Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CNCTR

2e Rapport d'activité 2017

Commission nationale de contrôle des techniques de renseignement

SOMMAIRE

Avant-propos

Dans le premier rapport de la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui couvrait la période s'étendant du 3 octobre 2015, date de son entrée en fonctions, au 2 octobre 2016, j'indiquais que la commission avait notamment dû relever deux défis, celui de la transition avec le cadre juridique antérieur à la loi du 24 juillet 2015 relative au renseignement et celui de l'effectivité de son contrôle. Le rapport pour 2017 permettra au lecteur de constater que la CNCTR exerce désormais pleinement les missions de contrôle que lui a confiées le législateur sur la mise en œuvre des techniques de renseignement.

La première année de fonctionnement de la CNCTR avait permis de bâtir un contrôle *a priori* complet et rigoureux, soucieux de garantir que les atteintes portées à la vie privée par les techniques de renseignement soient proportionnées aux menaces affectant les intérêts fondamentaux de la Nation. Il s'étend désormais, à la suite d'un accord intervenu entre le Premier ministre et la commission, à la surveillance des communications électroniques internationales. Le renforcement des effectifs de la CNCTR, engagé dès la fin de l'année 2015 et poursuivi tout au long des années 2016 et 2017, a permis de développer, tant en qualité qu'en quantité, le contrôle *a posteriori*, en particulier les vérifications sur pièces et sur place menées dans tous les services de renseignement. En effectuant plus de 130 contrôles sur pièces et sur place en 2017, alors qu'elle avait pu en mener environ 60 en 2016, la CNCTR s'est mise en mesure de remplir de manière adéquate sa mission de contrôle *a posteriori*.

La loi du 24 juillet 2015 relative au renseignement et celle du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales ont fixé le cadre juridique de l'activité des services de renseignement. Ces deux textes fondateurs ont cependant connu quelques évolutions et ils ont sans doute vocation à faire l'objet de retouches à la lumière du retour d'expérience. Plusieurs modifications tant législatives que réglementaires ont été apportées en 2017, comme la faculté offerte aux services chargés du renseignement pénitentiaire de mettre en œuvre des

techniques de renseignement, la rénovation des dispositions encadrant la surveillance des transmissions par voie hertzienne ou encore le contingentement des autorisations de recueil de données de connexion en temps réel. Consultée sur chacune de ces évolutions, la CNCTR a rempli sa mission de conseil auprès du Gouvernement comme du Parlement.

Toutes les techniques de renseignement prévues par le livre VIII du code de la sécurité intérieure sont désormais mises en œuvre. En octobre 2017, un traitement automatisé, prévu à l'article L. 851-3 du code de la sécurité intérieure à la seule fin de détecter des connexions susceptibles de révéler une menace terroriste, a été pour la première fois autorisé par le Premier ministre. Cette première demande concernant un « algorithme » a été analysée de manière très approfondie par la CNCTR, faisant ainsi l'objet de plusieurs échanges entre le Gouvernement et la commission avant que celle-ci ne s'estime en mesure d'émettre, au regard des garanties présentées par le dispositif, un avis favorable.

Pour mieux informer le public sur la mise en œuvre de l'ensemble des techniques, la CNCTR a fait le choix d'élargir le champ des éléments statistiques rendus publics. Couvrant une année civile entière, 2017, le présent rapport rend désormais publiques les proportions que représente chacune des finalités pouvant légalement fonder les demandes de techniques de renseignement. Le lecteur ne sera sans doute pas surpris de constater que, comme l'année précédente, la prévention du terrorisme, invoquée dans près de la moitié des demandes, est nettement prédominante. Il pourra également voir la part de chacune des autres finalités dans l'activité des services de renseignement.

D'une manière générale, les éléments statistiques témoignent de la stabilité globale des mesures de surveillance mises en œuvre. Le nombre de demandes de techniques a légèrement crû de 5% en 2017 par rapport à 2016. Quant au nombre de personnes ayant fait l'objet d'au moins une mesure de surveillance au cours d'une année, indicateur que la CNCTR s'était engagée dans son premier rapport à publier tous les ans, il a augmenté dans les mêmes proportions.

La CNCTR n'a pas découvert d'irrégularités majeures à l'occasion de ses vérifications portant sur la mise en œuvre des techniques de renseignement. Le chantier de la centralisation des renseignements recueillis et celui de la traçabilité des exploitations de données progressent. Prévues par la loi et gages de l'efficacité du contrôle, cette centralisation et cette traçabilité sont déjà en place pour la majorité des techniques mises en œuvre. Elles demeurent à parfaire pour d'autres. La CNCTR y sera attentive.

Outre les informations sur l'activité de la CNCTR, le lecteur trouvera dans le présent rapport une brève étude sur un sujet lié au contrôle des activités de renseignement. Elle porte sur la possibilité de notifier aux personnes ayant été surveillées dans le passé qu'elles ont fait l'objet de telles mesures de surveillance. L'étude que la CNCTR soumet au public met en perspective la solution retenue dans le cadre légal français, au regard de la jurisprudence des juges européens et d'exemples tirés de la législation d'autres États membres de l'Union européenne.

J'espère que ce deuxième rapport d'activité de la CNCTR apportera les précisions que le premier, conçu comme une présentation générale de la nouvelle architecture encadrant les activités de renseignement, n'avait pu aborder et qu'il contribuera à une meilleure connaissance du contrôle auquel sont soumises les activités des services de renseignement.

Francis DELON
Conseiller d'État honoraire
Président de la CNCTR

Un résumé du cadre juridique en vigueur

Le livre VIII du code de la sécurité intérieure, créé par la loi du 24 juillet 2015 relative au renseignement et complété par la loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, prévoit que les services de renseignement peuvent être autorisés à mettre en œuvre, pour des finalités limitativement énumérées, des techniques destinées à recueillir des renseignements. Chaque autorisation est accordée par le Premier ministre.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) s'assure que les techniques de renseignement sont mises en œuvre sur le territoire national conformément au cadre légal. Elle est consultée préalablement à la décision du Premier ministre sur toutes les demandes tendant à la mise en œuvre d'une technique. En matière de surveillance des communications électroniques internationales, la consultation préalable, non prévue par la loi, résulte d'un accord entre la commission et le Premier ministre. La CNCTR vérifie également *a posteriori* que les prescriptions légales ont été respectées, en contrôlant l'exécution des autorisations accordées. Elle exerce un contrôle de légalité, qui inclut un contrôle de la proportionnalité des atteintes portées à la vie privée par rapport aux finalités poursuivies.

Les services de renseignement peuvent être des services spécialisés, dits du « premier cercle ». Ce sont :

- la direction générale de la sécurité extérieure (DGSE) ;
- la direction du renseignement et de la sécurité de la défense (DRSD) ;
- la direction du renseignement militaire (DRM) ;
- la direction générale de la sécurité intérieure (DGSI) ;
- le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) ;

- le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin).

D'autres services peuvent se voir confier des missions de renseignement. Ces services, dits du « second cercle », se trouvent notamment au sein de la direction générale de la police nationale, de la direction générale de la gendarmerie nationale et de la préfecture de police de Paris. Il peut également s'agir de certains services de la direction de l'administration pénitentiaire.

