de loi sur le renseignement de 2015. Il soulignait que la France avait été une nouvelle fois condamnée par la Cour européenne des droits de l'homme, dans l'arrêt *Vetter* du 31 mai 2005, pour avoir procédé, en 1997, en police judiciaire, à

---

(1) Ibid., pages 31-32

(2) L'arrêt Uzun c. Allemagne du 2 septembre 2010 rappelant la nécessité, pour cette technique de renseignement, d'une loi particulièrement précise, en particulier compte tenu de ce que la technologie disponible devient de plus en plus sophistiquée.

(3) L'arrêt Van Mechelen et autres c. Pays-Bas du 23 avril 1997 ayant donné l'occasion à la CEDH d'admettre que l'utilisation de dépositions anonymes pour asseoir une condamnation ne soit pas en toutes circonstances incompatible avec la Convention à condition que l'atteinte portée aux droits de la défense soit compensée par la procédure suivie devant les autorités judiciaires.

la sonorisation d'un appartement sans base juridique suffisamment précise. Comme l'indique M. Jean-Jacques Urvoas, « *dans la mesure où notre pays a, sous l'effet conjugué des condamnations de la Cour européenne des droits de l'homme et de la jurisprudence interne, complété son appareil juridique en matière de police judiciaire, il apparaît désormais que le recours aux moyens spéciaux d'investigation mis en œuvre par les services de renseignement en dehors du cadre judiciaire, comme les sonorisations de lieux privés ou la pose de balises sur un véhicule, doit faire l'objet d'une définition précise.* »

Il est indéniable que la loi du 24 juillet 2015 a pris en compte la jurisprudence de la Cour européenne de Strasbourg. On peut citer plusieurs exemples de principes qui découlent de cette jurisprudence :

– le contingentement des services et des techniques de renseignement ;

– les durées maximales de mise en œuvre des techniques de renseignement et les délais de conservation.

Il en va de même du principe de subsidiarité énoncé à l'article L. 853-1 du code de la sécurité intérieure, qui dispose que l'utilisation des techniques de renseignement qu'il mentionne ne peut être autorisée que *« lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé. »*

La jurisprudence de la CEDH en matière de surveillance secrète a continué à se préciser depuis l'adoption de la loi de 2015. C'est pourquoi il importe aux membres de la mission d'information de tenir compte de ses derniers développements dans le cadre de l'évaluation de cette loi.

3. La jurisprudence de la CEDH post-loi de 2015 : l'arrêt *Big Brother Watch* et la question du partage de renseignement

Dans l'arrêt *Big Brother Watch et autres c. Royaume-Uni* [(1)] du 13 septembre 2018, la CEDH examine trois types de surveillance :

– l'interception massive de communications ;

– l'obtention de données de communication auprès de fournisseurs de services de communication ;

– le partage de renseignements – en l'espèce entre l'Agence nationale de sécurité américaine, la NSA, et le Royaume-Uni.

Le contexte de l'affaire est celui des révélations d'Edward Snowden, ancien agent contractuel de la NSA, sur l'existence de programmes de surveillance

---

(1) L'affaire Big Brother Watch *a été renvoyée en Grande chambre. L'audience a eu lieu le 10 juillet 2019. L'arrêt de Grande Chambre n'a pas encore été rendu. L'arrêt présenté ci-dessous est celui rendu par la première section de la Cour EDH le 13 septembre 2018.*

et de partage de renseignements entre les États-Unis et le Royaume-Uni. À la suite de ces révélations, plusieurs requêtes ont été introduites devant la Cour européenne des droits de l'homme.

Ce n'est pas la première fois, dans l'arrêt *Big Brother Watch*, que la CEDH examine la question de l'interception massive de communications. En juin 2018, elle avait déjà conclu, dans un arrêt *Centrum För Rättvisa c. Suède,* que la législation et la pratique suédoises dans le domaine du renseignement électromagnétique n'emportaient pas violation de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Elle avait notamment considéré que le système suédois offrait des garanties adéquates et suffisantes contre l'arbitraire et le risque d'abus. L'affaire *Big Brother Watch* est cependant la première affaire dans laquelle la CEDH étudie spécifiquement la portée de l'atteinte à la vie privée d'une personne, susceptible de résulter de l'interception et de l'examen de données de communication – et non du contenu des communications.

La question de l'obtention de communications auprès de fournisseurs de services de communication avait également déjà été examinée dans de précédents arrêts, notamment dans l'arrêt *Ben Faiza c. France* du 8 février 2018.

En revanche, c'est la première fois, avec l'arrêt *Big Brother Watch* que la CEDH est appelée à examiner la conformité à la Convention d'un régime d'échange de renseignements. Dès l'affaire *Szabó et Vissy c. Hongrie* du 12 janvier 2016, la CEDH avait été amenée à considérer [(1)] que la pratique des gouvernements, de plus en plus répandue, consistant à transférer et à partager entre eux des renseignements obtenus grâce à une surveillance secrète – une pratique dont l'utilité en matière de lutte contre le terrorisme international n'est aucunement remise en cause et qui concerne aussi bien les échanges entre les États membres du Conseil de l'Europe que les échanges avec d'autres États – était une raison supplémentaire pour exiger une attention particulière en matière de contrôle externe et de voies de recours. Cela étant, c'est avec l'affaire *Big Brother Watch* que la Cour examine véritablement la question.

a. L'interception massive de communications

Dans l'affaire *Big Brother Watch*, la CEDH conclut que **l'utilisation d'un régime d'interception massive n'emporte pas en lui-même violation de la Convention** européenne des droits de l'homme mais observe qu'un tel régime doit respecter les critères qui se trouvent énoncés dans sa jurisprudence. Outre les six exigences posées dans l'affaire *Weber et Saravia*, sont également pris en compte les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne – critères additionnels développés dans l'arrêt *Zakharov*. La CEDH précise qu'il est en principe souhaitable – et que cela constituerait même une

(1) Paragraphe 78 de la décision.

« meilleure pratique » – que le contrôle soit effectué par un juge, dans la mesure où un tel contrôle présente les meilleures garanties d'indépendance et d'impartialité. Cependant, une autorisation préalable n'est pas nécessaire dès lors qu'il existe un organe de contrôle indépendant.

La CEDH considère que le droit britannique ne répond pas à l'exigence de « qualité de la loi » et ne permet pas de conserver l'« ingérence » au niveau « nécessaire dans une société démocratique ». La Cour considère en effet qu'il y a insuffisance de la surveillance appliquée au choix des canaux de transmission pour l'interception, au filtrage, à la recherche et à la sélection des communications interceptées pour examen à raison du caractère inadéquat des garanties liées à la sélection des « données de communication pertinentes » pour examen [(1)]. Partant, la CEDH considère qu'il y a eu violation de l'article 8 de la Convention, s'agissant de l'interception massive de communications.

Si l'on s'en tient à son premier volet consacré à l'interception massive des communications, cet arrêt s'inscrit dans la continuité de la jurisprudence de la Cour et notamment dans celle l'arrêt *Zakharov c Russie* précité. Dans l'arrêt *Big Brother Watch*, la CEDH a rejeté la demande des requérants d'actualiser les six critères énoncés dans sa jurisprudence constante, à la lumière de l'avancée des technologies de surveillance. La Cour considère qu'ajouter le critère de « suspicion légitime » à l'encontre de la personne objet de la mesure, et celui de notification subséquente à la personne objet de l'interception serait incompatible avec le principe même de surveillance de masse. L'arrêt *Big Brother Watch* est aussi à rapprocher de l'arrêt *Centrum for Rattvisa c Suède* du 19 juin 2018. Dans cet arrêt, la Cour considère que la législation suédoise d'interception massive de signaux électroniques aux fins du renseignement étranger est compatible avec l'article 8 de la Convention.

b. L'obtention de données de communication auprès de fournisseurs de services de communication

Dans l'arrêt *Big Brother Watch*, la CEDH indique que le système britannique d'obtention de données de communication auprès de fournisseurs de

---

(1) « La Cour considère que la décision de mettre en œuvre un régime d'interceptions en masse relève de l'ample marge d'appréciation laissée à l'État contractant. De plus, compte tenu de la supervision indépendante exercée par le Commissaire à l'interception des communications et l'IPT, et des vastes enquêtes indépendantes qui ont suivi les révélations d'Edward Snowden, elle estime que les services de renseignement du Royaume-Uni prennent au sérieux les obligations que leur impose la Convention et n'abusent pas des pouvoirs que leur confère l'article 8 § 4 de la RIPA. Néanmoins, l'examen de ces pouvoirs soulève deux principaux points de préoccupation : premièrement, le fait que le processus de sélection ne fait pas l'objet d'une supervision d'ensemble, portant aussi sur la sélection des canaux de transmission sur lesquels l'interception aura lieu, les sélecteurs et les critères de recherche à appliquer pour le filtrage des communications interceptées et la sélection des éléments pour examen par un analyste ; et deuxièmement, l'absence de garanties réelles applicables à la sélection pour examen de données de communication associées. Au vu de ces lacunes et dans la mesure indiquée ci-dessus, la Cour conclut que le régime découlant de l'article 8 § 4 de la RIPA ne répond pas à l'exigence de " qualité de la loi " et ne permet pas de conserver l'" ingérence " au niveau " nécessaire dans une société démocratique ". Partant, il y a eu violation de l'article 8 de la Convention à cet égard. »

services de communication emporte violation de l'article 8 de la Convention EDH du fait qu'il n'est pas conforme à la loi.

La Cour relève que la réglementation britannique autorise un large éventail d'organes publics (1) à demander l'accès à des données de communication auprès d'entreprises de communication. La demande doit poursuivre un des objectifs limitativement énumérés (sécurité nationale, prévention des infractions graves) et être proportionnée à cet objectif. Comme pour les interceptions de masse, les professions protégées (avocats, journalistes, médecins, parlementaires) ne sont pas exclues par principe mais une attention particulière doit être portée dans ces cas afin de préserver la confidentialité des informations. Par ailleurs, des dispositions spécifiques sont prévues pour le cas où l'objet de la demande est de déterminer la source d'un journaliste.

La Cour rappelle qu'elle n'a statué qu'à deux reprises sur ce sujet : dans l'arrêt *Malone c. Royaume Uni* du 2 août 1984, et plus récemment, dans l'arrêt *Ben Faiza c. France* du 8 février 2018. Elle rappelle à cet égard qu'elle a distingué dans cet arrêt entre l'obtention de données de communication pouvant renseigner sur la localisation passée d'une personne et la géolocalisation en temps réel, cette dernière mesure étant plus attentatoire aux droits des personnes.

Elle rappelle par ailleurs que la CJUE a également eu à se prononcer sur ces questions. Bien que la CJUE se soit davantage concentrée sur la question de la conservation des données, la CEDH relève que la CJUE s'est également prononcée sur la question de l'accès à ces données conservées. La Cour rappelle que la CJUE a jugé que tout système permettant l'accès à des données détenues par des fournisseurs de services de communication doit se limiter au but fixé, en l'espèce la lutte contre la criminalité grave, et que l'accès devrait être soumis au contrôle préalable d'un tribunal ou d'un organe administratif indépendant et que les données demeurent au sein de l'espace de l'Union européenne.

Enfin, bien que faisant référence aux arrêts de la CJUE (2) sur la conservation des données et bien que se prononçant sur la question de l'obtention des données de communications, **la CEDH ne se prononce pas explicitement sur la question de la conservation des données**. Elle vient uniquement confirmer sa jurisprudence *Ben Faiza* en réaffirmant que les méthodes de géolocalisation en temps réel sont plus intrusives que les méthodes permettant de géolocaliser *a posteriori* une personne dans la mesure, où, s'agissant des secondes, les données sont déjà conservées, alors que pour les premières, il s'agit de mettre en place un dispositif de surveillance consistant à repérer spécifiquement les déplacements qu'une personne est en train d'effectuer. Cependant, selon les informations fournies à la mission d'information par la DAJ-MEAE, la CEDH s'est jusqu'à présent montrée moins exigeante que la CJUE dans le cadre de son examen de la législation portant sur les techniques de surveillance de masse. Ainsi, à la

(1) Police, Her Majesty's Revenue and Customs (HMRC), National Crime Agency.

(2) Cf. infra.

différence de la CJUE qui a censuré le principe même d'une conservation généralisée et indifférenciée indépendamment de l'existence de garanties entourant l'accès aux données conservées, **la CEDH ne semble pas s'opposer à une collecte et conservation indifférenciées de données dès lors que l'utilisation de ces données fait l'objet d'un encadrement suffisant** répondant à de stricts critères. En outre, il y a lieu de relever que la CEDH ne fait ici pas de distinction entre les régimes de traitement de données selon qu'ils poursuivent une finalité de renseignement ou de lutte contre la criminalité, distinction que la CJUE est invitée à opérer dans une question préjudicielle pendante (*Privacy International*).

c. Le partage de renseignements avec les États étrangers

Enfin, dans l'arrêt *Big Brother Watch*, **la CEDH est appelée pour la première fois à examiner la conformité à la Convention d'un régime d'échange de renseignements**. En l'espèce, la question concerne du renseignement *entrant* puisque certaines des requérantes contestaient la légalité de la réception, par le Royaume-Uni, d'éléments interceptés par la NSA, l'Agence de sécurité américaine.

La CEDH reprend sa grille d'analyse habituelle, vérifiant si ce partage est prévu par la loi et s'il est entouré des six garanties minimales définies dans sa jurisprudence constante, relatives à la nature des infractions susceptibles de donner lieu à un mandat d'interception ; à la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ; à la limite à la durée d'exécution de la mesure ; à la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; aux précautions à prendre pour la communication des données à d'autres parties ; et aux circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites.

En l'espèce, la Cour déclare qu'il n'y a pas eu violation de l'article 8 de la Convention à raison du régime d'échange de renseignements.

4. Une jurisprudence qui, si elle a des effets majeurs en droit interne, laisse davantage de marges d'appréciation aux États que celle de la CJUE en matière de droit du renseignement

La Cour européenne des droits de l'homme a eu l'occasion d'examiner progressivement, au cours des quarante dernières années, depuis l'arrêt *Klass c. Allemagne* de 1978, la mise en œuvre de diverses techniques de renseignement ainsi que les modalités de leur contrôle. Interrogé par la mission d'information, le président de la formation spécialisée du Conseil d'État chargée du contentieux de la mise en œuvre des techniques de renseignement, M. Edmond Honorat, a estimé que la Cour européenne des droits de l'homme prenait bien en compte les difficultés, les nécessités ainsi que les spécificités de l'activité de renseignement, notamment la préservation du secret inhérente à leur action. « *Elle laisse également une véritable marge d'appréciation aux États parties sur ce point. Elle*

a élaboré une jurisprudence qui, tout en étant contraignante pour les services, ne paralyse pas leur action et assure une protection élevée du droit des individus, notamment le droit au respect de la vie privée et la liberté d'expression. »

Le président de la formation spécialisée relève aussi, s'agissant du caractère asymétrique de la procédure devant cette formation, que « *la Cour, y compris dans l'arrêt* Big Brother Watch*, s'est montrée très prudente sur le maniement du principe de l'égalité des armes, pourtant cardinal dans sa jurisprudence, et sur l'applicabilité de l'article 6 de la Convention* (1)*, admettant assez largement les procédures de contrôle asymétriques, comme en France. Certaines opinions dissidentes révèlent toutefois les dissensions existant au sein de la Cour sur le degré de protection dont doit faire l'objet le secret de la défense nationale. »*

Au terme de l'ensemble des auditions et consultations qu'elle a menées, la mission d'information partage l'appréciation que porte le président de la formation spécialisée du Conseil d'État. S'il est des domaines dans lesquels on peut s'interroger quant à la volonté de la Cour européenne des droits de l'homme d'imposer sa propre vision du droit aux États, on ne peut que reconnaître le caractère équilibré de sa jurisprudence en matière de surveillance secrète ou de masse. La jurisprudence de la CEDH en matière de renseignement apparaît encore plus équilibrée, par contraste, si on la compare avec celle de la Cour de justice de l'Union européenne en la matière.

Les requêtes pendantes devant la CEDH concernant la loi du 24 juillet 2015 relative au renseignement

Plusieurs requêtes intéressant le droit du renseignement sont actuellement pendantes devant la Cour européenne des droits de l'homme.

Il s'agit tout d'abord de la requête *Association confraternelle de la presse judiciaire contre France* et onze autres requêtes. Communiquées au gouvernement français le 26 avril 2017, ces requêtes, qui ont été introduites par des avocats et des journalistes, ainsi que par des personnes morales en lien avec ces professions, concernent la loi dont la présente mission d'information doit évaluer l'application. La Cour a posé des questions aux parties sous l'angle de trois articles de la Convention européenne des droits de l'homme : l'article 8, sur le droit au respect de la vie privée et de la correspondance, l'article 10, sur la liberté d'expression, et l'article 13, sur le droit à un recours effectif.

Deux autres requêtes similaires sont également pendantes : la requête *Follorou contre France* et la requête *Johannes contre France*, communiquées au gouvernement français le 4 juillet 2017. L'affaire *Association confraternelle de la presse judiciaire c. France* est similaire à l'affaire *Big Brother Watch*.

Enfin, rappelons que l'affaire *Big Brother Watch* a été renvoyée en Grande chambre. L'audience a eu lieu le 10 juillet 2019. L'arrêt de Grande Chambre n'a pas encore été rendu. L'arrêt présenté ci-dessus est celui rendu par la première section de la CEDH le 13 septembre 2018.