Les techniques de renseignement pouvant être autorisées sont :

- les accès administratifs aux données de connexion[1], qui comprennent :
  - les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure),
  - les accès aux données de connexion en temps réel, à la seule fin de prévention du terrorisme (article L. 851-2 du code de la sécurité intérieure),
  - la mise en œuvre, à la seule fin de prévention du terrorisme, de traitements automatisés sur les seules données de connexion acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de services en ligne (article L. 851-3 du code de la sécurité intérieure),
  - la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure),
  - le balisage (article L. 851-5 du code de la sécurité intérieure),
  - le recueil de données de connexion par *IMSI catcher*[2] (article L. 851-6 du code de la sécurité intérieure) ;

1 - Définies à l'article L. 851-1 du code de la sécurité intérieure, les données de connexion sont les « *informations ou documents traités ou conservés par [les] réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ». Cette définition a été précisée par voie réglementaire à l'article R. 851-5 du code de la sécurité intérieure.

2 - Il s'agit de dispositifs techniques permettant de capter des données de connexion d'équipements terminaux, notamment le numéro de leur carte SIM ou IMSI *(international mobile subscriber identity)*.

- les interceptions de sécurité, qui comprennent :
  - l'interception des communications acheminées par les réseaux des opérateurs de communications électroniques ou des fournisseurs de services en ligne (article L. 852-1 du code de la sécurité intérieure),
  - l'interception des communications échangées au sein d'un réseau privatif empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques (article L. 852-2 du code de la sécurité intérieure) ;
- la captation de paroles prononcées à titre privé (article L. 853-1 du code de la sécurité intérieure) ;
- la captation d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure) ;
- le recueil ou la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure).

L'introduction dans un lieu privé, y compris à usage d'habitation, peut être autorisée, par décision spécifique, à la seule fin de mettre en place, utiliser ou retirer un dispositif de balisage, de captation de paroles, de captation d'images, de recueil ou de captation de données informatiques (article L. 853-3 du code de la sécurité intérieure).

Les finalités pouvant justifier la mise en œuvre des techniques de renseignement sont limitativement énumérées à l'article L. 811-3 du code de la sécurité intérieure :

- 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, la prévention des actions tendant au maintien ou à la reconstitution de groupements dissous, et la prévention 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.

Toute personne peut saisir la CNCTR d'une réclamation tendant à ce qu'elle vérifie qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Une fois cette faculté de réclamation utilisée, la personne peut présenter une requête devant une formation spécialisée du Conseil d'État pour demander au juge administratif de mener des vérifications similaires.

Pour une description plus détaillée du cadre légal, le lecteur est invité à consulter le premier rapport d'activité 2015/2016 de la CNCTR ainsi qu'à se rapporter à la première partie du présent rapport.

Compte-rendu de l'activité de la CNCTR

1. La mise en œuvre et les évolutions du cadre juridique : une vigilance exigeante de la CNCTR dans le cadre de sa mission de conseil auprès du Gouvernement et du Parlement

Les dispositions légales applicables aux techniques de renseignement, inscrites en 2015[3] au livre VIII du code de la sécurité intérieure, avaient été modifiées deux fois durant la première année d'activité de la CNCTR.

La première modification avait permis au service du ministère de la justice chargé du renseignement pénitentiaire d'être autorisé à mettre en œuvre certaines techniques de renseignement[4].

La seconde modification avait, en particulier, étendu à l'entourage des personnes surveillées à titre principal le champ d'application du recueil de données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure[5].

Entre le 3 octobre 2016 et le 31 décembre 2017, le livre VIII du code de la sécurité intérieure a été modifié trois fois[6].

---

3 - Voir la loi n° 2015-912 du 24 juillet 2015 relative au renseignement et la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

4 - Voir 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, notamment son article 14.

5 - Voir la 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, notamment ses articles 15 et 17. La modification avait également concerné les données de connexion susceptibles d'être recueillies sur le fondement d'une autorisation d'interception de sécurité prévue à l'article L. 852-1 du code de la sécurité intérieure, ainsi que le partage d'informations entre services spécialisés de renseignement prévu à l'article L. 863-2 du même code.

6 - Pour une présentation récapitulant toutes les modifications législatives depuis 2015, voir le tableau en annexe n° 8 au présent rapport.

En premier lieu, les règles de fonctionnement de la CNCTR ont été adaptées au nouveau statut général des autorités administratives indépendantes défini par la loi[7].

En deuxième lieu, des finalités spécifiques ont été reconnues au service chargé du renseignement pénitentiaire pour mettre en œuvre certaines techniques de renseignement[8].

En troisième lieu, afin de tirer les conséquences de deux déclarations d'inconstitutionnalité prononcées par le Conseil constitutionnel, un contingent, d'une part, a été institué pour limiter le nombre d'autorisations de recueil de données de connexion en temps réel simultanément en vigueur ; d'autre part, la surveillance des communications empruntant la voie hertzienne a pour l'essentiel été intégrée dans le droit commun des techniques de renseignement, le périmètre de la nouvelle « exception hertzienne » ayant été réduit à un champ d'application résiduel[9].

La troisième modification législative a également prolongé jusqu'au 31 décembre 2020 la période expérimentale durant laquelle est applicable l'article L. 851-3 du code de la sécurité intérieure[10]. Cet article, qui prévoit la possibilité de mettre en œuvre des traitements automatisés ou « algorithmes » sur des données de connexion à la seule fin de détecter des menaces terroristes, a fait l'objet d'une première mise en œuvre au cours de l'année 2017.

7 - Voir la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes, notamment son article 39.

8 - Voir la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique, notamment son article 35.

9 - Voir la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, notamment ses articles 15 et 18.

10 - Voir la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, notamment son article 17.

1.1. Un encadrement rigoureux de la première mise en œuvre d'un algorithme en application de l'article L. 851-3 du code de la sécurité intérieure

L'article L. 851-3 du code de la sécurité intérieure 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, qui ne peuvent porter que sur des données de connexion, ne doivent pas permettre d'identifier les personnes auxquelles se rapportent les données qu'ils traitent. Ce n'est que lorsque des données susceptibles de révéler une menace terroriste ont été détectées que le Premier ministre peut, après un nouvel avis de la CNCTR, autoriser le recueil par les services de renseignement de ces seules données détectées ainsi que l'identification des personnes auxquelles elles se rapportent.

Dans son premier rapport d'activité[11], la CNCTR indiquait avoir, par une délibération classifiée adoptée en formation plénière le 28 juillet 2016, rendu un avis au Premier ministre sur le projet d'architecture générale envisagé pour la mise en œuvre des traitements automatisés prévus à l'article L. 851-3 du code de la sécurité intérieure. Dans cet avis, 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.

La CNCTR avait notamment indiqué que la loi faisait, selon elle, obstacle à ce que les agents des services de renseignement puissent accéder aux données de connexion traitées, tant que le Premier ministre n'avait pas, après avis de la commission, autorisé cet accès ainsi que l'identification des

11 - Voir le point 2.1.4.1. du premier rapport d'activité 2015/2016 de la CNCTR.

personnes concernées. Elle avait ainsi préconisé que l'architecture générale du dispositif fût placée sous la responsabilité du groupement interministériel de contrôle (GIC), service du Premier ministre, et non sous celle des services de renseignement. La CNCTR avait également souligné qu'elle devait disposer d'un accès permanent, complet et direct à l'ensemble du dispositif et au mécanisme de traçabilité des accès aux données.

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 recommandations formulées par la CNCTR dans sa délibération du 28 juillet 2016.

Le 18 juillet 2017, la CNCTR a été saisie d'une demande tendant à la première mise en œuvre d'un traitement automatisé sur le fondement de l'article L. 851-3 du code de la sécurité intérieure.

Par une délibération classifiée adoptée en formation plénière le 26 juillet 2017, la CNCTR :

- a constaté que le traitement présenté correspondait, par ses caractéristiques techniques et sa fonction, à la définition légale prévue à l'article L. 851-3 du code de la sécurité intérieure ; lors d'un audit préalable sur pièces et sur place, elle avait pu vérifier que l'algorithme, notamment son code source, était conforme à la description qui en était faite dans la demande ;
- a considéré que le recours à ce traitement ne porterait pas à la vie privée une atteinte disproportionnée à la menace terroriste qu'il s'agissait de prévenir ;
- a cependant émis un avis défavorable à la mise en œuvre du traitement, après avoir relevé que l'architecture générale prévue pour cette mise en œuvre ne respectait pas toutes les garanties préconisées par la commission dans sa délibération du 28 juillet 2016 et fixées par le Premier ministre dans sa décision du 27 avril 2017 ;
- a toutefois estimé possible la réalisation de tests préalables sur des données fictives.

Saisie le 25 septembre 2017 d'une demande rectificative portant sur le même algorithme, la CNCTR, par une délibération classifiée adoptée en formation plénière le 5 octobre 2017 :

- a pris acte des mesures prises par le Gouvernement pour renforcer les garanties présentées par l'architecture générale de mise en œuvre du traitement automatisé ;
- a en conséquence émis un avis favorable à une première mise en œuvre de ce traitement pendant une durée limitée à deux mois, conformément au II de l'article L. 851-3 du code de la sécurité intérieure.

Le Premier ministre a alors autorisé la mise en œuvre de l'algorithme à compter du 12 octobre 2017. À l'issue des deux premiers mois de fonctionnement, la CNCTR, saisie le 1er décembre 2017 d'une demande de renouvellement, a émis en formation plénière le 9 décembre 2017 un avis favorable, sous réserve que l'autorisation accordée soit à nouveau limitée à une durée de deux mois. Au vu des premiers résultats, la CNCTR a en effet estimé nécessaire un réexamen à brève échéance du traitement automatisé pour s'assurer de la pertinence et de la fiabilité de ses caractéristiques techniques. Cet avis a été suivi par le Premier ministre.

Lorsqu'un deuxième renouvellement a été sollicité, la CNCTR, réunie en formation plénière, a émis le 8 février 2018 un avis favorable à la poursuite de la mise en œuvre du traitement pour la durée de droit commun de quatre mois.

Depuis le 12 octobre 2017, date à laquelle la mise en œuvre de l'algorithme a été autorisée pour la première fois, 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.

La CNCTR n'a pas reçu de demande portant sur un autre algorithme.

Eu égard à ce calendrier de mise en œuvre, le Parlement a voté en octobre 2017 le report au 31 décembre 2020[12] de la date, initialement fixée au 31 décembre 2018[13], à laquelle l'article L. 851-3 du code de la sécurité intérieure cessera d'être applicable. Les traitements automatisés prévus à cet article, conçus comme des dispositifs expérimentaux, ne pourront ainsi être mis en œuvre au-delà du 31 décembre 2020, à moins que le législateur, après avoir pris connaissance d'un rapport que le Gouvernement est tenu par la loi de lui présenter avant le 30 juin 2020, ne décide de prolonger à nouveau la période expérimentale ou de pérenniser les dispositions concernées. Dans sa délibération du 28 juillet 2016 évoquée ci-dessus, la CNCTR 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 traitements automatisés prévus à l'article L. 851-3 du code de la sécurité intérieure. La commission a rappelé cette recommandation dans sa délibération classifiée du 5 octobre 2017 portant sur le premier algorithme mis en œuvre.

12 - Voir la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, notamment son article 17.

13 - Voir, dans sa rédaction initiale, l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

1.2. Une réduction de la nouvelle « exception hertzienne » à un champ d'application résiduel

Dans son premier rapport d'activité[14], la CNCTR rappelait l'origine de « l'exception hertzienne », prévue à l'article L. 811-5 du code de la sécurité intérieure, qui soustrayait les mesures de surveillance des « *transmissions empruntant la voie hertzienne* » à la procédure de droit commun, notamment à la nécessité d'une autorisation préalable du Premier ministre accordée après avis de la CNCTR. Interprétées de manière restrictive par la commission, ces dispositions furent finalement abrogées par le Conseil constitutionnel dans sa décision n° 2016-590 QPC du 21 octobre 2016, au motif qu'elles portaient « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances*[15]» . Le Conseil constitutionnel ayant différé l'effet de l'abrogation jusqu'à l'entrée en vigueur d'une nouvelle loi et, au plus tard, jusqu'au 31 décembre 2017, la CNCTR adopta en formation plénière le 10 novembre 2016 une délibération[16] formulant plusieurs recommandations générales pour encadrer le recours à « l'exception hertzienne » par les services de renseignement durant cette période transitoire.

1.2.1. L'encadrement strict de la période transitoire sous le contrôle de la CNCTR

Dès la publication de la décision du Conseil constitutionnel, la CNCTR avait demandé aux services de renseignement concernés de lui fournir toutes informations lui permettant d'apprécier la nature des mesures prises jusqu'alors sur le fondement de l'article abrogé.

Au vu des informations obtenues, la CNCTR précisa, par une délibération classifiée adoptée en formation plénière le 8 décembre 2016, les recommandations qu'elle avait formulées le 10 novembre précédent. Il

14 - Voir le point 2.1.6. du premier rapport d'activité 2015/2016 de la CNCTR.

15 - Voir le paragraphe n° 9 de la décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016.

16 - Voir la délibération de la CNCTR n° 2/2016 du 10 novembre 2016, publiée sur le site internet de la commission.

s'agissait en particulier de garantir que, durant la période transitoire, aucune technique de renseignement soumise à autorisation préalable sous le contrôle de la CNCTR, conformément au titre II et au chapitre IV du titre V du livre VIII du code de la sécurité intérieure, ne fût mise en œuvre sur le fondement des dispositions censurées. Le Conseil constitutionnel avait en effet jugé que « *les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne sauraient être interprétées comme pouvant servir de fondement à des mesures d'interception de correspondances, de recueil de données de connexion ou de captation de données informatiques soumises à l'autorisation prévue* » aussi bien pour la surveillance du territoire national que pour celle des communications électroniques internationales[17].

À la fin de l'année 2016 et au début de l'année 2017, la CNCTR a effectué six déplacements afin d'inspecter, sur pièces et sur place, les dispositifs d'interception et d'exploitation des communications empruntant la voie hertzienne situés sur le territoire national. Lors de ces déplacements, elle a eu accès à des communications interceptées ainsi qu'à des transcriptions et des extractions réalisées à la suite de ces interceptions.

Conformément à l'une des recommandations formulées dans sa délibération du 10 novembre 2016, la CNCTR a été saisie pour avis le 9 février 2017 de deux projets d'instructions ministérielles, l'un du ministre de l'intérieur et l'autre du ministre de la défense, définissant les conditions dans lesquelles les services de renseignement concernés pourraient continuer à prendre des mesures relevant de « l'exception hertzienne » au plus tard jusqu'au 31 décembre 2017. Par une délibération classifiée adoptée en formation plénière le 23 mars 2017, la CNCTR a fait part de ses observations sur ces projets. Les instructions signées par les ministres et notifiées aux chefs des services de renseignement concernés ont tenu compte de toutes les observations de la commission.

En application des instructions ministérielles, la CNCTR a notamment été informée tous les trimestres par chaque service de renseignement concerné du champ et de la nature technique des interceptions réalisées. La commission a également été destinataire d'éléments statistiques sur les transcriptions et extractions effectuées à la suite de ces interceptions.

17 - Voir le paragraphe n° 12 de la décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016.

1.2.2. Le renforcement des procédures de droit commun dans le nouveau cadre juridique

Pour remédier à l'abrogation de « l'exception hertzienne » par le Conseil constitutionnel, le Gouvernement a choisi d'insérer des dispositions sur la surveillance des communications empruntant la voie hertzienne dans le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, élaboré dans la première moitié de l'année 2017[18].