(1) Sur le droit à un procès équitable.

B. LA JURISPRUDENCE *TELE2 SVERIGE AB* DE LA CJUE : UNE ÉPÉE DE DAMOCLÈS POUR LES SERVICES DE RENSEIGNEMENT

1. L'arrêt *Tele2 Sverige AB* : une remise en cause de l'obligation de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation des utilisateurs d'un réseau de communication

a. Le contexte

La directive 2002/58 du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications, régit les activités des fournisseurs de services de communications électroniques au public. Cette directive prévoit plusieurs garanties au bénéfice des utilisateurs desdits services. Elle dispose, en particulier, à son article 5, que les États membres doivent garantir la confidentialité des données, à son article 6, que les données concernant les abonnés et les utilisateurs doivent être effacées ou rendues anonymes dès qu'elles ne sont plus techniquement nécessaires pour assurer la bonne communication des données ou pour assurer la facturation des services et, à son article 9, que les données de localisation ne peuvent être utilisées sans avoir été anonymisées à moins de disposer du consentement du titulaire de ces données.

Cependant, l'article 15, paragraphe 1, de cette directive autorise les États membres à adopter des mesures législatives dérogeant aux garanties précitées pour sauvegarder la sécurité publique et pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées des systèmes de communication électronique. Cette disposition précise que **les États membres peuven**t, notamment, **imposer aux fournisseurs de conserver les données de connexion pendant une durée limitée**.

Cette habilitation faite aux États membres d'introduire une mesure imposant aux fournisseurs de conserver les données de connexion pendant une durée limitée a été transformée en **une obligation** pour les États membres **par la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006**, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication.

Cependant, dans son arrêt du 8 avril 2014, *Digital Rights Ireland et Seitlinger*, la Cour de justice de l'Union européenne a déclaré que la directive 2006/24 était invalide au motif que l'obligation de conservation des données portait une atteinte disproportionnée aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Dans cet arrêt, la Cour a jugé qu'une telle obligation poursuivait un objectif légitime, à savoir la lutte contre la criminalité grave et la protection de la sécurité publique, mais que l'atteinte aux droits fondamentaux qu'elle imposait était disproportionnée à ce qui est nécessaire pour poursuivre ces objectifs.

Compte tenu des termes de l'arrêt *Digital Rights Ireland*, il existait **une incertitude sur le point de savoir si le principe même d'une conservation généralisée des données était en soi une atteinte excessive** aux droits fondamentaux, ou si une telle conservation généralisée des données pouvait être maintenue, à condition de prévoir un encadrement très strict de l'accès à ces données, une durée de conservation réduite et des modalités renforcées de protection des données conservées.

L'arrêt *Digital Rights Ireland*, prémisse de l'affaire *Tele2 Sverige*

Dans l'arrêt *Digital Rights Ireland* du 8 avril 2014, la CJUE, saisie à titre préjudiciel par des juridictions irlandaise et autrichienne, invalide la directive 2006/24/CE [(1)] du 15 mars 2006. Cette directive obligeait les fournisseurs de communications électroniques à conserver, pendant six mois à deux ans, les données nécessaires pour retrouver et identifier la source et le destinataire d'une communication et permettre aux autorités nationales d'accéder à ces données. Cette directive instaurait un dispositif de conservation de données de trafic et de localisation par les fournisseurs d'accès à internet et les opérateurs de télécommunications pour en permettre l'utilisation dans le cadre de la lutte contre la criminalité et le terrorisme.

Selon la CJUE, ce texte portait une atteinte disproportionnée au droit au respect de la vie privée et au droit à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Selon la CJUE, le législateur de l'Union européenne avait « *excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7 [(2)], 8 [(3)] et 52, paragraphe 1, de la Charte* ». Parce qu'elle « *couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves* », parce qu'elle « *comporte une ingérence dans les droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* », la directive 2006/24/CE a été jugée par la CJUE contraire aux principes énoncés dans la Charte des droits fondamentaux. La CJUE a donc invalidé la directive dans toutes ses dispositions.

Fallait-il conclure de cette décision de la CJUE que les États membres de l'Union européenne ne pouvaient pas, eux non plus, instaurer de telles obligations de conservation en droit national ? De fait, **six juridictions nationales**, dont cinq de dernière instance, **ont annulé leurs dispositifs nationaux de conservation des données à la suite de cette jurisprudence – mais ni la Suède ni le Royaume-Uni**. La Suède avait déjà transposé la directive 2006/24 et le Royaume-Uni avait quant à lui déjà adopté des dispositions nationales avant que la directive soit adoptée. La conformité de ces dispositions nationales fut contestée devant la Cour administrative d'appel de Stockholm et la Cour d'appel d'Angleterre et du Pays-de-Galles qui saisirent alors la CJUE, dans ce qui allait devenir l'affaire *Tele2 Sverige AB*.

(1) Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

(2) Sur le respect de la vie privée.

(3) Sur la protection des données à caractère personnel.

b. Les termes de l'arrêt Tele2 Sverige AB

Dans son arrêt du 21 décembre 2016, *Tele2 Sverige et Watson e.a.*, confirmé depuis dans l'arrêt *Ministerio fiscal* du 2 octobre 2018, la CJUE a entendu résoudre la contradiction littérale qui existait entre l'article 1er, paragraphe 3, et l'article 15, paragraphe 1, de la directive de 2002, qui mentionnent les activités de l'État dans le domaine pénal et celles concernant la sécurité publique, la défense et la sûreté de l'État, à la fois comme des matières exclues du champ d'application de cette directive (clause d'exclusion), et comme des matières autorisant des limitations aux droits à la protection de la vie privée et des données personnelles (clauses de limitation). Pour résoudre cette contradiction, la CJUE, s'est appuyée sur l'économie générale de cette directive. D'une part, elle a jugé que l'exclusion pure et simple du champ d'application de la directive des traitements de données poursuivant des finalités telles que la répression des infractions pénales priverait d'effet utile les dispositions de l'article 15, paragraphe 1, lesquelles présupposaient nécessairement que les mesures nationales qui y sont visées relèvent de son champ d'application. D'autre part, elle a constaté que les mesures de conservation et d'accès imposées aux fournisseurs de services de communications électroniques pour les finalités mentionnées à l'article 15, paragraphe 1, régissent l'activité de ces fournisseurs, ce qui correspond au champ d'application de la directive tel qu'il est défini par son article 3.

Dès lors, la CJUE a choisi de juger qu'**une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de données était, en elle-même, contraire au droit de l'Union**. Elle n'a ainsi pas suivi l'avis de la Commission et des nombreux États membres intervenus à l'instance ni les conclusions de l'avocat général M. Saugmandsgaard Øe, présentées le 19 juillet 2016, qui estimait qu'une telle conservation généralisée était conforme au droit de l'Union, sous réserve qu'elle respecte certaines conditions strictes qu'il énumérait.

La CJUE a, tout d'abord, clairement jugé qu'une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique constituait en soi une atteinte disproportionnée aux droits fondamentaux.

Cependant, après avoir condamné le principe même d'une conservation généralisée des données, la Cour a admis que serait conforme au droit de l'Union une réglementation permettant, à titre préventif, la conservation **ciblée** des données de connexion, à des fins de lutte contre la criminalité grave, à condition que cette conservation soit – en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue – limitée au strict nécessaire. La CJUE a précisé les règles devant être respectées pour se conformer à ces exigences. Ainsi, selon la Cour, une telle réglementation devrait :

– prévoir des règles claires et précises régissant la portée et l'application d'une mesure de conservation en indiquant en quelles circonstances et sous quelles conditions une telle mesure peut être prise à titre préventif ;

– assurer que la conservation des données répond toujours à des critères objectifs, en établissant un rapport entre les données à conserver et l'objectif poursuivi, afin de **délimiter effectivement l'ampleur de la mesure et le public concerné** ;

– fonder la délimitation d'une telle mesure sur des éléments objectifs permettant de **viser un public** dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique, une telle délimitation pouvant être assurée notamment au moyen d'un critère géographique.

S'agissant des conditions d'accès aux données ainsi conservées, la CJUE a d'abord rappelé qu'eu égard à la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cet accès, lorsque l'accès aux données est motivé par la prévention, la recherche, la détection et la poursuite des infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un tel accès aux données, dans les limites du strict nécessaire. Cette considération n'exclut néanmoins pas que l'objectif de protection de la sécurité publique puisse aussi justifier un accès aux données sélectivement conservées.

Ensuite, la Cour a précisé qu'afin d'assurer que l'accès des autorités nationales aux données respecte le principe de proportionnalité, ledit accès doit être subordonné à des garanties appropriées. Ainsi, la réglementation nationale, qui doit être légalement contraignante en droit interne, doit prévoir :

– des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs doivent accorder aux autorités nationales compétentes l'accès aux données ainsi que les conditions matérielles et procédurales régissant cet accès ;

– des critères objectifs définissant ces circonstances et conditions, l'accès ne devant, en principe, être possible qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou d'être impliquée dans une telle infraction, sauf, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, auquel cas l'accès aux données d'autres personnes pourrait également être accordé ;

– un contrôle préalable par une juridiction ou une entité administrative indépendante de cet accès ;

– l'information des personnes concernées, sauf lorsque cette information est susceptible de compromettre l'enquête.

La Cour a enfin précisé que les fournisseurs doivent adopter les mesures d'ordre technique et organisationnel appropriées permettant d'assurer une protection efficace des données de connexion contre les risques d'abus ainsi que contre tout accès illicite. À ce titre, la réglementation nationale doit, en particulier, prévoir la conservation sur le territoire de l'Union ainsi que la destruction irrémédiable des données au terme de la durée de conservation de celles-ci. En outre, la Cour a rappelé qu'une autorité indépendante doit être chargée de contrôler le respect de cette obligation de protection rigoureuse par les opérateurs.

2. Une décision aux conséquences opérationnelles redoutées par la communauté du renseignement

a. Une décision qui remet en cause l'utilisation des techniques nécessitant la conservation des données

Selon la DAJ-MEAE, interrogée par la mission d'information sur les conséquences de cet arrêt, le droit national prévoit une conservation généralisée des données au sens de l'arrêt *Tele2*. Les services concernés assurent qu'aucune forme de conservation ciblée, telle que suggérée dans l'arrêt *Tele2* (1), n'est envisageable. Si la CJUE a pris le soin d'invalider toute forme de conservation généralisée des données avant de valider la conservation ciblée des données limitée au strict nécessaire, il en résulte nécessairement qu'il n'est pas possible de soutenir qu'une conservation de l'ensemble des données de la population puisse être justifiée par le haut niveau de la menace terroriste que la France connaît actuellement. Ce serait une interprétation par trop contraire au principe de l'interdiction de toute conservation généralisée des données.

Ainsi, cette décision *Tele2 Sverige AB*, si elle devait être confirmée, remettrait en cause les techniques nécessitant le recueil, en temps différé, de données de connexion conservées par les opérateurs, qui font l'objet de près de 40 000 demandes par an.

b. La préservation des techniques s'appuyant sur l'accès aux données en temps réel (accès aux données de connexion en temps réel et algorithme)

Pourraient seules continuer à être utilisés, sous réserve de notification, les géolocalisations en temps réel, le recueil de données en temps réel et l'algorithme qui n'impliquent pas, pour l'opérateur, d'obligation de conservation des données. Seules ces techniques permettraient de suppléer aux difficultés que représenterait la disparition de certaines techniques de renseignement actuellement utilisées par les services.

c. Des conséquences extrêmement préoccupantes

Les acteurs du renseignement ont dénoncé unanimement et avec énergie les conséquences qu'emporte une telle décision juridictionnelle.

---

(1) Ciblée sur une période temporelle, une zone géographique ou des cercles de personnes.

Parmi eux, le coordonnateur national du renseignement et de la lutte contre le terrorisme a souligné que cette jurisprudence, si elle devait être confirmée, **fragiliserait considérablement notre dispositif de renseignement** – sans parler du **domaine judiciaire, également très affecté**. Il a cité l'exemple des Suédois, concernés au premier chef par l'arrêt *Tele2 Sverige AB*, qui ont d'ores et déjà arrêté toute poursuite en matière de pédopornographie sur internet à la suite de cette décision. En effet, les services de renseignement risquent de **perdre une grande capacité de travail** : ils **n'ont ni le temps matériel ni la ressource** pour se passer de la possibilité de conserver des données.

Alors que **le cadre de la loi du 24 juillet 2015 repose sur un équilibre** entre protection de la vie privée et défense des intérêts fondamentaux de la nation, la **CJUE s'est placée du seul point de vue des droits individuels**. Le **cadre légal français est au plus haut niveau**, parmi les droits nationaux des États membres de l'Union européenne (1) : **peu d'autres pays disposent d'une autorité de contrôle indépendante ayant un accès permanent et complet aux locaux des services de renseignement telle que la CNCTR**. Ainsi, le directeur de la DGSE, M. Bernard Émié, a rappelé lors de son audition que la CNCTR effectuait au sein de sa direction **plus de trente visites de contrôle par an** – un contrôle portant sur les données collectées, les transcriptions, les extractions et la traçabilité de l'information. Et comme nous l'expliquons en première partie de ce rapport, les services de renseignement sont soumis non seulement au contrôle de la CNCTR mais également à une **multiplicité d'autres contrôles**, qu'il s'agisse de la CNIL, de la DPR, du Conseil d'État ou, sur le plan interne, du contrôle hiérarchique du chef de service sur ses subordonnés et de l'inspection générale des services de renseignement.

Enfin, les services de renseignement extérieurs, en particulier la DGSE, **prennent des risques importants** sur les territoires étrangers et font face à des **adversaires désinhibés, clandestins et qui font fi du droit international**. Il semble donc impératif de ne pas faire combattre les services de renseignement les mains liées derrière le dos. Les moyens dévolus aux services sont une garantie de l'État de droit. Il est capital de ne pas les en priver.

3. Une décision ayant suscité plusieurs questions préjudicielles des juridictions nationales

La décision *Tele2 Sverige AB* a suscité de très nombreux renvois préjudiciels de juridictions nationales, ce qui est inédit.

S'agissant de la France, le Conseil d'État a été saisi par plusieurs associations de recours tendant à l'annulation ou à l'abrogation de quatre décrets (2) pris pour l'application des articles L. 851-1 à L. 851-4 du code de la

---

(1) Cf., en troisième partie du rapport, l'analyse comparative des droits du renseignement des différents États membres de l'Union européenne.

(2) Il s'agit du décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, du décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des

sécurité intérieure (CSI), ainsi que de dispositions réglementaires prises pour l'application de l'article L. 34-1 du code des postes et des communications électroniques (CPCE) (1) et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (2).

Les dispositions contestées du CSI prévoient quatre techniques de recueil de renseignement susceptibles d'être utilisées par les services de renseignements du ministère des armées et du ministère de l'intérieur pour la défense et la promotion des intérêts fondamentaux de la nation. Ces techniques ont pour caractéristique commune de permettre l'accès des services de renseignement à des « données de connexion » des utilisateurs des réseaux de communications électroniques. Quant à l'article L. 34-1 du CPCE, il permet à l'État d'imposer aux opérateurs de communications électroniques la conservation, pendant une durée maximale d'un an, des données de connexion nécessaires à la recherche, à la constatation et à la poursuite des infractions pénales, tandis que l'article 6 de la loi du 21 juin 2004, précitée, étend cette obligation aux hébergeurs de contenus, afin de faciliter l'identification, par l'autorité judiciaire, des personnes ayant créé un contenu en ligne.

Les associations requérantes ont excipé de la non-conformité au droit de l'Union, tel qu'interprété par la Cour de justice notamment dans son arrêt du 21 décembre 2016, *Tele2 Sverige AB* de ces dispositions législatives, qui constituent les bases légales des dispositions réglementaires attaquées.

Par deux décisions du 26 juillet 2018, le Conseil d'État a saisi la Cour de justice de l'Union européenne (CJUE) de cinq questions préjudicielles, qui portent essentiellement sur les questions de savoir :

– d'une part, si des dispositifs de conservation et d'accès aux données de connexion par les autorités de l'État qui ont pour finalité la sauvegarde de la sécurité nationale relèvent du champ d'application du droit de l'Union ;

– d'autre part, si, et si oui, sous quelles conditions, la conservation générale et indifférenciée des données de connexion par les opérateurs de communications électroniques, afin de permettre aux autorités de l'État d'accéder à ces données à des fins de sécurité nationale ou de lutte contre la criminalité, peut être regardée comme conforme au droit de l'Union européenne ;

---

techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État, du décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure, et enfin, du décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

(1) Il s'agit de l'article R. 10-13 du code des postes et des communications électroniques

(2) Il s'agit du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

– enfin, si, compte tenu des garanties entourant l'accès des services de renseignement aux données de connexion à des fins de sécurité nationale, les modalités de recueil de renseignement régies par les articles L. 851-1 à L. 851-4 du CSI sont conformes au droit de l'Union.

Selon leur libellé, ces questions invitaient la CJUE à réviser les principes dégagés par sa jurisprudence, en particulier dans l'arrêt *Tele2*. Dans le cadre de cette instance, **le Gouvernement français a soutenu, à titre principal, que les dispositifs en cause dans ces affaires n'étaient pas régis par le droit de l'Union dès lors qu'ils avaient notamment pour finalité de sauvegarder la sécurité nationale, laquelle relève de la seule compétence des États membres en application de l'article 4, paragraphe 2, du Traité sur l'Union européenne**. À titre subsidiaire, le Gouvernement français s'est efforcé de démontrer à la Cour la conformité au droit de l'Union des dispositifs de conservation et d'accès aux données personnelles en cause, moyennant, à tout le moins, une réinterprétation de la jurisprudence *Tele2*, au regard, entre autres, de la jurisprudence moins restrictive de la Cour européenne des droits de l'homme.