Les dispositions projetées ont fait l'objet d'échanges entre le Gouvernement et la CNCTR, formalisés le 6 juin 2017 par une demande d'avis du Premier ministre sur le fondement de l'article L. 833-11 du code de la sécurité intérieure[19]. Par une délibération adoptée en formation plénière le 9 juin suivant[20], la CNCTR a approuvé l'économie générale du nouveau régime juridique, qui a consisté, d'une part, à intégrer toutes les mesures de surveillance attentatoires à la vie privée dans le droit commun de la mise en œuvre des techniques de renseignement et, d'autre part, à rendre d'application résiduelle les mesures pouvant être prises sans autorisation préalable du Premier ministre et constituant une nouvelle « exception hertzienne », d'ampleur nettement plus limitée que celle prévue à l'article L. 811-5 du code de la sécurité intérieure.

Dans sa délibération, la CNCTR a proposé plusieurs amendements pour préciser la rédaction des dispositions projetées ou renforcer les garanties protégeant la vie privée. Ces propositions ont été presque toutes intégrées dans le projet de loi déposé par le Gouvernement.

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme[21] est entrée en vigueur le 31 octobre 2017. C'est à cette date qu'a pris fin la période transitoire accordée par le Conseil constitutionnel dans sa décision du 21 octobre 2016 et que l'article L. 811-5 du code de la sécurité intérieure a cessé d'être applicable.

---

18 - Ce projet de loi est devenu, après sa discussion et son adoption par le Parlement, la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

19 - Cette disposition prévoit que la CNCTR « *répond aux demandes d'avis du Premier ministre, du président de l'Assemblée nationale, du président du Sénat et de la délégation parlementaire au renseignement* ».

20 - Voir la délibération de la CNCTR n° 4/2017 du 9 juin 2017, publiée en annexe n° 5 au présent rapport et sur le site internet de la commission.

21 - Cette loi sera désormais mentionnée comme « la loi du 30 octobre 2017 ».

Le nouveau cadre juridique ne concerne que les correspondances et les données de connexion échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques. Les communications acheminées successivement par la voie hertzienne et la voie filaire ne peuvent être interceptées sur le fondement des nouvelles dispositions[22]. L'éventuelle surveillance de ces communications demeure régie par les seules dispositions déjà en vigueur des chapitres Ier à IV du titre V du code de la sécurité intérieure[23]. La CNCTR estime ainsi définitivement levée l'ambiguïté que pouvait contenir la rédaction de l'article L. 811-5 du code de la sécurité intérieure.

Parmi les communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, le nouveau cadre juridique distingue celles échangées au sein d'un réseau conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs[24]. L'interception de telles communications, eu égard à leur caractère privé[25], ne peut désormais être réalisée que sur le fondement d'une interception de sécurité particulière, prévue à l'article L. 852-2 du code de la sécurité intérieure et soumise au droit commun de la mise en œuvre des techniques de renseignement. L'interception nécessite une autorisation préalable du Premier ministre

22 - Pour une synthèse présentant l'ensemble des communications susceptibles d'emprunter en tout ou partie la voie hertzienne et le régime juridique applicable à leur éventuelle interception par les services de renseignement, voir le tableau figurant aux pages n° 32 et n° 33 du rapport pour avis n° 161 déposé le 14 septembre 2017 au nom de la commission de la défense nationale et des forces armées de l'Assemblée nationale sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme.

23 - Il peut s'agir, selon le cas, d'accès aux données de connexion prévus aux articles L. 851-1 à L. 851-7 du code de la sécurité intérieure, d'interceptions de sécurité prévues à l'article L. 852-1 du même code, de recueils et de captations de données informatiques prévus à l'article L. 853-2 du code ou encore de mesures de surveillance des communications électroniques internationales prévues aux articles L. 854-1 à L. 854-9 du code. En ce qui concerne la captation de données informatiques, la loi du 30 octobre 2017 a modifié l'article L. 853-2 du code de la sécurité intérieure pour intégrer dans le champ d'application de cette technique certaines transmissions empruntant ponctuellement la voie hertzienne *via* un protocole de communication sans fil comme le « *wifi* ». La CNCTR estime bienvenue cette modification, dans la mesure où le recueil des communications concernées sera soumis au régime spécialement protecteur de la captation informatique, qui ne peut notamment être autorisée sans respecter le principe de subsidiarité.

24 - Ces réseaux peuvent être ceux dénommés « *private or professional mobile radio* » *(PMR)*, dans lesquels les communications sont échangées au moyen de *talkies-walkies* numériques. Il peut s'agir également de réseaux fonctionnant par protocole « *wifi* » et non reliés à internet.

25 - Dans la rédaction de la loi, le caractère privé des communications concernées résulte aussi bien de leur nature que de la configuration technique du réseau au sein duquel elles sont échangées.

accordée après avis de la CNCTR. Les correspondances interceptées ne peuvent être conservées plus de trente jours après leur recueil. La CNCTR exerce un entier contrôle aussi bien *a priori* qu'*a posteriori*, avec tous les outils prévus à cette fin au livre VIII du code de la sécurité intérieure.

Le reste des communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques peuvent être interceptées par les services de renseignement sur le fondement de la nouvelle « exception hertzienne », prévue aux articles L. 855-1 A à L. 855-1 C du code de la sécurité intérieure. Ce champ d'application résiduel ne concerne que des communications échangées au sein de réseaux hertziens ouverts, c'est-à-dire écoutables par toute personne qui règle un appareil de réception sur la fréquence utilisée[26]. La loi confère une autorisation générale aux services de renseignement, qui ne sont pas tenus de solliciter une autorisation préalable du Premier ministre pour chaque mesure de surveillance. Les communications collectées peuvent être conservées jusqu'à six ans après leur recueil.

Outre les services de renseignement, certaines unités des armées sont autorisées à mettre en œuvre les mesures relevant de la nouvelle « exception hertzienne ». La loi du 30 octobre 2017 a en effet créé un article L. 2371-1 dans le code de la défense, qui prévoit cette autorisation en la bornant aux besoins de la défense militaire et de l'action de l'État en mer[27].

En vertu de l'article L. 855-1 C du code de la sécurité intérieure, le contrôle exercé par la CNCTR sur « l'exception hertzienne » résiduelle, lorsqu'elle est utilisée par les services de renseignement, consiste à vérifier qu'aucune technique soumise à autorisation préalable du Premier ministre sous le contrôle de la commission n'est mise en œuvre sur le fondement des dispositions dérogatoires du droit commun. La CNCTR veille ainsi au respect des champs d'application respectifs des chapitres I^er^ à IV et du nouveau

26 - Parmi ces communications figurent notamment celles des radio-amateurs, celles échangées par *talkies-walkies* analogiques ou celles empruntant la bande de fréquences dénommée « *citizen's band* » ou « canaux banalisés » *(CB)*. Il peut encore s'agir de communications radio à longue distance, le plus souvent internationales.

27 - En créant un article L. 2371-2 dans le code de la défense, la loi du 30 octobre 2017 a également autorisé la direction générale de l'armement ainsi que des militaires des unités des armées définies par arrêté à utiliser des capacités d'interception relevant de la nouvelle « exception hertzienne » à la seule fin d'effectuer des tests de ces matériels et à l'exclusion de toute mesure d'exploitation des renseignements recueillis.

chapitre V du titre V du livre VIII du code de la sécurité intérieure. À cette fin, elle est non seulement « *informée du champ et de la nature des mesures prises en application* » de l'article L. 855-1 A du code, mais elle peut également, à sa demande, « *se faire présenter sur place les capacités d'interception mises en œuvre (…) et se faire communiquer les renseignements collectés conservés à la date de sa demande et les transcriptions et extractions réalisées* ». La commission peut en outre, « *à tout moment, adresser au Premier ministre, ainsi qu'à la délégation parlementaire au renseignement, les recommandations et observations qu'elle juge nécessaires au titre du contrôle qu'elle exerce* » sur la nouvelle « exception hertzienne ». La CNCTR se réserve enfin la possibilité de saisir le Conseil d'État d'un recours au cas où elle constaterait que les dispositions dérogatoires sont utilisées pour mettre en œuvre une technique de renseignement ne relevant pas de leur champ d'application.