4. Les conclusions rendues par l'avocat général de la CJUE à la suite de ces renvois préjudiciels sont décevantes mais témoignent d'un infléchissement par rapport à l'arrêt *Tele2*

L'avocat général Campos-Sanchez Bordona a rendu le 15 janvier dernier des conclusions, s'agissant des questions préjudicielles posées par le Conseil d'État.

a. La réaffirmation du raisonnement suivi par la CJUE

Ces conclusions se bornent pour l'essentiel à **réaffirmer le raisonnement suivi par la CJUE dans son arrêt *Tele2*** sans réfuter de manière convaincante l'argumentaire développé par les États membres et la Commission en faveur de sa révision. Si l'avocat général **semble avoir entendu les critiques des États membres sur la conservation ciblée et admet l'importance vitale de la conservation des données de connexion pour la protection de la sécurité publique et la lutte contre la criminalité, ses conclusions n'en témoignent pas moins** – selon les informations fournies à la mission d'information par la direction des affaires juridiques du ministère de l'Europe et des affaires étrangères – **d'un manichéisme simplificateur** qui consiste à **opposer ces objectifs à « la barrière infranchissable des droits fondamentaux des citoyens ».** Cette approche réductrice de la conservation des données de connexion le conduit ainsi à sermonner les États membres sur la nécessité de sacrifier l'efficacité pratique des politiques de préservation de la sécurité nationale et de lutte contre la criminalité au nom de la protection des droits fondamentaux. À cet égard, l'avocat général se contente de développements théoriques qui sont bien loin de répondre à l'expérience pratique et aux nombreux exemples mis en avant par les États membres dans le cadre de la procédure.

Par ailleurs, l'avocat général **ne répond pas à l'argumentaire du Gouvernement français et des autres États membres pointant les divergences de jurisprudence entre la Cour européenne des droits de l'homme et la CJUE**, alors que les stipulations de la Charte des droits fondamentaux reprennent de manière substantielle celles de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales.

***b. Un certain infléchissement par rapport à la jurisprudence* Tele2**

Bien qu'elles s'en défendent, **ces conclusions témoignent cependant d'un certain infléchissement par rapport à la jurisprudence *Tele2***.

D'une part, la **critique, formulée par l'avocat général, de la conservation ciblée** et la recherche d'une solution alternative à la fois conforme au droit de l'Union et praticable par les États membres attestent d'une certaine prise de conscience de la gravité des enjeux auxquels ceux-ci sont confrontés.

D'autre part, l'avocat général invite la CJUE à faire preuve de davantage de retenue et **renvoie au législateur de l'Union ou aux États membres, dans le cadre de la marge d'appréciation dont ils disposent, pour la détermination des dispositifs de conservation**.

Surtout, l'avocat général **estime possible la mise en place d'un dispositif de conservation, certes limitée et différenciée, mais qui concerne les données de connexion de l'ensemble des utilisateurs et des abonnés des réseaux internet et de téléphonie**, **et admet la conformité au droit de l'Union d'un dispositif de conservation générale plus étendu dans des situations exceptionnelles**.

c. Des conclusions qui ne lient pas la CJUE

Ces **conclusions ne lient pas la Cour de justice**, qui pourrait rendre son arrêt à l'été ou à la rentrée prochaine, de sorte qu'il n'est aucunement certain que la Cour suive son avocat général sur tout ou partie de ses propositions. En outre, **la CJUE pourrait,** ainsi que l'y invite son avocat général dans l'affaire préjudicielle belge, **valider dans son principe la modulation dans le temps, par la juridiction de renvoi, des effets d'une éventuelle invalidation de la législation nationale,** ce qui permettrait au Conseil d'État, d'une part, de ménager un délai suffisant pour réformer notre dispositif, et d'autre part, de sanctuariser les procédures notamment pénales fondées sur des données collectées et conservées en méconnaissance des exigences posées par la Cour.

Cette jurisprudence a été **évoquée par les gouvernements en conseil JAI** [(1)] et beaucoup de travaux ont été faits depuis deux ans sur le sujet. Par ailleurs, les procureurs de plusieurs États se sont exprimés sur le sujet, estimant

---

([1]) Conseil des ministres européens de la justice et des affaires intérieures.

que la décision de la Cour de justice de Luxembourg était absolument ingérable. Elle pose en effet un problème majeur dans le cadre des enquêtes pénales.

Peut-être la CJUE apportera-t-elle de la souplesse à sa décision initiale (1) mais les conclusions de l'avocat général pourraient laisser présager une ligne générale proche de l'arrêt initial. Dès lors, la mission d'information envisage plusieurs voies possibles pour sortir de cette impasse.

5. Plusieurs voies sont possibles pour sortir de cette impasse juridique et garantir la pleine efficacité des services de renseignement

Aux yeux des membres de la mission d'information, **la décision *Tele2 Sverige AB* s'apparente à un *hold-up* jurisprudentiel de la Cour de justice de l'Union européenne qui a débordé de sa compétence en méconnaissance des stipulations du Traité sur l'Union européenne, réservant la sécurité nationale à la compétence des États membres**.

Il n'est pas impossible que, dans une sorte de compétition avec la Cour de Strasbourg, la Cour de Luxembourg ait cherché à maximiser la portée de la Charte des droits fondamentaux, alors même que la CEDH joue déjà le rôle de gardien des droits fondamentaux et a défini depuis une quarantaine d'années, de l'arrêt *Klass* à l'arrêt *Big Brother Watch*, une jurisprudence mesurée et équilibrée sur la surveillance. Se saisir d'une directive sur le droit des opérateurs de télécommunication pour toucher au cœur du cœur du domaine régalien est très contestable.

Pour sortir de l'impasse et préserver l'efficacité des services de renseignement, plusieurs voies sont envisageables.

a. Faire évoluer la relation entre l'État et les opérateurs de télécommunications ?

Évoquée lors des auditions menées par la mission d'information, une option indirecte consisterait à faire en sorte que **la conservation des données soit assurée par l'État et non plus par les opérateurs de télécommunications** – puisque c'est sous cet angle que les législations nationales ont été remises en cause. On pourrait envisager qu'un commissaire du Gouvernement, placé auprès de chacun des opérateurs, soit chargé d'assurer la conservation des données, auquel cas notre législation nationale sortirait du champ de la directive de 2002.

b. Modifier le droit dérivé ?

Une autre option envisageable pour sortir de l'impasse que constitue l'arrêt *Tele2 Sverige AB* serait de faire évoluer le droit dérivé. C'est une option qu'a proposée la délégation parlementaire au renseignement dans son dernier

---

(1) Selon les informations fournies à la mission d'information, les observateurs attendaient cette décision avant l'été mais la crise sanitaire pourrait remettre en cause ce calendrier.

rapport [1], la DPR estimant qu'il importait « *de clarifier la portée de [l'] arrêt [Tele2] au regard de l'article 4-2 du TFUE selon lequel " la sécurité nationale reste de la seule responsabilité de chaque État membre ". Dans ces conditions, et pour protéger l'action des services de renseignement,* ***le projet de règlement*** **ePrivacy** *en cours de négociation devrait exclure le traitement de données visant exclusivement la sécurité publique, la défense et la sûreté de l'État.* »

L'article 2, paragraphe 2, du TFUE stipule que lorsque les traités attribuent à l'Union une compétence partagée avec les États membres dans un domaine déterminé, l'Union et les États membres peuvent légiférer et adopter des actes juridiquement contraignants dans ce domaine. Les États membres exercent leur compétence dans la mesure où l'Union n'a pas exercé la sienne. Les États membres exercent à nouveau leur compétence dans la mesure où l'Union a décidé de cesser d'exercer la sienne.

Or, pour juger que le droit de l'Union interdit toute forme de conservation généralisée des données, la Cour s'est fondée sur l'existence d'une compétence de l'Union qui est, selon elle, consacrée par l'article 15, paragraphe 1, de la directive 2002/58.

Par conséquent, la DAJ-MEAE a suggéré à la mission de s'interroger quant à la possibilité de supprimer l'article 15, paragraphe 1, de la directive 2002/58, à l'occasion de la refonte en cours de cette directive, et de préciser que « *la présente directive est sans préjudice du droit des États membres de prévoir une obligation faite aux opérateurs de conserver les données nécessaires aux fins de protection de la sécurité publique ou de lutte contre la criminalité grave, qui relève de la compétence des États membres* ». Une telle évolution ne ferait sortir du droit de l'Union que l'obligation de conservation généralisée des données et l'accès aux données conservées par les services concernés, et non le traitement de ces données par les fournisseurs et par les services concernés, une fois cet accès réalisé, qui resterait régi par le droit de l'Union. Cependant, comme le soulignent les services de la DAJ-MEAE, à supposer que le Parlement européen soit prêt à envisager une telle solution, ce qui n'apparaît pas probable au vu des positions qu'il soutient sur d'autres questions connexes [2], il ne peut être certain que la Cour se contenterait d'une telle évolution, même si elle constituerait un signal fort, pour se déclarer incompétente.

Selon les informations fournies par la direction des affaires juridiques du ministère de l'Europe et des affaires étrangères, d'une part, la directive 2002/58 régit de manière exhaustive les obligations susceptibles d'être imposées aux opérateurs de services de communication électronique. Par conséquent, il conviendrait de préciser, après chaque disposition de la directive 2002/58 portant sur la protection de la confidentialité des données relatives au trafic et à la

---

(1) Rapport n° 1869 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2018, tome 1, p. 77.

(2) Le Parlement a notamment demandé à la CJUE de rendre un avis sur l'accord conclu entre l'Union et le Canada concernant le PNR.

protection des données contre « tout accès » non autorisé que ces dispositions sont « *sans préjudice de la compétence des États membres pour réglementer la conservation et l'accès aux données de connexion à des fins de lutte contre la criminalité et de protection de la sécurité publique* » (notamment article 5 de l'actuelle proposition de règlement appelé à remplacer cette directive).

D'autre part, l'article 23, paragraphe 1, sous a) à e), du Règlement général sur la protection des données autorise expressément le droit de l'Union ou le droit national à apporter des limitations aux droits reconnus par ledit règlement en vue de garantir la sécurité nationale, la défense nationale, la sécurité publique et la prévention et la détection d'infractions pénales pourvu que ces limitations respectent l'essence des libertés et droits fondamentaux ainsi que le principe de proportionnalité. Ainsi, cet article, s'il permet des dérogations aux règles générales de protection des données, ne soustrait pas pour autant lesdites dérogations au droit de l'Union.

La CJUE pourrait donc considérer que cette disposition interdit également toute conservation généralisée des données. Pour faire échec à cette argumentation, il pourrait être avancé que la directive 2002/58 refondue, qui exclurait la conservation des données du champ du droit de l'Union, est une *lex specialis* qui fait obstacle à l'application de cette disposition, mais il n'est pas du tout certain que cette interprétation soit acceptée par la Cour.

c. Modifier le droit primaire ?

La solution la plus radicale pour affranchir les services de renseignement des effets de la jurisprudence *Tele 2 Sverige AB* consisterait à revenir sur le droit primaire, c'est-à-dire à modifier le Traité, afin d'affirmer que les questions de souveraineté et de sécurité nationale sont exclues du champ jurisprudentiel de la CJUE.

Cette solution serait évidemment la plus efficace mais également la plus complexe à mettre en application puisqu'elle devrait être décidée à l'unanimité et que, à ce stade, tous les États membres de l'Union européenne ne semblent pas prêts à s'engager dans une telle révision.

d. Une rébellion possible des juridictions nationales au nom du principe d'identité constitutionnelle de la France ?

Une rébellion des juridictions nationales au nom du principe d'identité constitutionnelle de la France ne semble pas à exclure. En effet, **depuis 2004 et dans plusieurs décisions depuis lors [(1)], le Conseil constitutionnel vérifie que les textes de l'Union européenne ne remettent pas en cause « *une règle ou un***

(1) La décision n°2004-496 DC du 10 juin 2004, dite « Loi pour la confiance dans l'économie numérique *» a été confirmée et affinée dans les décisions n°2004-497 DC du 1er juillet 2004, n° 2004-498 DC du 29 juillet 2004 et n° 2004-499 DC du 29 juillet 2004.*

principe inhérent à l'identité constitutionnelle de la France, sauf à ce que le constituant y ait consenti **».** **De même, le Conseil d'État, dans un arrêt du 8 février 2007** ***Société Arcelor Atlantique et Lorraine***, a défini les modalités de la conciliation du principe de suprématie de la Constitution avec l'exigence de transposition des directives : le juge administratif a ainsi recherché si les principes constitutionnels dont la méconnaissance était invoquée en l'espèce par le requérant étaient effectivement et efficacement protégés par les traités et principes généraux du droit de l'Union européenne.

Le juge administratif, dans le cadre des recours formés contre les textes réglementaires d'application de la loi de 2015, et le Conseil constitutionnel, en cas de question prioritaire de constitutionnalité relative à cette loi, **pourraient ainsi considérer que l'interdiction de la conservation généralisée des données, énoncée dans l'arrêt *Tele2*, est contraire au principe de souveraineté, défini au titre premier de la Constitution – principe inhérent, s'il en est, à l'identité constitutionnelle de la France.**

Comme nous l'avons souligné en première partie de ce rapport, la loi du 24 juillet 2015 a constitué un apport majeur en matière de droit du renseignement, établissant un subtil équilibre entre protection des libertés et garanties de la sécurité. Le Conseil constitutionnel s'est prononcé sur le texte et en a validé l'essentiel. Le Conseil d'État et la Cour européenne des droits de l'homme sont également régulièrement amenés à se prononcer au contentieux. La CJUE n'a, aux yeux des membres de la mission, aucune place dans ce système. Si, lorsqu'elle aura à se prononcer prochainement sur les renvois préjudiciels pendants dans l'affaire *Tele2 Sverige AB*, la Cour de justice de Luxembourg devait persister dans sa position de blocage, **on n'aurait sans doute d'autre solution que de considérer que la primauté du droit européen cesse quand on se trouve au cœur du cœur de la souveraineté nationale et de notre droit constitutionnel**.

La mission a conscience du caractère encore très incertain des pistes qu'elle suggère pour sortir d'un contentieux extrêmement préoccupant mais encore évolutif. En tout état de cause, elle tient à alerter la représentation nationale sur cette difficulté majeure que notre pays doit surmonter.

TROISIÈME PARTIE : LES PROPOSITIONS DE LA MISSION D'INFORMATION : AMÉLIORER L'EFFICACITÉ OPÉRATIONNELLE DES SERVICES ET RENFORCER LA PROTECTION DES LIBERTÉS INDIVIDUELLES DANS LE RESPECT DES GRANDS ÉQUILIBRES DE LA LOI DU 24 JUILLET 2015

Il importe de conserver l'économie générale de la loi relative au renseignement, qui est robuste et qui permet de répondre à des évolutions à cadre légal constant.

Pour reprendre une expression entendue lors d'une audition, « *certains ajustements techniques pourraient faciliter le travail des agents mais il ne faut pas de* big bang ».

I. LA MISSION PRÉCONISE DE NE PAS RETENIR CERTAINES PROPOSITIONS QUI LUI SEMBLENT DE NATURE À PORTER ATTEINTE À L'ÉQUILIBRE DU RÉGIME ACTUEL

A. LE CONTRÔLE DES ÉCHANGES INTERNATIONAUX : UNE RÉFORME INOPPORTUNE

Formulée par la CNCTR, la proposition d'instaurer un contrôle sur les échanges de renseignements – dans le sens entrant comme dans le sens sortant – entre services français et étrangers semble inopportune à la mission d'information. En effet, elle soulève plusieurs **difficultés d'application** concrète, au premier rang desquelles figure la **nécessité d'appliquer la règle du tiers service**. D'autre part, les **comparaisons européennes font apparaître de telles divergences** entre les régimes juridiques nationaux qu'elles ne permettent pas de plaider en faveur d'une telle évolution.

1. Une mesure proposée par la CNCTR

Dans son rapport public annuel de 2018, la CNCTR estime qu'« *eu égard aux conséquences potentielles sur la vie privée des Français et, de manière générale, de toute personne résidant en France ainsi qu'aux évolutions du contexte juridique, en particulier international, une réflexion doit être menée sur l'encadrement légal des échanges de données entre les services de renseignement français et leurs partenaires étrangers*. »

● Une question n'ayant pas été discutée lors du débat préalable à l'adoption de la loi de 2015

La CNCTR voit dans le non-traitement de cette question une véritable lacune de la loi, rappelant que « *lors de la discussion parlementaire sur le projet de loi relatif au renseignement en 2015, le sujet des échanges de données entre les services de renseignement français et leurs partenaires étrangers n'a presque pas été abordé. La rédaction de l'article L. 833-2 du code de la sécurité intérieure résulte d'un amendement adopté en première lecture du projet de loi par l'Assemblée nationale, lors de l'examen du texte en commission des lois. Conçu comme un élargissement des pouvoirs de la CNCTR, à laquelle était désormais attribuée une faculté de demander au Premier ministre communication de tous éléments nécessaires à ses missions, l'amendement n'a fait l'objet d'aucun débat sur l'exclusion des " flux entrants " de son champ d'application. L'éventualité d'un encadrement spécifique des échanges internationaux de renseignements n'a pas non plus été réellement examinée.* »

● Des échanges dont la CNCTR ne remet en cause ni la légitimité ni le caractère sensible

La CNCTR ne remet évidemment pas en cause **la légitimité** de ces échanges puisqu'elle rappelle que « *la prévention des menaces communes, notamment terroristes, auxquelles sont confrontés la France et ses alliés justifie l'existence d'une intense coopération entre services de renseignement de ces différents pays* ».

La commission nationale de contrôle reconnaît aussi la **sensibilité** du sujet : « *Par nature très sensible et participant de la souveraineté de l'État dans la conduite de sa politique étrangère, la coopération internationale entre services de renseignement a vocation, comme le reste des activités de ces services, à demeurer couverte par le secret. Une gestion imprudente des données échangées pourrait entraîner notamment de graves complications diplomatiques ou une perte de crédibilité des services français nuisant à leur action. Une coutume, dite du " tiers service ", est à cet égard souvent invoquée pour justifier qu'un service de renseignement recevant des données d'un partenaire étranger s'interdise, sauf autorisation de ce partenaire, de communiquer les données à un troisième organe.* »

● La CNCTR se demande si les échanges internationaux ne sont pas susceptibles de porter atteinte à la vie privée des Français

S'appuyant sur la définition légale de son champ de compétence, la CNCTR se demande dans son rapport public de 2018 si les flux – aussi bien sortants qu'entrants – de renseignements ne seraient pas « *susceptibles de comprendre des données dont le recueil, l'exploitation et la conservation entrent dans le champ d'application* (…) *du cadre légal institué en 2015* ».

S’agissant des flux sortants de renseignements, la CNCTR souligne dans son rapport qu’ils pourraient contenir des données recueillies à l’aide des techniques visées par la loi de 2015 ou bien des transcriptions et des extractions réalisées à partir de ces données et elles-mêmes soumises à la loi. La CNCTR estime que « *la transmission éventuelle de tels éléments à des services de renseignement étrangers a pour conséquence implicite de les soustraire à l’application des dispositions légales françaises* ». La CNCTR songe notamment aux règles de conservation des données et de destruction de ces dernières.

Pour la CNCTR, la question est encore plus délicate **pour le renseignement entrant**, qu’il soit constitué de données brutes ou de données transformées. Il convient, selon elle, d’éviter la tentation que pourrait avoir un service de renseignement français de demander à un service étranger l’obtention d’un renseignement qu’il n’aurait pu se procurer lui-même Il ne peut être non plus exclu, selon la CNCTR, que les renseignements entrants contiennent des données dont le recueil, l’exploitation et la conservation auraient été soumis au livre VIII du code de la sécurité intérieure si les services de renseignement français les avaient collectées par eux-mêmes. « *De telles données pourraient ainsi*, selon la CNCTR, *être privées des garanties légales dont elles auraient bénéficié si elles avaient été recueillies au moyen d’une technique de renseignement prévue par la loi*. »

Or, non seulement la loi n’a pas prévu l’intervention de l’autorité de contrôle s’agissant de ces échanges de renseignements mais elle a même **explicitement exclu** cette intervention s’agissant des flux entrants : l’article L. 833-2 du code de la sécurité intérieure prévoit en effet que la CNCTR peut solliciter du Premier ministre tous les éléments nécessaires à l’accomplissement de ses missions à l’exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux.

La CNCTR concède que **les échanges de renseignements entre services français et étrangers sont vraisemblablement formalisés par des conventions liant les services de renseignement français à leurs partenaires étrangers** mais déplore qu’« *aucune disposition légale n’ait fixé de cadre pour la conclusion et l’application de tels accords* ».

● La CNCTR met en avant la jurisprudence de la CEDH et le droit de certains États européens

Estimant qu’il n’existe pas, en l’état actuel du droit, de dispositif permettant de pallier ces difficultés, **la CNCTR cite *a contrario* l’exemple d’États voisins** en s’appuyant sur un rapport de l’Agence des droits fondamentaux de l’Union européenne [(1)], tout en reconnaissant qu’une « *étude comparative plus approfondie* » serait nécessaire. Elle indique notamment qu’en Allemagne, plusieurs dispositions encadrent les échanges internationaux, en particulier les flux

(1) Cf. infra.

sortants, selon le type de données concernées. Elle note en outre que dans certains États – la Belgique, le Danemark, les Pays-Bas, la Norvège et la Suisse –, l'existence de législations encadrant les échanges internationaux a permis à des organes de contrôle indépendants de mener, à ce sujet, une première expérience de coopération.

Toujours au niveau international, la CNCTR rappelle aussi que la **Cour européenne des droits de l'homme** s'est prononcée, comme nous l'avons vu en deuxième partie du présent rapport, sur le partage international de données entre services de renseignement dans sa jurisprudence *Big Brother Watch* (1).

Enfin, la commission de contrôle indique dans son rapport **avoir été saisie de la question par des organisations de défense des libertés publiques**, notamment en 2017.

● La CNCTR formule une proposition d'ordre général, renvoyant à l'exécutif le soin de définir les modalités de cette dernière

Lors de son audition par la mission d'information, M. Francis Delon a indiqué que dans son rapport, la commission qu'il présidait ne formulait pas de proposition, se contentant d'appeler l'attention du Gouvernement, afin d'« *éviter des voies irréalistes et impraticables* ».

2. La mise en application d'une telle proposition soulèverait des difficultés majeures, en particulier au regard de la règle du tiers service

Outre le fait qu'une telle proposition laisse planer des soupçons infondés sur les services de renseignement, sa mise en application concrète soulèverait plusieurs difficultés :

– d'une part, elle remettrait en cause la règle du tiers service, principe fondamental en matière de coopération internationale entre services de renseignement ;

– d'autre part, elle entraînerait un glissement du contrôle des techniques de renseignement vers le contrôle de la production des services de renseignement.

● Une proposition qui laisse planer des soupçons infondés sur les services de renseignement

Tout d'abord, si tel n'est pas le cas de la CNCTR, ce type de proposition émane d'ordinaire de personnes soupçonnant les services de renseignement de détourner la loi française en faisant faire par les services étrangers ce que la loi française leur interdit. Au terme de ses travaux, la mission d'information ne peut que s'inscrire en faux contre pareil soupçon : elle estime que c'est **faire un faux**

(1) Cf. la deuxième partie du rapport.

procès aux services de renseignement que de penser que lorsqu'ils n'obtiennent pas d'autorisation de recourir à une technique de renseignement applicable à un citoyen français, ils font appel aux services américains. De fait, la mission même des services de renseignement français est de **défendre l'autonomie stratégique de la France et donc de prémunir les Français contre les tentatives d'espionnages d'États étrangers**. C'est donc aussi une question de fierté pour les services : un service français n'ira pas demander à un service étranger de faire le travail à sa place.

La CNCTR l'a souligné elle-même lors de la cérémonie des vœux organisée par le GIC en janvier dernier : certes**, des erreurs ont pu être commises par les services mais il s'agissait soit d'erreurs techniques, soit d'erreurs liées à une mauvaise compréhension**. En aucun cas n'ont été relevés des cas de violations délibérées du cadre légal français. Interrogé sur le sujet par le président de la mission d'information, M. Francis Delon a admis qu'il « *n'avait pas d'éléments* » lui permettant de penser que des services français seraient susceptibles d'utiliser la coopération avec des services étrangers pour contourner la loi française ou pour blanchir des informations recueillies de manière illégale. M. Francis Delon a indiqué qu'il « *ne portait aucune accusation à cet égard* ».

● Une proposition qui soulèverait des difficultés majeures d'application au regard de la règle du tiers service

Raison centrale pour laquelle la mission s'oppose à cette proposition, la mise en application de cette dernière se heurte à la règle du tiers service.

Principe cardinal de la coopération internationale entre services de renseignement, la règle du tiers service « ***interdit la transmission à une tierce partie, sans autorisation de l'émetteur, d'un renseignement reçu d'un partenaire*** » [(1)]. Si les services étrangers partenaires, qui font confiance aux services français, apprenaient que l'utilisation des informations qu'ils leur transmettent doit être soumise au contrôle de la CNCTR, ils préféreraient sans nul doute assécher ce canal d'information [(2)].

Lors de leurs auditions, M. Bernard Émié, directeur général de la sécurité extérieure, et le général Éric Bucquet, directeur de la DRSD, ont beaucoup insisté sur la nécessité impérieuse, pour les services de renseignement, **d'assurer la protection de leurs sources – et donc le plein respect de la règle du tiers service** – **qui conditionne l'efficacité des directions du renseignement** : la coopération internationale, qui vise essentiellement à lutter contre le terrorisme, est fondée sur une confiance « *longue à gagner et rapide à perdre* », a indiqué le

---

(1) Cf. Renseigner les démocraties, renseigner en démocratie, *Jean-Claude Cousseran et Philippe Hayez, Odile Jacob, 2015.*

(2) On peut à cet égard citer l'exemple d'un service belge de renseignement qui a été placé en 2003 sous l'autorité du ministère de la justice et le contrôle étroit d'une commission de magistrats. Une telle évolution a entraîné l'arrêt immédiat des communications d'informations, en provenance des partenaires européens et en direction des services belges de renseignement, ce qui a naturellement été très handicapant pour la Belgique. Les échanges ont repris depuis car la Belgique a fait évoluer son dispositif.

directeur général de la DGSE. Les deux directeurs l'ont souligné, **les services partenaires sont des sources et ces sources ont un degré de confidentialité supérieur à celui même des informations échangées**. L'un des rôles des services de renseignement est **d'entretenir un maximum de contacts avec ce type de sources**, ce qui suppose de garantir la **confidentialité totale** de ces relations et contacts. Lorsqu'un service partenaire dialogue avec un service français, il **va parfois jusqu'à dévoiler une partie de ses capacités, de ses modes opératoires et de ses accès techniques** et il le fait parce qu'il a la certitude que le service français protégera cette source étrangère, mieux qu'il ne le fait lui-même. M. Bernard Émié a donc martelé que **la règle du tiers service n'était pas un prétexte pour pouvoir contourner la loi mais bien un impératif opérationnel, s'appliquant essentiellement aux relations bilatérales**. Il a conclu en rappelant que les renseignements reçus par la France de ses partenaires anglo-saxons avaient permis à plusieurs reprises de sauver des vies et qu'il serait donc suicidaire de tarir une telle source d'informations.

La mission d'information note que **la CNCTR se garde bien de formuler des préconisations spécifiques** pour étayer sa proposition, tant la difficulté d'application pratique est majeure. Elle tient aussi à rappeler que la règle du tiers service s'applique non seulement à la CNCTR (1) mais également à la délégation parlementaire au renseignement (2). En effet, la loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement a explicitement interdit la transmission à la délégation de tout élément relatif aux échanges avec des services étrangers ou des organismes internationaux compétents dans le domaine du renseignement, afin de garantir la protection de la règle du « tiers de confiance ». C'est le même raisonnement qui a conduit le législateur en 2015 à explicitement exclure ces échanges du champ de compétence de la CNCTR.

● Une préconisation qui entraînerait un glissement du contrôle des techniques de renseignement vers le contrôle de la production des services de renseignement

Enfin, la proposition de la CNCTR pose un problème en raison de **la nature même du contrôle qui serait exercé** : on passerait du contrôle des techniques de renseignement à un contrôle de la production des services, ce qui est très différent. Les membres de la mission d'information s'opposent formellement à ce type de glissement du rôle de la CNCTR.

3. Les comparaisons internationales sont peu pertinentes

Indépendamment de ce problème majeur d'application pratique, la mission d'information s'interroge quant à la pertinence de comparer – comme le fait la

---

(1) En vertu de l'article L. 833-2 du code de la sécurité intérieure.

(2) Conformément au dernier alinéa de l'article 6 nonies *de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires.*

CNCTR pour motiver sa proposition – les différents régimes applicables aux services de renseignement des États membres l'Union européenne, pour deux raisons. La première, c'est que la France est une puissance diplomatique et militaire. La seconde, c'est que les dispositions nationales en matière de renseignement sont extrêmement diverses au plan européen au point qu'il n'y a pas deux systèmes comparables.

● Des régimes juridiques très hétérogènes sur le continent européen

Ainsi que le souligne le magistrat belge Guy Rapaille (1), on trouve dans une quinzaine de pays européens (2), à des degrés variables trois éléments :

– une loi sur les services de renseignement ;

– un contrôle parlementaire des services ;

– et une autorité administrative ou judiciaire de contrôle.

Mais en dehors de ce triptyque commun, le juriste souligne **l'hétérogénéité des situations** : « *Ce constat étant posé, l'analyse fine s'avère délicate et complexe en raison de* ***l'extrême variabilité*** *dans chacun des éléments du triptyque. Les compétences et l'organisation des services varient d'un pays à l'autre, l'apparition des nouvelles technologies et donc des nouvelles menaces augmentant encore la complexité. Les commissions parlementaires diffèrent dans leur composition et leurs missions légales : contrôle de la politique publique du renseignement ou contrôle des activités des services. Le contrôle non parlementaire mis en place dans chaque pays présente aussi de très grandes variantes. Si la plupart des pays disposent d'une autorité administrative de contrôle indépendante, certains pays confient le contrôle à des autorités judiciaires (Italie, Espagne, Luxembourg) dont la mission est limitée au contrôle des techniques de renseignement. Dans certains pays, le contrôle exercé par cette autorité est large et couvre les activités des services (Belgique, Pays-Bas, Royaume-Uni). Dans d'autres, le contrôle se concentre sur les techniques de renseignement. Certaines autorités cumulent le contrôle des activités et celui des techniques.* »

L'Agence des droits fondamentaux de l'Union européenne a également établi une étude comparative du droit applicable aux services de renseignement des vingt-huit États membres (3). Dans le résumé en français de son étude (4), l'Agence des droits fondamentaux indique : « *La surveillance ciblée est*

---

(1) In Le droit du renseignement, Ibid., *page 58, Approche comparée des droits du renseignement.*

(2) La comparaison porte sur les États suivants : Allemagne, Autriche, Belgique, Danemark, Espagne, France, Grèce, Italie, Luxembourg, Norvège, Pays-Bas, Portugal, Royaume-Uni, Suède et Suisse.

(3) Surveillance by intelligence services : fundamental safeguards and remedies in the EU. Volume II : field perspectives and legal update. On trouvera un résumé en français de cette étude : Surveillance par les services de renseignement : protection des droits fondamentaux et voies de recours dans l'Union européenne, *Office des publications de l'Union européenne, 2016 et 2017.*

(4) Ibid., *page 4.*

réglementée de manière assez précise dans la majeure partie des vingt-huit États membres de l'Union européenne. En revanche, seuls cinq États membres disposent actuellement d'une législation détaillée sur la surveillance générale des communications. Les mesures de sauvegarde limitent les possibilités d'abus et ont été renforcées dans certains États membres (moins en matière de surveillance internationale). » L'Agence note que différentes entités supervisent le travail des services de renseignement dans les vingt-huit États membres de l'Union européenne : le juge, des organes d'experts, des commissions parlementaires et les autorités chargées de la protection des données. Si l'ensemble des États membres de l'Union européenne dispose d'au moins un organe de contrôle indépendant, certains de ces organes n'ont pas de pouvoir de décision.

● **Une hétérogénéité des systèmes qui se retrouve en matière de coopération internationale entre services de renseignement**

Dans le résumé de son étude en français [(1)], l'Agence reconnaît que *« les mesures de sauvegarde sont* ***généralement plus faibles (et moins transparentes) dans le contexte de la coopération internationale*** *en matière de renseignement. »*

Dans son étude *in extenso* [(2)] , elle rappelle tout d'abord qu'à l'exclusion de la Slovénie, les services de renseignement de tous les États membres doivent recueillir l'assentiment de l'exécutif avant de conclure un accord de coopération avec des services étrangers. Elle **souligne** [(3)] **ensuite que si le contrôle des échanges internationaux de renseignement existe dans certains États membres, il demeure limité**. **L'agence indique ainsi que les lois de la majorité des États membres – dix-sept sur vingt-huit – ne contiennent pas de disposition claire indiquant si, et dans quelle mesure, les organes de contrôle des services de renseignement sont compétents en matière de coopération internationale**.

L'Agence des droits fondamentaux de l'Union européenne indique que l'absence de toute mention spécifique du contrôle de la coopération internationale dans une loi peut être interprétée différemment d'un État membre à l'autre. Dans certains cas, cette absence pourrait être interprétée comme une autorisation implicite pour les organes de surveillance d'exercer un contrôle similaire sur la coopération internationale par rapport aux efforts de renseignement nationaux. D'autres peuvent coupler cette absence avec la règle du tiers service et l'interpréter comme une interdiction tacite de contrôler le partage international de renseignements.

---

(1) Page 4. L'Agence des droits fondamentaux tire de ce constat « la nécessité d'un approfondissement de la législation dans ce domaine ».

(2) Surveillance by intelligence services : fundamental safeguards and remedies in the EU. Volume II : field perspectives and legal update. Chapter 11 : *Oversight of international intelligence cooperation (pages 101 et sq.).*

(3) Ibid., *page 103*.