Lorsque « l'exception hertzienne » est utilisée par des unités des armées, l'article L. 2371-2 du code de la défense prévoit seulement que la CNCTR est « *informée du champ et de la nature des mesures prises* ». Lors de la première lecture par le Sénat du projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, un amendement déposé en séance publique au nom de la commission des affaires étrangères, de la défense et des forces armées a proposé de compléter ces dispositions en attribuant à la CNCTR des pouvoirs de contrôle équivalents à ceux qu'elle peut exercer à l'égard des services de renseignement. Elle aurait pu ainsi se faire présenter sur place les capacités d'interception mises en œuvre et se faire communiquer les renseignements collectés ainsi que les transcriptions et extractions réalisées. Cet amendement n'a pas été adopté.

1.3. Un accompagnement attentif de la croissance du renseignement pénitentiaire

Dans son premier rapport d'activité[28], la CNCTR rappelait que la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement[29] avait ouvert au Gouvernement la possibilité d'inclure le service du ministère de la justice chargé du renseignement pénitentiaire dans le « second cercle » des services de renseignement. Depuis lors, la CNCTR s'est prononcée sur le projet de décret en Conseil d'État nécessaire pour appliquer cette loi.

Par la suite, la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique a prévu des finalités spécifiques au renseignement pénitentiaire pour mettre en œuvre des techniques de renseignement. La CNCTR a été à nouveau consultée sur les textes d'application projetés.

Tout en s'adaptant au contexte particulier du recueil de renseignements en milieu carcéral, les avis exprimés par la CNCTR s'inspirent des positions générales[30] définies lors de l'examen du premier projet de décret en Conseil d'État désignant des services du « second cercle ». Selon la commission, la nature et le nombre des techniques auxquelles peuvent avoir accès ces services dépendent de la part qu'occupe le renseignement au sein de leurs missions ainsi que de l'expertise technique requise pour mettre en œuvre les techniques de renseignement de manière sûre, en particulier les techniques les plus intrusives. Cette analyse a conduit la CNCTR à formuler, sur un point développé ci-dessous, des recommandations plus restrictives que ce que le Gouvernement a finalement choisi d'accorder aux services concernés.

28 - Voir le point 2.1.3. du premier rapport annuel 2015-2016 de la CNCTR.

29 - Cette loi sera désormais mentionnée comme « la loi du 3 juin 2016 ».

30 - Voir la délibération de la CNCTR n° 2/2015 du 12 novembre 2015, publiée sur le site internet de la commission.

1.3.1. L'intégration de l'administration pénitentiaire parmi les services de renseignement du « second cercle »

La loi du 3 juin 2016 avait modifié l'article L. 811-4 du code de la sécurité intérieure pour prévoir que des services du ministère de la justice pourraient désormais être autorisés à recourir à des techniques de renseignement. Le 7 novembre 2016, le garde des sceaux a saisi la CNCTR pour avis d'un projet de décret en Conseil d'État visant à désigner ces services destinés à intégrer le « second cercle » ainsi que les techniques de renseignement auxquelles ils pourraient recourir et les finalités qu'ils pourraient invoquer. Les services concernés étaient, en l'espèce, le bureau central du renseignement pénitentiaire, au sein de la direction de l'administration pénitentiaire, et les cellules interrégionales du renseignement pénitentiaire, au sein des directions interrégionales des services pénitentiaires.

Dans une délibération adoptée en formation plénière le 8 décembre 2016[31], la CNCTR, après avoir étudié les missions, l'organisation, les besoins opérationnels et les moyens techniques des services chargés du renseignement pénitentiaire, n'a pas émis d'objection à leur intégration dans le « second cercle » des services de renseignement et a considéré que la prévention du terrorisme et celle de la criminalité et de la délinquance organisées, respectivement prévues au 4° et au 6° de l'article L. 811-3 du code de la sécurité intérieure, étaient deux finalités adaptées à leur action.

Dans ce cadre, la CNCTR a émis un avis favorable à ce que les services chargés du renseignement pénitentiaire puissent être autorisés à recourir aux accès à des données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), à la géolocalisation en temps réel (article L. 851-4 du code), au balisage (article L. 851-5 du code), au recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code), à l'interception de sécurité réalisée *via* le GIC (I de l'article L. 852-1 du code), à la captation de paroles prononcées à titre privé et à la captation d'images dans un lieu privé (article L. 853-1 du code) ainsi qu'au recueil et à la captation de données informatiques (article L. 853-2 du code).

31 - Voir la délibération de la CNCTR n° 3/2016 du 8 décembre 2016, publiée en annexe n° 1 au présent rapport et sur le site internet de la commission.

La CNCTR a formulé trois réserves :

- s'agissant des personnes susceptibles d'être surveillées, elle a estimé que les services chargés du renseignement pénitentiaire devaient concentrer leur action sur les seules personnes détenues[32] ;

- s'agissant des techniques susceptibles d'être utilisées, elle a émis un avis défavorable à la possibilité d'intercepter des correspondances par *IMSI catcher*, en application du II de l'article L. 852-1 du code de la sécurité intérieure, après avoir relevé que la mise en œuvre de cette technique, d'un emploi que le législateur a voulu exceptionnel, suppose un niveau d'expérience et de technicité très élevé qui nécessiterait de toute façon l'implication d'un service du « premier cercle » ;

- s'agissant de la qualification juridique des lieux de détention au regard du livre VIII du code de la sécurité intérieure, la CNCTR a considéré que les lieux gérés par l'administration pénitentiaire ne pouvaient être regardés comme des lieux publics et devaient être assimilés à des lieux privés au sens des articles L. 853-1 et L. 853-3 du code de la sécurité intérieure. Dès lors que ces lieux privés sont mis à la disposition et placés sous le contrôle de l'administration pénitentiaire, la CNCTR a estimé que, pour y mettre en œuvre des techniques de renseignement autorisées à l'être, les services chargés du renseignement pénitentiaire n'étaient pas tenus, en principe, de demander une autorisation d'introduction dans un lieu privé sur le fondement de l'article L. 853-3 du code de la sécurité intérieure. Toutefois, la commission a considéré que les cellules de détention et les unités de vie familiale devaient bénéficier d'un statut particulier. La personne détenue s'y voyant reconnaître une protection

32 - Cette notion inclut les personnes détenues au sens strict, y compris lorsqu'elles bénéficient d'une permission de sortir prévue à l'article 723-3 du code de procédure pénale, mais aussi les personnes placées sous les régimes de la semi-liberté ou du placement à l'extérieur avec hébergement en établissement pénitentiaire, prévus à l'article 132-26 du code pénal. En revanche, la commission a estimé que les techniques de renseignement concernant les personnes placées sous main de justice en milieu ouvert et celles écrouées mais non hébergées en établissement pénitentiaire, telles que les personnes placées sous surveillance électronique en application de l'article 132-26-1 du code pénal, devaient être mises en œuvre par d'autres services de renseignement déjà structurés pour effectuer cette mission.

particulière de sa vie privée, aussi bien dans les dispositions du code de procédure pénale[33] que dans la jurisprudence de la Cour de cassation[34] ou celle de la Cour européenne des droits de l'homme[35], la CNCTR en a conclu que la cellule de détention et les unités de vie familiale devaient être soumises au régime le plus protecteur prévu par la loi. Ces lieux devaient être regardés, pour l'application du livre VIII du code de la sécurité intérieure, comme des lieux d'habitation au sens de l'article L. 853-3 de ce code. Des techniques de renseignement ne pourraient donc y être mises en œuvre sans que, outre l'autorisation d'y recourir, une autorisation d'introduction dans un lieu d'habitation ait été également accordée après avis rendu par la CNCTR en formation collégiale[36].