Dans le résumé de son étude en français, l'Agence européenne conclut : « *L'analyse juridique comparative de la FRA (1) montre que* ***presque tous les États membres disposent de lois concernant la coopération internationale en matière de renseignement. Cependant, seul un tiers de ces États exige que les services de renseignement se dotent d'un règlement intérieur concernant les procédures et les modalités de la coopération internationale et les mesures de garantie en matière de partage des données. Lorsqu'elles existent, ces règles sont généralement secrètes. Seuls quelques États membres autorisent l'évaluation externe des accords internationaux de coopération en matière de renseignement***. »

Il se dégage de ce bref panorama des systèmes de contrôle des services de renseignement européens la **confirmation d'une très grande diversité et d'une très grande hétérogénéité de systèmes dont la logique varie, comme dans bien d'autres domaines du droit, selon les traditions nationales**. La mission d'information a finalement l'impression que les exemples de pays cités par la CNCTR ne sont pas pertinents, tant le contrôle appliqué par les États concernés est sans rapport avec le type de contrôle envisagé par notre commission nationale de contrôle. Qui plus est, très peu d'États ont prévu un contrôle.

Encore une fois, comme nous l'avons expliqué en première partie de ce rapport, les services de renseignement français sont parmi les mieux encadrés et les mieux contrôlés au monde. La mission d'information considère donc la proposition de la CNCTR comme tout à fait inopportune.

4. La mission propose d'écarter cette proposition

La mission d'information considère que les relations entre services de renseignement français et étrangers se situent au cœur de la souveraineté des États, domaine réservé dans lequel une autorité indépendante n'a pas à intervenir puisqu'elle contrôle des techniques et non des services – d'autant qu'il existe déjà, au sein de ces services, des voies de contrôle interne. Il est une tendance naturelle des autorités administratives indépendantes que de vouloir étendre leur champ de compétence.

Mais la mission d'information, si elle salue l'excellente qualité du travail accompli par la CNCTR depuis sa création, n'est pas favorable à ce qui serait un glissement des missions de cette autorité indépendante d'un contrôle des techniques de renseignement vers un contrôle des services de renseignement. Préservons le climat de dialogue et de confiance qui s'est établi entre les différents acteurs depuis près de cinq ans.

---

(1) Fundamental Rights Agency.

B. LE CONTRÔLE *A PRIORI* PAR LE GIC DES DEMANDES D'IDENTIFICATION D'ABONNÉS

1. Une proposition de la CNCTR tenant au caractère peu intrusif de la technique d'annuaire inversé

L'article L. 851-1 du code de la sécurité intérieure permet aux services de renseignement, sur autorisation du Premier ministre accordée après avis de la CNCTR, d'accéder, en temps différé, aux données, conservées par des opérateurs de communications électroniques ou des fournisseurs de services au public en ligne, relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ainsi que celles relatives au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée. Comme le précise la CNCTR dans son rapport public de 2018, les informations recherchées peuvent être soit l'identité d'un abonné ou d'une personne connectée à une ligne téléphonique, un accès à internet ou un service au public en ligne, soit les numéros d'abonnement ou de connexion d'une personne désignée à des services de communications électroniques. Par exemple, un service de renseignement disposant d'un numéro de téléphone peut demander à connaître l'identité du titulaire de la ligne. À l'inverse, s'il connaît l'identité d'une personne, il peut demander à connaître ses numéros de téléphone. Dans ces situations, la technique de renseignement prévue à l'article L. 851-1 du code de la sécurité intérieure remplit principalement une fonction d'annuaire.

Dans son dernier rapport public, la CNCTR fait état, statistiques à l'appui, de ses interrogations quant à la pertinence du niveau de contrôle qu'elle exerce sur ces demandes : « *Depuis l'entrée en vigueur de l'article L. 851-1 du code de la sécurité intérieure le 1er février 2016, les demandes fondées sur ces dispositions ont représenté environ deux tiers des quelque 70 000 demandes de techniques de renseignement présentées chaque année. En 2018, sur les plus de 46 000 demandes qui portaient sur des accès à des données de connexion en temps différé, environ les deux tiers concernaient des identifications d'abonnés ou des recensements de numéros d'abonnement, soit autour de 30 000 demandes par an en moyenne* ».

La CNCTR considère le recueil d'identifications d'abonnés ou de numéros d'abonnement non tant comme une mesure de surveillance en soi que comme une mesure préparatoire à des mesures de surveillance à proprement parler : « *Un service de renseignement peut ainsi obtenir le numéro de téléphone d'une personne suspecte dans le but de solliciter ensuite une autorisation d'accès à une " facture détaillée " afférente à ce numéro ; il peut également chercher à préparer une demande d'interception des communications émises ou reçues par ce numéro. Les identifications d'abonnés ou les recensements de numéros d'abonnement peuvent aussi compléter des mesures de surveillance déjà autorisées, par exemple pour identifier les correspondants d'une personne, dont une " facture détaillée " fait apparaître les numéros. Dans tous les cas, pour la CNCTR, ce sont les*

techniques que les opérations d'identification préparent ou complètent qui portent atteinte à la vie privée, non ces opérations elles-mêmes ».

La Commission rappelle aussi que les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement sont déjà soumises à un régime dérogatoire, étant directement présentées à la CNCTR puis au Premier ministre par les agents des services de renseignement dont elles émanent. Compte tenu du caractère faiblement intrusif de ces demandes, la CNCTR « *exerce un contrôle de légalité réduit* » qui s'apparente à un « *contrôle de l'erreur manifeste d'appréciation* ».

C'est pourquoi, estimant que son contrôle *a priori* sur ces demandes est « *de faible valeur ajoutée* », la CNCTR propose de confier ce contrôle *a priori* au GIC et de ne conserver cette compétence *a priori* que lorsque la demande porte sur une personne exerçant une profession ou un mandat bénéficiant d'une protection particulière en vertu de la loi – parlementaires, magistrats, avocats et journalistes. Elle conserverait en tout état de cause sa compétence *a posteriori*.

2. Une mesure inopportune

Il est vrai que les demandes d'annuaire ou d'annuaire inversé sont très peu intrusives, même si elles manifestent l'intérêt des services à l'égard d'une personne ou de ses correspondants. Cependant, confier au GIC un avis sur la légalité de la demande d'une technique de renseignement conduirait à placer entre les mains d'une même instance le contrôle de légalité et la mise en œuvre, ce qui ne serait pas satisfaisant.

C'est pourquoi la mission d'information propose le maintien du droit en vigueur à l'article L. 851-1 du code de la sécurité intérieure.

II. LA MISSION PROPOSE DEUX ÉVOLUTIONS PERMETTANT DE RENFORCER LE CONTRÔLE

A. SÉCURISER LES CONDITIONS DE CONTRÔLE JURIDICTIONNEL DU CONSEIL D'ÉTAT PAR LA CONSÉCRATION D'UN DROIT DE VISITE

Comme l'a souligné Edmond Honorat, la formation spécialisée du Conseil d'État est tributaire, dans ses délais de traitement, de ceux de l'administration. Elle ne peut, en effet, statuer sans avoir accès aux informations dont seule l'administration dispose.

La formation spécialisée a déjà pratiqué les visites en matière de contentieux sur les fichiers [(1)]. Si cela n'a pas posé de difficulté à ce stade, le prévoir explicitement dans le code de justice administrative permettrait de parer à toute contestation à ce sujet.

---

(1) Cf. première partie du rapport.

Il paraît ainsi opportun de prévoir explicitement un droit de visite sur place, comme en fait la CNIL sur le fondement de l'article 19 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Proposition n° 1

Consacrer la possibilité d'un droit de visite pour les membres de la formation spécialisée du Conseil d'État dans le code de justice administrative.

B. ACTER LE RENFORCEMENT DE LA CENTRALISATION : UNE GARANTIE SUPPLÉMENTAIRE EN MATIÈRE DE CONTRÔLE

La centralisation est un enjeu crucial pour assurer un contrôle efficace de la mise en œuvre des techniques de renseignement par les services spécialisés.

Depuis 2015, le nombre de lieux dans lesquels les données de renseignement peuvent être stockées a été drastiquement réduit. **Trois points de centralisation des données** ont été retenus : un à la DGSE pour les techniques qu'elle met en œuvre, un à la DGSI pour les techniques qu'elle met en œuvre, et un au GIC pour les autres services des premier et second cercles ainsi que pour les techniques dont la loi exige qu'elles soient centralisées au GIC, comme les interceptions de sécurité.

Pour les balises de géolocalisation, la centralisation a été assez aisée car les balises sont des objets communicants qui envoient des données vers un serveur. Le GIC a donc installé les serveurs des principaux fournisseurs en son sein et a offert aux agents des services de renseignement la possibilité de s'y connecter de manière simple *via* une application.

Dans une zone peu couverte par des opérateurs ou quand un service de renseignement a besoin de bénéficier d'une grande discrétion, il est nécessaire d'utiliser un capteur qui ne communique pas les données qu'il recueille mais qui les stocke. Dans ce mode de mise en œuvre, le service qui procède au recueil doit relever les données sur site et les envoyer vers les serveurs centralisés du GIC où elles seront exploitées. Le contrôle du « dernier mètre », entre le moment où le service relève les données du capteur et celui où il les envoie au serveur, ne peut pas être d'ordre technique et doit reposer sur des déclarations qui engagent la responsabilité du service. Dans ce mode opératoire, le service peut être amené à n'envoyer sur les serveurs que certains enregistrements et à effacer les autres. Comme cela a été indiqué à la mission, « *le fait que les services d'assistance technique, chargés du recueil localement, effacent le plus tôt possible les enregistrements illisibles ou qui à l'évidence ne présenteront aucun intérêt pour l'exploitant, est protecteur de la vie privée* ».

Le GIC n'a pas à ce stade mis en place la centralisation des techniques de recueil et de captation des données informatiques car elles sont très peu utilisées

par les services en dehors de la DGSI et de la DGSE qui sont habilitées à centraliser elles-mêmes ces techniques.

Après avoir défini, en 2017, les modalités de la centralisation des paroles et des images captées sur le fondement des dispositions de l'article L. 853-1 du code de la sécurité intérieure et expérimenté le dispositif au cours de l'année 2018 en matière de captation de paroles puis d'images, dans trois services « pilotes », le GIC a généralisé celui-ci à tous les services de renseignement concernés (1) au cours de l'année 2019.

La majorité des techniques de renseignement sont ainsi couvertes par le dispositif de centralisation des renseignements collectés dans le système d'information du GIC, à l'exception des techniques de recueil de données de connexion par IMSI catcher (article L. 851-6 du code de la sécurité intérieure) et de celles de recueil et de captation de données informatiques (article L. 853-2 du même code), toutes deux caractérisées par une collecte décentralisée et des modalités diverses de stockage des données recueillies.

La mission prend acte de ces évolutions du périmètre de la centralisation, qui sont conformes à l'esprit de la loi de 2015. Il paraîtrait dès lors opportun d'inscrire dans le code de la sécurité intérieure la pratique existante.

Proposition n° 2

Inscrire dans le code de la sécurité intérieure les évolutions en matière de centralisation par le GIC.

III. LA MISSION ESTIME QU'UNE CLARIFICATION DU RÉGIME DE PARTAGE D'INFORMATIONS ENTRE LES DIFFÉRENTS SERVICES ET ADMINISTRATIONS EST DÉSORMAIS NÉCESSAIRE

A. LES INCERTITUDES DU DROIT EN VIGUEUR

1. Les dispositions de l'article L. 863-2 du code de la sécurité intérieure

Le premier alinéa de l'article L. 863-2 du code de la sécurité intérieure prévoit que les services de renseignement des premier et second cercles peuvent partager toutes les informations utiles à l'accomplissement de leurs missions.

Le deuxième alinéa de cet article dispose que les autorités administratives que sont les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes

(1) Tous les services de renseignement sont tenus de recourir au dispositif géré par le GIC, hormis la DGSI et la DGSE, qui en ont la faculté mais non l'obligation. Ces deux services disposent, en effet, d'un dispositif propre de centralisation des renseignements recueillis.

de protection sociale et les autres organismes chargés de la gestion d'un service public administratif peuvent transmettre aux services de renseignement du premier et du second cercles, de leur propre initiative ou sur requête de ces services, des informations utiles à l'accomplissement de leurs missions.

2. Un décret d'application qui n'a jamais été publié

L'article L. 863-2 du CSI prévoit que ses modalités d'application sont définies par décret en Conseil d'État. Ce décret est le seul acte réglementaire d'application de la loi du 24 juillet 2015 à ne pas avoir été publié.

3. Une disposition ayant donné lieu à un recours pendant devant le Conseil d'État

Une association a saisi le Conseil d'État en juin 2019 d'un recours (1) pour excès de pouvoir contre ce qu'elle considère être un acte administratif pris sur le fondement de l'article L. 863-2 du code de la sécurité intérieure. Selon les informations fournies à la mission d'information par le président de la formation spécialisée du Conseil d'État, l'affaire est en cours d'instruction.

B. LA NÉCESSITÉ D'UN ENCADREMENT PLUS STRICT MAIS QUI N'INTERDISE PAS DES COOPÉRATIONS NÉCESSAIRES À LA SÉCURITÉ NATIONALE

La mission d'information considère qu'il est souhaitable de remédier aux imprécisions juridiques de l'article L. 863-2 du CSI et de mieux préciser les contours du partage de renseignements entre services. En l'état actuel, ainsi que le souligne la CNIL, « *l'absence de décret pris pour l'application des dispositions prévues au premier alinéa du même article L. 863-2 du CSI fait peser un risque juridique sur les échanges entre services et la conservation éventuelle de ces informations. En particulier, toute conservation systématique dans un traitement de données de telles informations devrait faire l'objet d'un décret en Conseil d'État pris après avis de la CNIL* ».

En outre, comme nous l'avons rappelé en première partie, certains services de renseignement ne sont habilités à recourir aux techniques de renseignement que sur le fondement de certaines finalités. Il convient que cet encadrement de l'action des services en fonction des finalités poursuivies soit pris en compte dans le cadre du partage de renseignements entre services. Il conviendrait donc notamment de préciser qu'un service qui n'est pas compétent pour une finalité n'a pas à recevoir de renseignement brut ni de transcription obtenue à l'aide d'une technique de renseignement, sur le fondement de ladite finalité. Il importe de **ne pas altérer le principe de responsabilité du service ayant recueilli une donnée**, sans pour autant interdire des coopérations qui sont nécessaires à la sécurité nationale.

---

(1) https://www.laquadrature.net/2019/06/28/partage-de-donnees-le-renseignement-francais-encore-et-toujours-dans-lillegalite/

Proposition n° 3

Clarifier la rédaction de l'article L. 863-2 du code de la sécurité intérieure en y précisant les modalités du partage d'informations entre services de renseignement.

IV. LA MISSION PROPOSE DE RETENIR QUATRE AJUSTEMENTS TECHNIQUES, CONSENSUELS ET OPÉRATIONNELS

A. UNE DURÉE MAXIMALE DE CONSERVATION UNIQUE POUR LES DONNÉES COLLECTÉES PAR LES DISPOSITIFS DE CAPTATION DE PAROLES ET CEUX DE CAPTATION D'IMAGES

Comme les membres de la mission d'information l'ont montré dans la première partie du rapport, le régime actuel de conservation des données s'agissant du son et de l'image est pour le moins paradoxal. Pour rappel, les durées actuelles sont de :

– 30 jours à compter de leur recueil, pour les paroles prononcées à titre privé ;

– 120 jours à compter de leur recueil, pour les images captées dans un lieu privé.

La durée de 30 jours a été retenue pour les paroles car c'est celle qui s'applique pour les interceptions de sécurité. Mais elle est profondément inopérante s'agissant de **vidéos qui contiennent à la fois du son et de l'image**. Les services en sont rendus, au bout de 30 jours, à supprimer l'audio et à garder des vidéos muettes. Les paroles ne sont ni plus ni moins sensibles que les images au regard des libertés fondamentales.

La CNTR, dans son rapport d'activité 2018, a d'ailleurs considéré que le caractère éventuellement plus intrusif d'une technique par rapport à l'autre ne justifie pas une distinction entre les durées maximales de conservation des données recueillies [(1)].

En outre, la durée de 120 jours a également été choisie pour le recueil et la captation de données informatiques qui sont au moins aussi intrusives pour la vie privée.

La situation actuelle a été déplorée par l'ensemble des services de renseignement que les membres de la mission d'information ont auditionné. Il existe un réel consensus sur la nécessité d'harmoniser ces durées de conservation.

Les membres de la mission d'information estiment donc qu'il faudrait prévoir une **durée maximale de conservation unique pour les données**

(1) CNCTR, rapport d'activité 2018, p. 44.

collectées par les dispositions de captation de parole et ceux de captation d'images prévus à l'article L. 853–1 du CSI.

S'agissant de la **durée à retenir**, les membres de la mission d'information estiment que celle de 120 jours est plus logique. Elle présenterait l'avantage d'harmoniser les durées de conservation s'agissant des techniques de recueil de renseignement du chapitre III – sonorisation, fixation d'image, recueil et captation de données informatiques.

Proposition n° 4

Prévoir une durée maximale de conservation unique de 120 jours pour les données collectées par les dispositions de captation de parole et ceux de captation d'images prévus à l'article L. 853–1 du code de la sécurité intérieure.

B. UNE SIMPLIFICATION DE LA PROCÉDURE PERMETTANT DE RETIRER UN DISPOSITIF TECHNIQUE DANS UN DOMICILE

Le président de la CNCTR, lors de son audition par les membres de la mission d'information, a formulé une proposition de bon sens s'agissant de la procédure relative à l'introduction dans un lieu privé afin de procéder au retrait d'un dispositif technique.