Dans le décret d'application[37], le Gouvernement a en définitive maintenu la possibilité pour les services chargés du renseignement pénitentiaire de solliciter la mise en œuvre d'interceptions de correspondances par *IMSI catcher*. En 2017, cette technique n'a fait l'objet d'aucune demande émanant de ces services.

Les autres recommandations de la commission n'ont pas soulevé de difficulté et sont appliquées aux demandes de mise en œuvre de techniques qu'elles concernent.

33 - L'article D. 270 du code de procédure pénale dispose, par exemple, que « *pendant la nuit (…) personne ne doit (…) pénétrer [dans les cellules] en l'absence de raisons graves ou de péril imminent* ». De plus, l'article 46 du règlement intérieur type des établissements pénitentiaires annexé à l'article R. 57-6-18 du code de procédure pénale autorise la personne détenue à « *aménager sa cellule d'une façon personnelle* ».

34 - Voir l'arrêt de la Cour de cassation du 17 mars 2015, chambre criminelle, n° 14-88351.

35 - Voir notamment l'arrêt de la CEDH du 5 novembre 2002, n° 48539/99, affaire Allan contre Royaume-Uni.

36 - Pour mémoire, le D et le F de l'article R. 853-3 du code de la sécurité intérieure restreignent à la seule finalité de prévention du terrorisme la possibilité d'autoriser des services de renseignement du « second cercle » à mettre en œuvre des techniques de renseignement dans un lieu d'habitation.

37 - Voir le décret n° 2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la justice, 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.

1.3.2. 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

Parallèlement à la montée en puissance du renseignement pénitentiaire pour la prévention du terrorisme et celle de la criminalité et de la délinquance organisées, le Gouvernement a souhaité renforcer la compétence de l'administration pénitentiaire dans le domaine de la sécurité et du bon ordre des lieux de détention, ce qui a entraîné la définition de nouvelles finalités pouvant motiver la mise en œuvre de techniques de renseignement prévues au livre VIII du code de la sécurité intérieure. Ces finalités sont distinctes de celles constituant des intérêts fondamentaux de la Nation au sens de l'article L. 811-3 du code. Les personnes à l'égard desquelles les techniques peuvent être mises en œuvre sont les seules personnes détenues[38].

Prévues à l'article 727-1 du code de procédure pénale, les mesures prises « *aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé habilités à recevoir des détenus* » ne concernaient initialement que l'écoute des communications téléphoniques légalement passées par les personnes détenues. L'administration pénitentiaire était compétente pour effectuer ces écoutes, sous le contrôle du procureur de la République. Les personnes détenues étaient informées de la possibilité de telles écoutes.

Dans un premier temps, la loi du 3 juin 2016 a élargi le champ d'application de l'article 727-1 du code de procédure pénale à une liste de techniques similaires à celles prévues au livre VIII du code de la sécurité intérieure[39]. La volonté d'entourer la mise en œuvre de ces techniques de garanties supplémentaires a conduit le législateur, dans un second temps, à concevoir un nouveau dispositif dans la loi n° 2017-258 du 28 février 2017 relative à la

38 - Voir la note n° 32 ci-dessus.

39 - Étaient ainsi autorisés des accès aux données de connexion en temps différé par réquisition auprès des opérateurs de communications électroniques et des fournisseurs de services sur internet, des accès aux données de connexion par *IMSI catcher*, des interceptions de correspondances par réquisition auprès des opérateurs ou par *IMSI catcher*, des captations et des recueils de données informatiques.

sécurité publique. Ce nouveau dispositif partage entre le code de la sécurité intérieure et le code de procédure pénale les techniques auxquelles l'administration pénitentiaire est autorisée à recourir pour prévenir les évasions et assurer la sécurité et le bon ordre des lieux de détention.

L'article 727-1 du code de procédure pénale continue d'encadrer l'écoute des communications régulièrement passées par les personnes détenues. S'y ajoute désormais l'accès aux données informatiques stockées dans un appareil qu'utilise un détenu, licitement ou non[40]. Dans ce régime, qui s'applique sous réserve d'éventuelles procédures judiciaires, l'autorisation de mettre en œuvre les techniques est accordée par le garde des sceaux. Le procureur de la République peut accéder aux renseignements collectés et aux relevés de mise en œuvre, qui doivent être établis pour chaque mesure. Des durées maximales de conservation sont prévues pour les données recueillies ainsi que pour les transcriptions et les extractions réalisées. Enfin, le juge administratif peut être saisi d'un recours contentieux portant sur la légalité de la mise en œuvre d'une technique.

Parallèlement, un nouvel article L. 855-1 du code de la sécurité intérieure prévoit que des services de l'administration pénitentiaire devant être désignés par décret en Conseil d'État pourront être autorisés à accéder à des données de connexion en temps différé (article L. 851-1 du code), à géolocaliser des terminaux téléphoniques en temps réel (article L. 851-4 du code), à baliser des objets (article L. 851-5 du code), à recueillir des données de connexion par *IMSI catcher* (article L. 851-6 du code) et à intercepter des correspondances *via* le GIC (I de l'article L. 852-1 du code). La mise en œuvre de ces techniques, qui concernent les moyens de communication irrégulièrement utilisés par les personnes détenues[41], est soumise à toutes les procédures prévues au livre VIII du code de la sécurité intérieure. Elle doit ainsi être préalablement autorisée par le Premier ministre après avis de la CNCTR. Elle entre dans le champ d'application des contrôles *a posteriori* conduits par la commission.

40 - Bien que l'introduction, la détention et l'usage de téléphones portables et de clefs USB ou 3G ne soient pas autorisés en détention (voir l'article 27 du règlement intérieur type des établissements pénitentiaires annexé à l'article R. 57-6-18 du code de procédure pénale), l'administration pénitentiaire rencontre des difficultés à faire respecter cette interdiction.

41 - Voir la note n° 40 ci-dessus.

La coexistence des deux cadres juridiques succinctement décrits ci-dessus s'explique notamment par la différence de nature entre les mesures de surveillance qu'ils régissent[42]. 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 sont, en revanche, 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.

Le nouvel article L. 855-1 du code de la sécurité intérieure nécessitant des mesures d'application, le garde des sceaux a saisi la CNCTR le 24 février 2017 d'un projet de décret en Conseil d'État visant à désigner les services du ministère de la justice pouvant être autorisés à mettre en œuvre les techniques de renseignement concernées. Ces services étaient, en l'espèce, le bureau central du renseignement pénitentiaire, les cellules interrégionales du renseignement pénitentiaire et les délégations locales au renseignement pénitentiaire présentes dans les établissements de détention.

Dans une délibération adoptée en formation plénière le 16 mars 2017[43], la CNCTR a repris les observations générales qu'elle avait formulées sur le projet de décret intégrant certains services de l'administration pénitentiaire dans le « second cercle » des services de renseignement. Elle a en outre émis deux réserves particulières :

- s'agissant des techniques, elle a considéré que la loi ne permettait pas aux services concernés, lorsque sont seuls en cause la prévention des évasions et le maintien de la sécurité et du bon ordre

42 - Voir l'intervention du garde des sceaux en séance publique du 24 janvier 2017, lors de la première lecture par le Sénat du projet de loi relatif à la sécurité publique.

43 - Voir la délibération de la CNCTR n° 1/2017 du 16 mars 2017, publiée en annexe n° 2 au présent rapport et sur le site internet de la commission.

au sein des lieux de détention, de mettre en œuvre des techniques après introduction dans un lieu privé, tel qu'une cellule[44] ;

- s'agissant des services, elle a admis que les délégations locales au renseignement pénitentiaire, pour des finalités qui touchent au bon fonctionnement quotidien des établissements de détention, puissent être à l'origine de demandes tendant à mettre en œuvre les techniques prévues par la loi. En revanche, elle a considéré que l'expertise technique requise pour une mise en œuvre sûre du balisage (article L. 851-5 du code de la sécurité intérieure) et du recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code) faisait obstacle à ce que cette mise en œuvre et même, dans le cas de la seconde technique, l'exploitation des données recueillies puissent être directement confiées aux délégations locales.

La première réserve a été admise par le Gouvernement. La seconde, qui ne relevait pas nécessairement du niveau réglementaire, n'a pas été incluse dans le décret d'application[45]. La CNCTR vérifiera son respect lors de contrôles au sein des services chargés du renseignement pénitentiaire.

Depuis l'entrée en vigueur du décret le 6 mai 2017, la CNCTR n'a eu à traiter que peu de demandes de mise en œuvre d'une technique sur le fondement des nouvelles finalités spécifiques au renseignement pénitentiaire. Les services chargés de cette mission n'acquièrent que progressivement la maîtrise des techniques de renseignement.

44 - L'article L. 855-1 du code de la sécurité intérieure fixe une liste limitative de techniques de renseignement dont la mise en œuvre peut être autorisée pour prévenir les évasions et assurer la sécurité et le bon ordre au sein des établissements pénitentiaires. Cette liste n'inclut pas la possibilité, prévue à l'article L. 853-2 du même code, de s'introduire dans un lieu privé pour y mettre en place, utiliser ou retirer un dispositif de surveillance.

45 - Voir le décret n° 2017-749 du 3 mai 2017 relatif à la désignation des services relevant du ministère de la justice pris en application de l'article L. 855-1 du code de la sécurité intérieure.

1.4. Une redéfinition limitée du recueil de données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure

Comme la CNCTR l'indiquait dans son premier rapport d'activité[46], le champ d'application de l'article L. 851-2 du code de la sécurité intérieure, qui prévoit le recueil de données de connexion en temps réel à la seule fin de prévenir le terrorisme, avait été modifié par la 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 :

- les personnes surveillées à titre principal n'étaient plus seulement celles « *préalablement identifiée[s] comme présentant une menace* » mais celles « *préalablement identifiée[s] susceptible[s] d'être en lien avec une menace* » ;
- l'entourage des personnes surveillées à titre principal pouvait désormais être visé par la technique ;
- la durée maximale d'autorisation était portée de deux à quatre mois, durée de droit commun[47], applicable y compris à des techniques plus intrusives.

Cette modification législative avait pour but de redéfinir la cible du recueil de données de connexion en temps réel pour renforcer l'utilité de cette technique. En réservant l'article L. 851-2 du code de la sécurité intérieure aux menaces terroristes caractérisées, la rédaction initiale de la loi pouvait en effet apparaître, d'un point de vue opérationnel, comme redondante avec les dispositions régissant d'autres techniques. Les personnes présentant une menace peuvent, si les éléments portés à la connaissance de la CNCTR et du Premier ministre le justifient, faire notamment l'objet d'une interception de sécurité réalisée *via* le GIC, technique plus intrusive que le recueil de données de connexion en temps réel, dès lors qu'elle porte sur le contenu des

46 - Voir le point 2.1.4.1. du premier rapport annuel 2015/2016 de la CNCTR.
47 - Voir l'article L. 821-4 du code de la sécurité intérieure.

correspondances, tout en offrant elle aussi la possibilité d'accéder aux données de connexion liées aux correspondances de la personne surveillée[48].

Dans ce contexte, l'utilité du recueil de données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure était faible d'un point de vue opérationnel, d'autant plus que la durée maximale d'autorisation était limitée à deux mois. Une redéfinition a paru nécessaire au législateur pour restaurer la visée propre de la technique, à savoir la surveillance des personnes qui, sans constituer une menace terroriste justifiant que des techniques de renseignement plus intrusives soient mises en œuvre à leur encontre, sont néanmoins regardées, sous le contrôle de la CNCTR, comme entretenant un lien plausible avec une telle menace. Destiné à remplir un rôle d'alerte, le recours au recueil de données de connexion en temps réel peut ainsi permettre, selon le cas, d'écarter l'hypothèse d'une menace terroriste ou d'en confirmer l'existence.

Saisi par le Conseil d'État d'une question prioritaire de constitutionnalité portant sur la nouvelle rédaction de l'article L. 851-2 du code de la sécurité intérieure, le Conseil constitutionnel a, par une décision n° 2017-648 QPC du 4 août 2017[49], rappelé que le recueil de données de connexion en temps réel excluait l'accès au contenu des correspondances et, par conséquent, ne portait pas atteinte au secret des correspondances[50]. Il a ensuite jugé conforme à la Constitution la redéfinition du champ des personnes surveillées à titre principal ainsi que l'alignement de la durée maximale d'autorisation sur la durée de droit commun. Eu égard à l'ensemble des garanties prévues au livre VIII du code de la sécurité intérieure, le législateur avait assuré « *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* »[51].

48 - Le III de l'article L. 852-1 du code de la sécurité intérieure prévoit que l'autorisation de réaliser une interception de sécurité vaut autorisation de recueillir les données de connexion associées à l'exécution et à l'exploitation de l'interception.

49 - Voir l'annexe n° 6 au présent rapport.

50 - Voir le paragraphe n° 6 de la décision du Conseil constitutionnel n° 2017-648 QPC du 4 août 2017. Cette jurisprudence a déjà été affirmée dans des décisions antérieures, telles que la décision n° 2015-478 QPC du 24 juillet 2015 (voir les paragraphes n° 12 et n° 17) ou la décision n° 2015-713 DC du 23 juillet 2015 (voir le paragraphe n° 55). Ces décisions consacrent la distinction entre données de connexion et contenu des correspondances ou des informations consultées. La CNCTR, conformément aux recommandations formulées dans sa délibération n°1/2016 du 14 janvier 2016 publiée sur son site internet, veille au respect de cette stricte distinction.

51 - Voir les paragraphes n° 6 à n° 10 de la décision du Conseil constitutionnel n° 2017-648 QPC du 4 août 2017.

Ont en revanche été déclarées inconstitutionnelles les dispositions permettant de recourir à cette technique à l'encontre de l'entourage d'une personne surveillée à titre principal. Par cet élargissement, selon le Conseil constitutionnel, le législateur avait permis « *que fasse l'objet de cette technique de renseignement un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit* ». *Dès lors,* « *faute d'avoir prévu que le nombre d'autorisations simultanément en vigueur doive être limité, le législateur n'a[vait] pas opéré une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée* »[52].

Le Conseil constitutionnel ayant différé l'effet de l'abrogation au 1er novembre 2017, la loi du 30 octobre 2017 a remédié à cette censure en instituant un contingent global des autorisations de recueil de données de connexion en temps réel simultanément en vigueur.