Aux termes de l'article L. 853–3 du CSI, l'introduction d'agents de services de renseignement dans un lieu privé pour y mettre en place, utiliser ou retirer certains dispositifs de surveillance (balisage, captation de paroles et d'images, recueil et captation de données informatiques) doit être autorisée par le Premier ministre, après avis de la CNCTR. Cet avis doit être rendu en formation collégiale, restreinte ou plénière, lorsque le lieu concerné est à usage d'habitation.

S'il paraît justifié que les demandes d'introduction dans un lieu d'habitation pour y mettre en place et utiliser des dispositifs de surveillance fassent l'objet d'un examen en formation collégiale, la situation est bien différente s'agissant du seul retrait de ces dispositifs.

En effet, l'atteinte à la vie privée de la personne concernée a lieu au moment de **l'installation d'un dispositif**. En revanche, lorsque le service souhaite reprendre son matériel, la commission, comme l'a souligné M. Francis Delon, ne peut, dans les faits, qu'émettre un avis favorable puisque le retrait du dispositif de surveillance bénéficie à la protection de la vie privée de la personne intéressée.

Il ne paraît pas opportun de supprimer toute autorisation du Premier ministre ou tout avis de la CNCTR, dans la mesure où les services pénètrent bien dans le domicile, fût-ce uniquement pour y retirer un dispositif.

Il s'agirait plutôt de prévoir qu'une introduction dans un lieu d'habitation à la seule fin de retirer un dispositif ayant servi à recueillir des renseignements

puisse être autorisée par le Premier ministre au vu d'un **avis rendu par un membre seul de la CNCTR** et non plus uniquement par une formation collégiale de la Commission [(1)].

Cette proposition possède un réel **caractère opérationnel puisqu'elle permet en outre de resserrer les délais d'examen**. Si un membre de la CNCTR ayant la qualité de magistrat ou de membre du Conseil d'État pouvait émettre seul l'avis de la commission, selon le droit commun du traitement des demandes, il disposerait de 24 heures pour se prononcer, tandis que le collège de la commission statue dans un délai de 72 heures.

En outre, il aurait un intérêt certain pour la CNCTR, puisque les formations collégiales pourraient concentrer leurs réunions sur les demandes nécessitant une réelle délibération pour apprécier la proportionnalité de l'atteinte portée à la vie privée.

Cette proposition a recueilli l'assentiment des services de renseignement entendus par les membres de la mission d'information.

Proposition n° 5

Prévoir un avis par un membre de la CNCTR statuant seul s'agissant des demandes de retrait d'un dispositif technique nécessitant l'introduction dans un lieu d'habitation (article L. 853–3 du CSI).

C. L'ALLONGEMENT DE LA DURÉE D'AUTORISATION DE LA SURVEILLANCE INTERNATIONALE

Dans le cadre de la surveillance des communications électroniques internationales, le III de l'article L. 854–2 du CSI prévoit que le Premier ministre, après avis de la CNCTR peut autoriser les exploitations des données de connexion et des communications de certaines zones géographiques, d'organisations, de groupes de personnes ou de personnes.

Ces autorisations sont délivrées pour une durée maximale de quatre mois et sont renouvelables.

Comme l'ont fait remarquer les services de renseignement concernés, certaines de ces autorisations sont renouvelées maintenant depuis plusieurs années sans discontinuer. Certaines sont géographiques ou thématiques et dès que l'agent a terminé la demande d'autorisation, il doit faire commencer à préparer la demande suivante. Cela ne parait pas le meilleur usage des agents en charge de ces sujets.

Il ne s'agit pas de supprimer cette autorisation mais de rendre son renouvellement moins fréquent.

(1) CNCTR, rapport d'activité 2018, pp. 44 et 45.

Plusieurs solutions étaient dès lors envisageables :

– augmenter la durée de l'autorisation à un an ;

– augmenter la durée du renouvellement. La première autorisation serait valable pour quatre mois et ensuite le renouvellement pour 6 mois ou un an. Ce dispositif existe pour l'algorithme. Ce dernier est autorisé pour deux mois, puis renouvelable pour quatre mois.

Les membres de la mission privilégient la solution de l'augmentation de la durée maximale de l'autorisation qui présente l'avantage de la simplicité tout en conservant la procédure normale.

Proposition n° 6

Augmenter la durée de l'autorisation prévue sur le fondement de III de l'article L. 854–2 du code de la sécurité intérieure à un an.

D. UNE HARMONISATION À LA MARGE DES DURÉES D'AUTORISATION

L'article L. 853-2 du CSI sur le recueil et la captation de données informatiques prévoit deux durées différentes d'autorisation de mise en œuvre :

– 30 jours pour le recueil (accès au stock) ;

– 2 mois pour la captation (accès au flux).

Dans les faits, cette période de 30 jours peut s'avérer un peu courte car la mise en œuvre de cette technique de recueil de renseignement est complexe.

Il pourrait donc être opportun d'aligner la durée de l'autorisation de recueil de données informatiques sur la durée de deux mois prévue pour les autres techniques de renseignement du chapitre III : sonorisation, fixation d'image, captation de données informatiques.

Proposition n° 7

Porter à deux mois la durée de l'autorisation permettant de mettre en œuvre le recueil de données informatiques.

V. LA MISSION PRÉCONISE DE CLARIFIER LES DISPOSITIONS APPLICABLES EN MATIÈRE DE DROIT D'ACCÈS AUX FICHIERS ET DE RENFORCER L'ACCESSIBILITÉ DES FICHIERS AUX SERVICES DE RENSEIGNEMENT AINSI QUE LES POSSIBILITÉS D'INTERCONNEXION DES FICHIERS

A. CLARIFIER LES DISPOSITIONS APPLICABLES EN MATIÈRE DE DROIT D'ACCÈS AUX FICHIERS

Comme souligné au D du I de la deuxième partie du rapport, les règles applicables en matière d'exercice du droit d'accès des administrés aux fichiers de certains services de renseignement sont complexes. Ainsi, on peut s'interroger quant à la pertinence de maintenir sous le régime du droit d'accès direct des fichiers faisant systématiquement l'objet, de la part de leur responsable – et à juste titre –, de restrictions voire d'un refus total d'accès en cas de demande d'un administré. D'autre part, la création de la formation spécialisée du Conseil d'État constitue une véritable avancée de la loi du 24 juillet 2015 mais le contentieux devant cette formation spécialisée soulève plusieurs difficultés.

C'est pourquoi la mission d'information juge opportun de simplifier les règles en vigueur sur deux points. Il conviendrait :

– de prévoir un accès indirect aux fichiers auxquels une restriction au droit d'accès est systématiquement appliquée, de sorte que les administrés saisissent la CNIL en premier, sans s'adresser d'abord au ministère de tutelle d'un responsable de fichier ;

– de réviser les textes réglementaires applicables aux différents fichiers afin que ces textes précisent systématiquement, pour chaque fichier, de quel titre de la loi de 1978 « Informatique et libertés » le fichier relève, comment s'exerce le droit d'accès des administrés et quelle juridiction est compétente en cas de contentieux.

Proposition n° 8

Prévoir un droit d'accès indirect aux fichiers auxquels une restriction au droit d'accès direct est systématiquement appliquée et préciser par voie réglementaire le régime juridique applicable à chaque fichier.

B. RENFORCER L'ACCESSIBILITÉ DES FICHIERS AUX SERVICES DE RENSEIGNEMENT

La mission d'information l'a évoqué au 6 du D du I de la deuxième partie du rapport, le problème du manque d'accès aux fichiers concerne plusieurs services de renseignement. Or, il importe de renforcer l'efficacité opérationnelle de ces derniers. C'est pourquoi, globalement, les membres de la mission d'information sont ouverts à un élargissement de l'accès des services de

renseignement aux fichiers existants, compte tenu à la fois du caractère stratégique de ces fichiers pour ces services et de la persistance, à un haut niveau, des menaces qui pèsent sur la sécurité nationale, à commencer par la menace terroriste.

De manière plus spécifique, la mission d'information propose :

– de permettre à la direction du renseignement et de la sécurité de la défense d'accéder au traitement ACCReD, ce qui favorisera l'accélération de ses enquêtes administratives et facilitera la gestion des dossiers de demandes d'habilitation dont cette direction est chargée ;

– que le fichier national des détenus, qui est une extraction du traitement GENESIS de l'administration pénitentiaire et qui permet aux officiers de police judiciaire de la police et de la gendarmerie d'avoir accès à quelques catégories de données collectées dans ce traitement, soit utilisable par les services de renseignement de la direction générale de la police nationale ;

– de prévoir explicitement que la DGSI peut accéder aux fichiers PASP (article R. 236-16 du code de la sécurité intérieure) et GIPASP (article R. 236-26 du même code).

Proposition n° 9

Renforcer l'accessibilité de certains fichiers nécessaires aux missions des services de renseignement.

C. RENFORCER LES POSSIBILITÉS D'INTERCONNEXION DES FICHIERS DES SERVICES DE RENSEIGNEMENT

L'interconnexion des fichiers est stratégique pour les services de renseignement. Elle favorise leur collaboration étroite et la mutualisation du fruit de leurs investigations. Comme nous l'avons vu en deuxième partie du rapport, l'interconnexion des fichiers poursuit plusieurs objectifs : l'échange d'informations automatiques entre différents services, la mutualisation de l'alimentation de différents fichiers, la mise à jour automatique des données, la consultation simultanée des fichiers et le recoupement des informations.

La question de l'élargissement des possibilités d'interconnexion étant régulièrement abordée dès lors qu'on traite de renseignement, la mission estime qu'il est grand temps de faire évoluer notre droit afin de répondre aux besoins des services.

Il n'est pas indispensable de modifier la loi pour élargir le champ des interconnexions. Il suffit d'encadrer les interconnexions par voie réglementaire en modifiant les textes régissant les fichiers de renseignement

concernés, tout en maintenant le cadre législatif actuel – à condition, toutefois, d'exclure une interconnexion généralisée de tous les fichiers visés.

Dans cette hypothèse, plusieurs conditions doivent être remplies :

– les agents des autres services que ceux qui mettent en œuvre un traitement, qui sont habilités à procéder à une interconnexion de fichiers, doivent être mentionnés par les dispositions réglementaires relatives aux destinataires des traitements concernés ;

– l'interconnexion elle-même doit être prévue par le texte réglementaire qui régit ledit traitement ;

– l'interconnexion et ses modalités de mise en œuvre (finalités, données concernées, mesures de sécurité) doivent être portées à la connaissance de la CNIL lors de la modification de l'arrêté ou du décret en Conseil d'État relatif à chaque traitement concerné par l'interconnexion ;

– le texte réglementaire doit préciser que l'interconnexion doit, pour être effectuée, être justifiée par les besoins spécifiques des services – ce, afin d'éviter un détournement des finalités d'un fichier.

Si l'objectif est de faire du criblage, la création d'interfaces dites « *hit*/*no hit* », c'est-à-dire d'interfaces permettant la consultation automatique et simultanée de plusieurs fichiers de renseignement aux seules fins de vérifier si l'identité de la personne concernée y est enregistrée, devra être assortie de plusieurs garanties :

– ces interfaces devront être circonscrites dans leur périmètre, dans le respect des principes de finalité, de nécessité et de proportionnalité ;

– aucune décision juridique ne devra être exclusivement fondée sur de telles interfaces ;

– des mesures de sécurité rigoureuses devront être prévues afin de prévenir le risque d'interceptions ou d'attaques : il s'agira de prévoir des mesures de confidentialité des transmissions, de traçabilité des consultations automatiques et d'habilitation des personnels autorisés à accéder à des données.

Par ailleurs, il serait également possible de modifier la partie législative du livre VIII du code de la sécurité intérieure afin de préciser que « pour les besoins de l'accomplissement de leurs missions, les services de renseignement peuvent interconnecter leurs fichiers ».

Enfin, **modifier les textes réglementaires – et, le cas échéant, les textes législatifs – pour favoriser les interconnexions de fichiers permettrait d'apporter une assise juridique forte aux interconnexions plus approfondies que les simples interfaces *hit/no hit*.**

Proposition n° 10

Modifier les textes réglementaires et, le cas échéant, les textes législatifs, afin d'élargir, en les encadrant, les possibilités d'interconnexion de fichiers des services de renseignement.

VI. LA MISSION PLAIDE POUR LA CRÉATION D'UN RÉGIME PERMETTANT LA RECHERCHE-DÉVELOPPEMENT À PARTIR DE DONNÉES RÉELLES

Comme nous l'avons indiqué en deuxième partie du rapport, les services de renseignement souhaiteraient pouvoir faire de la recherche-développement afin d'entraîner leurs outils d'intelligence artificielle et ainsi traiter plus efficacement la masse de données qu'ils captent. Cet entraînement suppose de prévoir dans la loi une exception aux durées de conservation des données prévues par le droit commun. Ce régime, nécessaire à des strictes fins de recherche, d'analyse et de test, nécessaire à la phase d'apprentissage des outils d'intelligence artificielle, sera à distinguer strictement du régime de droit commun des données qui pourra s'appliquer à la phase opérationnelle d'usage des outils d'IA.

La mission d'information souhaite en outre que ce régime dérogatoire de conservation des données soit assorti de garanties très strictes : il s'agira en particulier d'exclure explicitement tout usage opérationnel des données d'entraînement. Les opérations de recherche, d'analyse et de test ne devront être réalisées qu'après autorisation du ministre de tutelle du service demandeur – soit le ministre de l'intérieur, le ministre des armées ou le ministre de l'économie – par des agents habilités et après déclaration à la CNCTR (comme le prévoit déjà la loi pour les tests de la DGA). Les modalités d'application du dispositif pourraient être précisées par le pouvoir réglementaire, s'agissant notamment des modalités de pseudonymisation des données conservées et du fait que les agents habilités à effectuer ces opérations doivent être un tiers de confiance indépendant des services de renseignement.

Proposition n° 10

Définir un régime dérogatoire de conservation des données à des fins de recherche, d'analyse et de test nécessaire à la phase d'apprentissage des outils d'intelligence artificielle utilisés pour traiter les données captées par les services de renseignement.

VII. LA MISSION JUGE NÉCESSAIRE DE PROROGER LA TECHNIQUE DE L'ALGORITHME

Les membres de la mission d'information savent que cette technique de renseignement a suscité beaucoup de débats en 2015. À la suite de leurs travaux, ils estiment qu'**il faut démythifier l'algorithme : ce n'est pas un outil de surveillance de masse, mais de détection de signaux faibles,** qui pourra ensuite

justifier l'usage d'une technique de renseignement, dans le cadre du droit commun.

Les membres de la mission n'ont pas souhaité qu'une éventuelle prorogation de l'algorithme puisse être décidée par le gouvernement au moyen d'une ordonnance (1) : **un débat parlementaire est nécessaire** pour qu'une disposition législative puisse le prévoir. Le présent rapport se propose de l'éclairer.

A. PROLONGER LA MISE EN ŒUVRE DE L'ALGORITHME : UNE NÉCESSITÉ OPÉRATIONNELLE

1. Une mise en œuvre encore limitée, mais qui commence à produire des résultats

Comme on l'a vu dans la première partie du rapport, le premier algorithme a été autorisé le 12 octobre 2017 seulement. Il s'agit donc encore, pour reprendre l'expression utilisée par l'un des directeurs d'un service de renseignement, d'un « *jeune enfant* ». Cette mise en œuvre tardive a justifié que la loi du 30 octobre 2017 précitée prolonge l'expérimentation de ce dispositif, qui devait initialement s'éteindre fin 2018, jusqu'au 31 décembre 2020.

Cet outil a fait l'objet d'une mise en œuvre relativement limitée puisqu'à la fin de l'année 2019, **trois algorithmes** avaient été mis en œuvre depuis l'entrée en vigueur de la loi du 24 juillet 2015 et étaient en fonctionnement, même si le secret-défense ne permet pas de détailler ici le périmètre de ces algorithmes.

Le soupçon initial d'une surveillance de masse des Français relève donc du fantasme. Les services français, pour reprendre une expression employée lors d'une audition, ne pratiquent pas la surveillance mondiale car « *ils n'en ont pas les moyens et qu'ils n'y ont pas intérêt* ». L'algorithme, dans l'architecture qui a été retenue, est un **outil de détection** ciblée – et non de surveillance – **en fonction de paramètres déterminés et dans un seul objectif : révéler une menace terroriste**.

Est–ce que ces algorithmes ont d'ores et déjà produit des résultats dans la lutte contre le terrorisme ? La mission comprend de ses échanges avec les services de renseignement que la réponse à cette question n'est pas négative, même si nous ne sommes encore qu'au début de l'utilisation de cette technique, et que les services disent opérer *« avec des enclumes et des poids aux chevilles* ».

---

(1) Les membres de la mission ont déposé un amendement à cette fin, en mai 2020, lors de l'examen du projet de loi nº 2907 portant diverses dispositions urgentes pour faire face aux conséquences de l'épidémie de covid-19.

2. Une nécessaire prolongation de l'algorithme

Dès lors, faut-il prolonger la technique de renseignement de l'algorithme ? Les membres de la mission d'information en sont convaincus, car la menace qu'il permet de prendre en compte, le terrorisme, n'est évidemment pas derrière nous. **Le volume de données que l'algorithme permet d'appréhender ne peut pas l'être par des moyens classiques.**

En effet, même si les trois algorithmes en cours n'ont pas encore atteint leur pleine mesure (1), ils se révèlent malgré tout **très prometteurs. Si elle renonçait à cette faculté, la France se priverait d'une grande chance et prendrait du retard par rapport aux puissances partenaires.**

B. CONSERVER LES GRANDS ÉQUILIBRES DU DISPOSITIF ACTUEL

1. Une procédure dorénavant rodée

Lorsque l'un algorithme déclenche une alerte, le GIC la notifie au service bénéficiaire de l'autorisation. L'alerte en elle-même ne contient ni ne révèle les données qui l'ont déclenchée. À partir de cette information minimale, le service peut demander d'accéder aux données à l'origine de l'alerte. Il a été observé que la demande de levée de doute est systématique car les alertes ont porté sur un nombre relativement faible de données de connexion. Elle est soumise à l'avis de la CNCTR puis à l'autorisation du Premier ministre. Dès que l'autorisation est prononcée, le GIC réunit les données et les communique au service. Ce ne sont que des données de connexion dépourvues de tout contenu.

Selon le directeur du GIC, « *le dispositif tourne, sous le contrôle de la CNCTR* » (2). La CNCTR a confirmé cette appréciation.

Dès lors, il n'est pas apparu opportun aux membres de la mission d'information de proposer des modifications dans la procédure d'autorisation ou dans le fonctionnement de l'algorithme.

2. Étendre les finalités justifiant la mise en œuvre de l'algorithme ?

Aujourd'hui, la mise en œuvre de l'algorithme est limitée à la finalité de prévention du terrorisme.

Ici et là, des voix s'élèvent pour demander une extension de l'utilisation de l'algorithme à d'autres finalités que celle actuellement prévue à l'article L. 851–3 du code de la sécurité intérieure. Il pourrait en effet se révéler particulièrement utile en matière de contre-espionnage et de criminalité organisée.

---

(1) Aujourd'hui, les algorithmes ne sont mis en œuvre que sur les données téléphoniques même si la loi permet qu'ils soient mis en œuvre à partir de données de connexion.

(2) Audition de M. Pascal Chauve, directeur du GIC, par les membres de la mission d'information.

Par ailleurs, si la jurisprudence *Tele2* de la CJUE devait être confirmée, seule cette technique algorithmique permettrait de suppléer aux difficultés que représenterait la disparition de certaines techniques de renseignement actuellement utilisées par les services.

Pour autant, les membres de la mission d'information n'ont pas retenu cette option à ce stade. À moyen terme, il paraît préférable de conserver les grands équilibres du régime actuel, ciblé sur la lutte antiterroriste.

C. ÉTENDRE L'ALGORITHME AUX URL

1. La question du périmètre des données de connexion

L'article L. 851-3 du CSI permet de détecter des connexions susceptibles de révéler une menace terroriste. Il est précisé que l'algorithme utilise exclusivement les données de connexion, « *sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent*. »

La définition des données de connexion figure à l'article L. 34-1 du code des postes et des communications électroniques [(1)] mais elle ne permet pas d'épuiser entièrement **le débat entre ce qui relève du contenant et du contenu**. Or, cette question s'est posée avec une particulière acuité lors de la mise en œuvre de l'algorithme. Elle est relativement simple s'agissant des données téléphoniques (fadettes) mais plus compliquée s'agissant d'internet. Pour le dire de manière la plus claire possible, familière à tous les usagers d'un moteur de recherche : **à partir de quelle barre oblique (« slash ») de l'URL une donnée cesse–t–elle d'être une donnée de connexion pour devenir une donnée de correspondances ?**

2. L'extension de l'algorithme aux URL

Un algorithme fonctionnant uniquement avec des données téléphoniques est intéressant mais il n'apporte pas aux enquêteurs un niveau de finesse et de pertinence suffisant. Les services de renseignement estiment qu'il leur serait extrêmement utile de pouvoir intégrer les URL aux algorithmes. L'URL révélant les données consultées, une telle extension demanderait une modification législative.

---

(1) « VI. – Les données conservées et traitées *(…)* portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. »

La mission d'information relève qu'**il existe déjà des techniques de renseignement qui permettent d'avoir accès aux correspondances électroniques et aux données informatiques.**

La question porte sur l'application de l'algorithme car celui–ci permet un changement de l'ampleur, cette technique de renseignement ne ciblant pas une personne.

Les membres de la mission pensent que le système actuel offre des garanties importantes, avec un triple sas. La CNCTR exerce un contrôle sur les paramètres de l'algorithme ainsi que sur la levée de l'anonymat de la personne détectée par l'algorithme puisque, lorsqu'il y a un « *hit* », il faut une autorisation nouvelle pour savoir qui a été détecté. Enfin, il faut une autorisation pour recourir à une technique de renseignement concernant cette personne. Il faut donc trois autorisations pour suivre un individu.

Si une telle extension devait être décidée, les membres de la mission estiment que cela justifierait de conserver le caractère expérimental de l'algorithme pour une durée de cinq ans.

Proposition n° 12

Étendre le champ de l'algorithme aux URL. En conséquence, prolonger l'expérimentation de l'algorithme pendant cinq ans.

Par voie de conséquence, **si cette extension aux URL était apportée à l'article L. 851-3 du CSI, il paraîtrait pertinent de l'apporter également à une autre technique de renseignement, celle prévue à l'article L. 851–2 et qui concerne le recueil des données de connexion d'un individu en temps réel**. Comme l'algorithme, cette technique de renseignement est limitée à la prévention du terrorisme.

Elle permet aujourd'hui de recueillir des informations intéressantes sur le comportement numérique de personnes radicalisées : est-ce que cet individu sort d'un périmètre défini, entre-t-il en contact avec une personne définie, a–t–il une consommation internet de nuit, sa consommation internet change–t–elle ?

Il serait utile aux services de renseignement, dans le cadre limité de la prévention du terrorisme, de disposer également des URL s'agissant de ces personnes.

En revanche, eu égard à l'atteinte à la vie privée représentée par cette extension, il conviendrait de la restreindre aux seules personnes ayant un lien avec la menace terroriste. Elle ne pourrait pas s'appliquer à leur entourage.

Proposition n° 13

Étendre le champ du recueil de données de connexion en temps réel des personnes susceptibles d'être en lien avec une menace terroriste aux URL.

CONCLUSION

Au terme de la présentation de ce bilan législatif, les membres de la mission d'information souhaitent remercier l'ensemble de leurs interlocuteurs, présentés en annexe du rapport, pour leur disponibilité et la clarté de leurs analyses d'un texte d'application somme toute assez récente.

Ils tiennent aussi à insister sur l'esprit de consensus qui a régné entre eux tout au long de leurs travaux, aussi bien dans la phase d'auditions que dans celle de l'élaboration de leur rapport. Cet esprit doit, selon eux, perdurer dans le cadre des débats à venir sur le droit du renseignement.

En effet, l'article L. 851-3 du code de la sécurité intérieure n'est en vigueur que jusqu'au 31 décembre 2020. Le législateur aura donc à se prononcer prochainement sur cette disposition.

Les membres de la mission d'information estiment important que ce véhicule législatif constitue une opportunité d'examiner au fond les différentes possibilités d'évolution du cadre de la loi du 24 juillet 2015 et ne se limite pas à la prorogation pour quelques mois d'une seule des techniques de recueil de renseignement.

Ce débat doit fédérer le plus largement possible les partis de gouvernement, par-delà les clivages partisans, afin de faire œuvre utile et de garantir l'équilibre entre sécurité et libertés des Français.

TRAVAUX DES COMMISSIONS

Lors de leur réunion du mardi 9 juin 2020, la commission des Lois et la commission de la Défense ont examiné ce rapport d'information et en ont autorisé la publication.

Ces débats ne font pas l'objet d'un compte rendu écrit et sont accessibles sur le portail vidéo du site de l'Assemblée à l'adresse suivante :

http://assnat.fr/yrgFVi

LISTE DES PROPOSITIONS DE LA MISSION D'INFORMATION

Proposition n° 1 : Consacrer la possibilité d'un droit de visite pour les membres de la formation spécialisée du Conseil d'État dans le code de justice administrative.

Proposition n° 2 : Inscrire dans le code de la sécurité intérieure les évolutions en matière de centralisation par le GIC.

Proposition n° 3 : Clarifier la rédaction de l'article L. 863-2 du code de la sécurité intérieure en y précisant les modalités du partage d'informations entre services de renseignement.

Proposition n° 4 : Prévoir une durée maximale de conservation unique de 120 jours pour les données collectées par les dispositions de captation de parole et ceux de captation d'images prévus à l'article L. 853–1 du code de la sécurité intérieure.

Proposition n° 5 : Prévoir un avis par un membre de la CNCTR statuant seul s'agissant des demandes de retrait d'un dispositif technique nécessitant l'introduction dans un lieu d'habitation (article L. 853–3 du code de la sécurité intérieure).

Proposition n° 6 : Augmenter la durée de l'autorisation prévue sur le fondement de III de l'article L. 854–2 du code de la sécurité intérieure à un an.

Proposition n° 7 : Porter à deux mois la durée de l'autorisation permettant de mettre en œuvre le recueil de données informatiques.

Proposition n° 8 : Prévoir un droit d'accès indirect aux fichiers auxquels une restriction au droit d'accès direct est systématiquement appliquée et préciser par voie réglementaire le régime juridique applicable à chaque fichier.

Proposition n° 9 : Renforcer l'accessibilité de certains fichiers nécessaires aux missions des services de renseignement.

Proposition n° 10 : Modifier les textes réglementaires et, le cas échéant, les textes législatifs, afin d'élargir, en les encadrant, les possibilités d'interconnexion de fichiers des services de renseignement.

Proposition n° 11 : Définir un régime dérogatoire de conservation des données à des fins de recherche, d'analyse et de test nécessaire à la phase d'apprentissage des outils d'intelligence artificielle utilisés pour traiter les données captées par les services de renseignement.

Proposition n° 12 : Étendre le champ de l'algorithme aux URL. En conséquence, prolonger l'expérimentation de l'algorithme pendant cinq ans.

Proposition n° 13 : Étendre le champ du recueil de données de connexion en temps réel des personnes susceptibles d'être en lien avec une menace terroriste aux URL.

ANNEXE N° 1 : PERSONNES AUDITIONNÉES, DÉPLACEMENT ET CONTRIBUTIONS ÉCRITES

1. Personnes auditionnées [(1)]

- **Commission nationale de contrôle des techniques de renseignement - CNCTR**

  — M. Francis Delon, président

- **Coordonnateur ministériel en matière d'intelligence artificielle au ministère de l'Intérieur**

  — M. Renaud Vedel, préfet

- **Coordination nationale du renseignement et de la lutte contre le terrorisme**

  — M. Pierre de Bousquet de Florian, coordonnateur national

- **Direction des affaires criminelles et des grâces du ministère de la Justice**

  — Mme Catherine Pignon, directrice

- **Direction des affaires juridiques du ministère des Armées**

  — Mme Claire Legras, directrice

- **Direction générale de la sécurité extérieure**

  — M. Bernard Émié, directeur général

- **Direction générale de la sécurité intérieure**

  — M. Nicolas Lerner, directeur général

- **Direction des libertés publiques et des affaires juridiques du ministère de l'Intérieur**

  — M. Thomas Campeaux, directeur

- **Direction nationale du renseignement et des enquêtes douanières**

  — Mme Corinne Cléostrate, directrice

- **Direction du renseignement militaire**

  — M. le général Jean-François Ferlet, directeur

(1) Les auditions sont présentées par ordre alphabétique.

- **Direction du renseignement de la préfecture de police**

— Mme Françoise Bilancini, directrice

- **Direction du renseignement et de la sécurité de la défense**

— M. le général Éric Bucquet, directeur

- **Groupement interministériel de contrôle**

— M. Pascal Chauve, directeur

- **Secrétariat général de la défense et de la sécurité nationale**

— Mme Claire Landais, secrétaire générale

- **Service central du renseignement territorial de la direction générale de la police nationale**

— Mme Lucile Rolland, chef de service

- **Service national du renseignement pénitentiaire du ministère de la Justice**

— M. Stéphane Bredin, directeur de l'administration pénitentiaire

- **Sous-direction de l'anticipation opérationnelle de la direction générale de la gendarmerie nationale**

— M. le général Jean-Marc Cesari, sous-directeur

- **Traitement du renseignement et action contre les circuits financiers clandestins**

— Mme Maryvonne Le Brignonen, directrice

2. Déplacement

- **Groupement interministériel de contrôle**

— M. Pascal Chauve, directeur

3. Contributions écrites

- **Commission nationale de l'informatique et des libertés**

— M. Louis Dutheillet de Lamothe, secrétaire général

- **Conseil d'État**

— M. Edmond Honorat, président de la formation spécialisée du Conseil d'État chargée du contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État

- **Direction des affaires juridiques du ministère de l’Europe et des Affaires étrangères**

— M. François Alabrune, directeur

- **Direction générale de la police nationale**

— M. Frédéric Veaux, directeur général

ANNEXE N° 2 :
ÉCHÉANCIER DE MISE EN APPLICATION DE LA LOI

Articles	Base légale	Objet	Objectif initial de publication / Décrets publiés / Observations
Article 2	Article L. 811-2, code de la sécurité intérieure	Désignation des services spécialisés de renseignement.	Décret n° 2015-1185 du 28/09/2015
Article 2	Article L. 811-4, code de la sécurité intérieure	Services autres que les services spécialisés de renseignement, relevant des ministres de la défense et de l'intérieur ainsi que des ministres chargés de l'économie, du budget ou des douanes autorisés à recourir aux techniques de recueil de renseignement mentionnées au titre V.	Décret n° 2015-1639 du 11/12/2015
Article 2	Article L. 841-2, code de la sécurité intérieure	Liste des traitements ou parties de traitement intéressant la sûreté de l'État dont les contentieux relatifs au droit d'accès indirect relèvent du Conseil d'État.	Décret n° 2015-1808 du 28/12/2015
Article 5	article L. 851-1, code de la sécurité intérieure	Modalités relatives à l'accès administratif aux données de connexion.	Décret n° 2016-67 du 29/01/2016
Article 6	Article L. 853-1, III, code de la sécurité intérieure	Liste des services auxquels doivent appartenir les agents habilités à utiliser des 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.	Décret n° 2015-1185 du 28/09/2015
Article 6	Article L. 853-1, III, code de la sécurité intérieure	Liste des services auxquels doivent appartenir les agents habilités à utiliser des 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.	Décret n° 2015-1639 du 11/12/2015
Article 6	Article L. 853-2, III, code de la sécurité intérieure	Liste des services auxquels doivent appartenir les agents habilités à utiliser des dispositifs techniques permettant l'accès et le traitement de données informatiques.	Décret n° 2015-1185 du 28/09/2015
Article 6	Article L. 853-2, III, code de la sécurité intérieure	Liste des services auxquels doivent appartenir les agents habilités à utiliser des dispositifs techniques permettant l'accès et le traitement de données informatiques.	Décret n° 2015-1639 du 11/12/2015
Article 6	Article L. 853-3, I, code de la sécurité intérieure	Liste des services auxquels doivent appartenir les agents habilités à s'introduire dans un véhicule ou dans un lieu privé.	Décret n° 2015-1185 du 28/09/2015
Article 6	Article L. 853-3, I, code de la sécurité intérieure	Liste des services auxquels doivent appartenir les agents habilités à s'introduire dans un véhicule ou dans un lieu privé.	Décret n° 2015-1639 du 11/12/2015
Article 8, V	Article L. 863-2, code de la sécurité intérieure	Détermination des modalités et des conditions d'échanges d'informations entre les services de renseignement et les autres autorités	

		administratives.	
Article 10, 2°	Article L. 773-2 du code de justice administrative	Contentieux de la mise en œuvre des techniques de renseignement : composition de la formation spécialisée et de la formation restreinte de l'assemblée du contentieux ou de la section du contentieux du Conseil d'État.	Décret n° 2015-1211 du 01/10/2015
Article 19, I	Article 706-25-14 du code de procédure pénale	Modalités et conditions d'utilisation du fichier judiciaire national automatisé des auteurs d'infractions terroristes et conditions de conservation de la trace des interrogations et des consultations dont le fichier a fait l'objet.	Décret n° 2015-1840 du 29/12/2015
Article 19 II , B		Délai à partir duquel peut être saisi le président de la chambre de l'instruction.	Décret n° 2015-1840 du 29/12/2015
Article 20	Article L. 234-4, code de la sécurité intérieure	Détermination des services pouvant avoir accès aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6 du code de procédure pénale et modalités d'accès.	Décret n° 2015-1807 du 28/12/2015

Source : https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000030375694&type=echeancier&typeLoi=&legislature=14

Date de dernière mise à jour des décrets publiés : 08/02/2016

ANNEXE N° 3 :
LES LOIS AYANT MODIFIÉ LA LOI DU 24 JUILLET 2015

1. Loi n° 2015–1536 du 30 novembre 2015 relative aux mesures de surveillance des communications internationales : conséquence de la censure du Conseil constitutionnel

2. Article 14 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale : intégration du renseignement pénitentiaire au second cercle

3. Article 15 de la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste : élargissement de la technique de recueil de données de connexion en temps réel

4. Article 39 de la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes : modification des dispositions applicables à la CNCTR

5. Article 35 de la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique : finalités propres au renseignement pénitentiaire

6. Articles 5, 15 et 17 de la loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme :

– création d'une nouvelle technique de renseignement sur l'hertzien privatif ;

– prolongation de l'expérimentation de l'algorithme ;

– encadrement du recueil des données de connexion de l'entourage ;

– élargissement du périmètre de la captation de données informatiques.

7. Articles 36 et 37 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense :

– vérifications ponctuelles sur les seules données de connexion légalement interceptées dans le cadre de la surveillance des communications internationales aux seules fins de détecter une menace pour les intérêts fondamentaux de la Nation liée aux relations entre des numéros d'abonnement ou des identifiants techniques rattachable au territoire français et des zones géographiques, des organisations ou des personnes faisant l'objet d'une surveillance internationale ;

– nouvelle mesure de surveillance individuelle ;

– mise en cohérence de l’exploitation de certaines données ;

– régime de test des appareils ;

– extension du contrôle a priori de la CNCTR.

8. Article 89 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice : mise en œuvre du renseignement pénitentiaire.

ANNEXE N° 4 : LES FINALITÉS PERMETTANT L'UTILISATION DE TECHNIQUES DE RENSEIGNEMENT

Art. L. 811.3 CSI	Finalités
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 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 (ADM)
Art. L. 855–1 CSI	**Finalités spécifiques au renseignement pénitentiaire**
	La prévention des évasions et le maintien de la sécurité au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.

ANNEXE N° 5 : LES TECHNIQUES DE RECUEIL DE RENSEIGNEMENT

Disposition du code de la sécurité intérieure	Techniques
Chapitre I^er^ : Des accès administratifs aux données de connexion	
Article L. 851–1	Accès aux données techniques de connexion (DC)
Article L. 851–2	Accès aux données techniques de connexion (DC) en temps réel
Article L. 851–3	Algorithme
Article L. 851–4	Géolocalisation en temps réel
Article L. 851–5	Balisage
Article L. 851–6	*IMSI-catcher* aux fins de recueil des données techniques de connexion
Chapitre II : Des interceptions de sécurité	
Article L. 852–1	Interceptions de sécurité (IS)
	Interceptions de sécurité (IS) au moyen d'un IMSI–catcher
Article L. 852–2	Interceptions de sécurité (IS) hertzien privatif
Chapitre III : De la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques	
Article L. 853–1	Sonorisations de lieux ou véhicules privés ou publics Fixations d'images dans un lieu privé
Article L. 853–2	1° Recueil de données informatique (RDI) – stock : accéder à des données informatiques stockées dans un système informatique, les enregistrer, les conserver et les transmettre
	2° Captation de données informatiques (CDI) –flux : accéder à des données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran
Article L. 853–3	Introduction dans un lieu privé (ILP) pour mettre ou retirer un dispositif
Chapitre IV : Des mesures de surveillance internationale	
Article L. 854–1	Surveillance des communications qui sont émises ou reçues à l'étranger (communications + DC)
Article L. 854–2	(II) Exploitation non individualisée des DC, (III) Exploitation des communications ou des DC, (IV) Vérifications ponctuelles des DC + communications (V) Exploitations communications + DC
Chapitre V : Des mesures de surveillance de certaines communications hertziennes	
Article L. 855-1 A	Interception et exploitation des communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques

ANNEXE N° 6 : LES CARACTÉRISTIQUES DES TECHNIQUES DE RENSEIGNEMENT

Disposition CSI	Techniques	Finalité	Contingentement	Centralisation	Entourage
Art. L. 851–1	Accès aux données techniques de connexion	Toutes	Non	Oui	Non
Art. L. 851–2	Accès aux données techniques de connexion en temps réel	Prévention du terrorisme	Oui	L. 871– 6	Oui
Art. L. 851–3	Algorithme	Prévention du terrorisme	Non	L. 871– 6	N/A
Art. L. 851–4	Géolocalisation en temps réel	Toutes	Non	Oui	Non
Art. L. 851–5	Balisage	Toutes	Non	Non	Non
Art. L. 851–6	*IMSI-catcher* aux fins de recueil des données techniques de connexion	Toutes	Oui	Oui	Non
Art. L. 852–1	Interceptions de sécurité (IS)	Toutes	Oui	Oui	Oui
	Interceptions de sécurité (IS) au moyen d'un IMSI–catcher	Indépendance nationale / Terrorisme / Atteintes à la forme républicaine des institutions	Oui	Oui	Oui
Art. L. 852–2	Interceptions de sécurité (IS) hertzien privatif	Toutes	Non	Non	N/A
Art. L. 853–1	Sonorisations de lieux ou véhicules privés ou publics Fixations d'images dans un lieu privé	Toutes	Non	Non	Non
Art. L. 853–2	1° Recueil de données informatique (RDI)	Toutes	Non	Non	Non
	2° Captation de données informatiques (CDI)	Toutes	Non	Non	Non
Art. L. 853–3	Introduction dans un lieu privé (ILP) pour mettre ou retirer un dispositif	Toutes	Non	Non	Non
Art. L. 854–2	Surveillance des communications internationales (IS + DC)	II (Toutes) III (Toutes) IV (Prévention du terrorisme + cyberattaque/indépendance nationale) V (Indépendance nationale / Terrorisme / intérêts majeurs de la politique étrangère/ prévention criminalité organisée et prolifération ADM)	V (oui)	Oui	N/A
Art. L. 855-1 A	Interception et exploitation des communications électroniques empruntant exclusivement la voie hertzienne	Toutes	Non	Non	N/A

ANNEXE N° 7 : LES DURÉES D'AUTORISATION ET DURÉES DE CONSERVATION

Disposition CSI	Techniques	Durée d'autorisation initiale	Durée de conservation des données	Exception déchiffrement
Art. L. 851–1	Accès aux données techniques de connexion	4 mois	4 ans	6 ans (à compter de leur recueil)
Art. L. 851–2	Accès aux données techniques de connexion en temps réel	4 mois	N/A	
Art. L. 851–3	Algorithme	2 mois	60 jours (+ si menace sérieuse)	
Art. L. 851–4	Géolocalisation en temps réel	4 mois	N/A	
Art. L. 851–5	Balisage	4 mois	N/A	
Art. L. 851–6	*IMSI-catcher* aux fins de recueil des données techniques de connexion	2 mois	4 ans /90 jours si pas en rapport avec l'autorisation	
Art. L. 852–1	Interceptions de sécurité (IS)	4 mois	30 jours	
	Interceptions de sécurité (IS) au moyen d'un IMSI–catcher	48 heures	30 jours	
Art. L. 852–2	Interceptions de sécurité (IS) hertzien privatif	4 mois	30 jours	
Art. L. 853–1	Sonorisations de lieux ou véhicules privés ou publics Fixations d'images dans un lieu privé	2 mois	30 jours (paroles) 120 jours (images)	
Art. L. 853–2	1° Recueil de données informatique (RDI)	30 jours	120 jours	
	2° Captation de données informatiques (CDI)	2 mois	120 jours	
Art. L. 853–3	Introduction dans un lieu privé (ILP) pour mettre ou retirer un dispositif	30 jours	N/A	N/A
Art. L. 854–2	(II) Exploitation non individualisée des DC	1 an	12 mois pour les correspondances, dans la limite de 4 ans à partir de leur recueil 6 ans pour les DC	8 ans (à compter du recueil)
	(III) Exploitation des IS ou des DC	4 mois		
	(IV) Vérifications ponctuelles des DC	4 mois		
	V (Exploitation IS + DC)	4 mois		
Art. L. 855-1 A	Interception et exploitation des communications électroniques empruntant exclusivement la voie hertzienne	N/A	6 ans	8 ans (à compter du recueil)

ANNEXE N° 8 :
LE FICHIER ACCRED (DÉCRET N° 2017-1224 DU 3 AOÛT 2017 (1))

La DGPN et la DGGN du ministère de l'intérieur sont autorisées à mettre en œuvre le traitement « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD) ayant pour finalité de faciliter la réalisation d'enquêtes administratives précédant des décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'État, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, soit les emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes ou d'une entreprise de transport de marchandises dangereuses soumise à l'obligation d'adopter un plan de sûreté, soit l'accès de personnes à de grands événements exposés, par leur ampleur ou leurs circonstances particulières, à un risque exceptionnel de menace terroriste. Les données figurant dans le fichier peuvent être conservées pendant cinq ans à compter de leur enregistrement, sauf en cas de contentieux.

Sont autorisés à accéder à tout ou partie des données du fichier :

– les agents du service national des enquêtes administratives de sécurité habilités par le directeur général de la DGPN ;

– les agents du commandement spécialisé pour la sécurité nucléaire habilités par le directeur général de la DGGN.

Peuvent être destinataires de tout ou partie de ces mêmes données, dans la limite du besoin à en connaître :

– tout autre agent du ministère de l'intérieur chargé d'effectuer les enquêtes administratives précitées ;

– les personnes morales ou l'autorité administrative à l'origine de la demande, pour les seules données relatives au sens de l'avis ou de la décision ou, le cas échéant, pour les seules données relatives aux résultats de l'enquête administrative ;

– le préfet de département du lieu d'exercice de l'emploi, de la mission ou de la fonction de la personne à l'origine de la demande d'avis.

Le traitement ACCReD peut procéder à la consultation automatique et, le cas échéant, simultanée des traitements suivants, aux seules fins de vérifier si l'identité de la personne concernée y est enregistrée :

– le traitement des antécédents judiciaires (TAJ) ;

– le fichier des enquêtes administratives liées à la sécurité publique (EASP) ;

(1) L'article 7 du décret du 3 août 2017 a été modifié par l'article 6 du décret n° 2019-1074 du 21 octobre 2019.

– le fichier de prévention des atteintes à la sécurité publique (PASP) ;

– le fichier de gestion de l'information et prévention des atteintes à la sécurité publique (GIPASP) ;

– le fichier des personnes recherchées (FPR) ;

– le fichier de signalement pour la prévention de la radicalisation à caractère terroriste (FSPRT) ;

– le fichier des objets et véhicules volés ou signalés (FOVeS).

Le fichier ACCReD peut être mis en relation, sous la forme d'une interrogation, par les agents du SNEAS habilités par le DGPN et les agents du commandement spécialisé de la sécurité nucléaire habilités par le DGGN, avec les fichiers suivants :

– le fichier CRISTINA (Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux) ;

– le fichier GESTEREXT (Gestion du terrorisme et des extrémismes à potentialité violente) ;

– le fichier SIREX ;

– le fichier de la DGSE.

Le droit d'accès à ACCReD s'exerce de manière indirecte auprès de la CNIL.

ANNEXE N° 9 : LE DROIT APPLICABLE AUX FICHIERS INTÉRESSANT LA SÛRETÉ DE L'ÉTAT, LA DÉFENSE OU LA SÉCURITÉ PUBLIQUE

Le droit applicable aux fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique

La notion de **« fichiers de souveraineté »** n'existe pas en tant que telle en droit positif. Elle peut renvoyer à plusieurs catégories de traitements de données à caractère personnel, et en particulier, aux traitements de données à caractère personnel qui bénéficient d'une ou plusieurs des dérogations au cadre général des **fichiers régaliens ou de la sphère répressive** mis en œuvre par l'État, prévu par la loi « Informatique et Libertés ».

L'article 31 de la loi du 6 janvier 1978 modifiée concerne les traitements mis en œuvre par l'État qui « **intéressent la sûreté de l'État, la défense ou la sécurité publique** » ou « **qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté** ».

Juridiquement, ces traitements peuvent relever – parfois de manière cumulative – du champ d'application du RGPD (soit du titre II de la loi « Informatique et Libertés », comme par exemple certains traitements fiscaux poursuivant notamment une finalité de lutte contre la fraude fiscale), du champ d'application de la directive « Police-Justice » (titre III de la loi, comme par exemple les traitements d'antécédents judiciaires ou d'analyse sérielle mentionnés au code de procédure pénale) ou du « hors-champ » du droit de l'Union européenne (titre IV de la même loi, comme par exemple les traitements mis en œuvre par la DGSI ou la DGSE).

L'article 31 de la loi « Informatique et Libertés » constitue le droit commun de l'ensemble de ces fichiers « répressifs » et conditionne leur création ou leur modification à la prise d'un arrêté ministériel, ou d'un décret en Conseil d'État en cas de traitement de données « sensibles », pris après avis motivé et publié de la CNIL.

Ces traitements peuvent bénéficier d'une ou plusieurs des dérogations suivantes :

– les dossiers de saisine de la CNIL peuvent ne pas comporter tous les éléments habituellement portés à la connaissance de la CNIL dans le cadre des demandes d'avis qui lui sont adressées (dernier alinéa de l'article 33-I de la loi du 6 janvier 1978 modifiée) ; en particulier, la durée de conservation et les mesures de sécurité mises en œuvre peuvent ne pas être mentionnées dans le dossier de saisine (cf. article 67 du décret d'application de la loi).

– ils peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire en portant création ou modification (article 31-III de la loi « Informatique et Libertés »). Dans ce cas, seul le sens de l'avis de la CNIL, et non son intégralité, fait l'objet d'une publication ; ce sens ne peut porter que la mention « favorable », « favorable avec réserve » ou « défavorable » (article 70 du décret d'application de la loi).

Ils peuvent enfin ne pas être soumis au contrôle *a posteriori* de la CNIL (article 19-IV de la loi précitée) s'ils intéressent la sûreté de l'État et s'ils n'ont pas fait l'objet d'une publication dans les conditions précitées. Les prérogatives de contrôle de la Commission, applicables à tous les autres traitements, publics ou privés, visent à s'assurer du respect pratique des dispositions de la loi « Informatique et Libertés » ou des dispositions législatives ou réglementaires portant création de traitements, en permettant notamment aux agents de la CNIL de se rendre sur place et de se faire communiquer tout document utile à leurs investigations. Ces prérogatives ne sont pas applicables à certains traitements intéressant la sûreté de l'État.

La CNIL reste néanmoins compétente pour exercer certains contrôles, dans le cadre de l'exercice du droit d'accès indirect, qui permet de vérifier la licéité du traitement de données des personnes qui la saisissent (et non de l'ensemble des conditions de mise en œuvre du traitement, au-delà des cas particuliers). Cette mission permet ainsi un contrôle « par carottage » de ces traitements.

Les traitements bénéficiant de l'une ou de plusieurs de ces dérogations sont mentionnés dans le décret n° 2007-914 du 15 mai 2007 modifié. On peut considérer qu'ils constituent les « fichiers de souveraineté », qui seraient alors actuellement au nombre de quinze.

Cependant, trois nuances peuvent être apportées à une telle définition.

Tout d'abord, tous ces traitements ne sont pas nécessairement mis en œuvre, ni par des services spécialisés de renseignement. On retrouve notamment dans cette liste :

– des traitements mis en œuvre par ce qu'il est communément admis d'appeler des services du second cercle, voire par des services extérieurs au renseignement : par exemple, le traitement CAR de l'administration pénitentiaire (service national du renseignement pénitentiaire), le traitement GESTEREXT de la direction du renseignement de la préfecture de police ou le traitement LEGATO du commandement de la Légion étrangère ;

– des **traitements mis en œuvre à des fins qui ne relèvent pas, au sens strict, de la seule politique publique de renseignement : par exemple, les traitements PASP, de la DGPN, et GIPASP, de la DGGN**, de prévention des atteintes à la sécurité publique, ou encore le traitement ASTREE de la protection judiciaire de la jeunesse.

En outre, tous les traitements mentionnés dans cette liste ne bénéficient pas de l'ensemble des dérogations précitées.

D'une part, certains de ces traitements, tels que le PASP et le GIPSP, ne sont pas exonérés de l'obligation de publication du texte en portant création. D'autre part, certains de ces traitements sont soumis aux pouvoirs de contrôle *a posteriori* de la CNIL, comme par exemple les fichiers précités PASP et GIPASP mais également des traitements dont les textes régissant la mise en œuvre ne sont pas publiés tels que le fichier STARTRAC de Tracfin), le FSPRT, le fichier CAR et le fichier ASTREE.

Ainsi, si quinze traitements figurent dans le décret précité, treize d'entre eux ne font pas l'objet d'une publication et seuls neuf d'entre eux bénéficient de l'ensemble des dérogations précitées. Les « fichiers de souveraineté » peuvent donc renvoyer à l'une ou l'autre de ces trois « catégories » de traitements.

Enfin, cette liste ne comprend pas **certaines parties de traitements qui intéressent la sûreté de l'État et qui relèvent de la compétence de la formation spécialisée du Conseil d'État, s'agissant des requêtes concernant le droit d'accès des personnes aux données qui les concernent** (cf. article L. 841-2 du code de la sécurité intérieure). Les requêtes relatives aux données intéressant la sûreté de l'État (et non nécessairement à l'ensemble des données du traitement concerné) enregistrées dans le Fichier des personnes recherchées (fiches « S »), dans le Système informatique national du système d'information Schengen dénommé « N-SIS II » ou dans le traitement « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD), relèvent, conformément aux dispositions de l'article R. 841-2 dudit code, de la compétence de cette formation spécialisée. **Le pouvoir réglementaire a ainsi estimé que ces parties de traitements, qui peuvent notamment comporter des données issues de certains traitements mentionnés dans le décret n° 2007-914 précité, justifiaient la mise en œuvre d'une procédure contentieuse particulière en matière de droits des personnes, eu égard à leur sensibilité**. Ces parties de traitements pourraient dès lors également relever de la notion de « fichiers de souveraineté »