Le nouveau I bis de l'article L. 851-2 du code de la sécurité intérieure prévoit ainsi que le Premier ministre fixe, après avis de la CNCTR, un nombre maximal d'autorisations simultanément en vigueur. Ce nombre inclut toutes les autorisations accordées au titre de l'article L. 851-2 du code et non seulement celles à l'encontre de l'entourage d'une personne surveillée à titre principal. En cela, le législateur s'est inspiré de dispositions similaires applicables aux interceptions de sécurité[53].

Saisie par le Premier ministre le 10 novembre 2017 d'un projet de fixer à 500 le contingent global, la CNCTR, par une délibération classifiée adoptée en formation plénière le 7 décembre 2017, a rendu un avis favorable. Après avoir comparé en particulier ce chiffre avec le nombre d'interceptions de sécurité autorisées pour la prévention du terrorisme, la CNCTR a considéré que le contingent projeté n'était pas manifestement disproportionné. Au vu de cet avis, le Premier ministre a, par une décision du 8 janvier 2018, fixé à 500 le nombre maximal de recueils de données de connexion en temps réel pouvant être autorisés simultanément.

52 - Voir le paragraphe n° 11 de la décision du Conseil constitutionnel n° 2017-648 QPC du 4 août 2017.
53 - Voir le VI de l'article L. 852-1 du code de la sécurité intérieure.

Les techniques de renseignement soumises à contingentement

Trois techniques de renseignement sont désormais soumises à un principe de contingentement, en vertu duquel le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par une décision du Premier ministre prise après avis de la CNCTR. Pour chacune des techniques, les capacités sont réparties par le Premier ministre entre les ministres ayant autorité sur les services de renseignement.

Régissant à l'origine les interceptions de sécurité (article L. 852-1 du code de la sécurité intérieure)[54], le principe a été étendu en 2015 au recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code) puis, en 2017, au recueil de données de connexion en temps réel (article L. 851-2 du code).

Le contingentement est conçu comme une incitation pour les services de renseignement à mettre un terme aux autorisations devenues inutiles avant de pouvoir en obtenir de nouvelles et, d'une manière générale, à ne recourir aux techniques concernées que « *dans les seuls cas de nécessité d'intérêt public prévus par la loi* », ainsi que l'énonce l'article L. 801-1 du code de la sécurité intérieure à propos des atteintes que l'autorité publique peut légalement porter à la vie privée dans le cadre de la politique de renseignement.

Le contingentement est, en particulier, apparu nécessaire au Conseil constitutionnel pour les techniques susceptibles d'être mises en œuvre à l'égard de l'entourage de personnes surveillées à titre principal[55]. Tel est le cas des interceptions de sécurité *via* le GIC et, depuis 2017, des recueils de données de connexion en temps réel.

Le GIC, qui centralise les demandes tendant à la mise en œuvre des techniques de renseignement, s'assure quotidiennement du respect des trois contingents et en rend compte à la CNCTR.

54 - Pour une brève mise en perspective historique de cette limitation, voir le point 3.2.3. du premier rapport d'activité 2015/2016 de la CNCTR.

55 - Voir le paragraphe n° 11 de la décision du Conseil constitutionnel n° 2017-648 QPC du 4 août 2017.

1. Le recueil de données de connexion en temps réel : un contingent nouveau imposé par le Conseil constitutionnel

Par une décision du 8 janvier 2018, prise au vu d'une délibération classifiée de la CNCTR adoptée en formation plénière le 7 décembre 2017[56], le Premier ministre a fixé et réparti le contingent comme indiqué dans le tableau ci-dessous.

	2018
Intérieur	430
Défense	50
Douanes	20
Total	500

2. Le recueil de données de connexion par *IMSI catcher* : un contingent stable depuis l'entrée en vigueur du nouveau cadre légal en 2015

Saisie par le Premier ministre d'un projet d'arrêté fixant le nombre maximal d'*IMSI catchers* pouvant être utilisés simultanément, la CNCTR avait, par une délibération classifiée adoptée le 18 décembre 2015, émis un avis sur les chiffres proposés. Par un arrêté du 15 janvier 2016, le Premier ministre a fixé et réparti le contingent en suivant les recommandations de la commission.

	2016
Intérieur	35
Défense	20
Douanes	5
Total	60

56 - Pour une analyse du contexte ayant entraîné l'instauration de ce contingent, voir le point 1.4. du présent rapport.

Le contingent n'a pas été modifié depuis lors[57].

3. Les interceptions de sécurité : un contingent récemment augmenté pour tenir compte notamment de la menace terroriste

Saisie par le Premier ministre en avril 2017 d'un projet d'augmentation de 13% du contingent applicable aux autorisations d'interception de sécurité, la CNCTR s'est prononcée par une délibération adoptée en formation plénière le 26 avril 2017[58]. Après avoir constaté que le contingent en vigueur était presque entièrement utilisé, la commission a estimé avéré le besoin d'accorder simultanément un nombre supérieur d'autorisations d'interception, eu égard, d'une part, à l'aggravation de la menace terroriste et, d'autre part, à la faculté, désormais ouverte aux services du ministre de la justice chargés du renseignement pénitentiaire[59], de recourir aux interceptions de sécurité.

Par une décision du 26 avril 2017, le Premier ministre a fixé et réparti le nouveau contingent comme suit.

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

57 - Bien que les services chargés du renseignement pénitentiaire puissent, depuis le 1er février 2017, former des demandes tendant au recueil de données de connexion par *IMSI catcher* (voir le point 1.3. du présent rapport), 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 ministre de la justice.

58 - Voir la délibération de la CNCTR n° 3/2017 du 26 avril 2017, publiée en annexe n° 4 au présent rapport et sur le site internet de la commission.

59 - Voir le point 1.3. du présent rapport.

1.5. Une suppression définitive du pouvoir de réquisition administrative de données de connexion prévu à l'article L. 871-2 du code de la sécurité intérieure

Dans son premier rapport d'activité[60], la CNCTR faisait état de sa recommandation de portée générale contenue dans une délibération classifiée du 28 avril 2016, tendant à ce que le Premier ministre n'ait plus recours aux réquisitions de données de connexion prévues à l'article L. 871-2 du code de la sécurité intérieure[61]. Survivance de textes antérieurs, ces dispositions, qui ne prévoyaient pas de consultation préalable de la CNCTR, avaient perdu toute utilité depuis l'institution des régimes d'accès aux données de connexion plus protecteurs prévus aux articles L. 851-1 et suivants ainsi qu'au III de l'article L. 852-1 du code.

Décidant de suivre la préconisation de la commission, le Premier ministre a, par une note du 20 mai 2016, fait savoir aux services de renseignement qu'aucune autorisation de mise en œuvre de l'article L. 871-2 du code de la sécurité intérieure ne serait plus accordée en matière de police administrative. Au regard des demandes d'accès aux données de connexion soumises à son contrôle *a priori* ainsi qu'au cours de contrôles *a posteriori* conduits dans les services de renseignement, la CNCTR a constaté le respect de cette directive et la désuétude des dispositions concernées.

La rédaction de l'article L. 871-2 du code de la sécurité intérieure demeurait néanmoins inchangée.

La CNCTR a saisi l'occasion d'une modification envisagée de cet article dans le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, élaboré dans la première moitié de l'année 2017, pour recommander la suppression, en droit, du pouvoir de réquisition auquel le Premier ministre

60 - Voir le point 4.4. du premier rapport d'activité 2015/2016 de la CNCTR.

61 - Il s'agissait d'obtenir des opérateurs de communications électroniques et des fournisseurs de services sur internet les données de connexion nécessaires pour la réalisation et l'exploitation des interceptions autorisées par la loi.

avait renoncé, en fait. Ce projet de loi prévoyait d'abroger des pouvoirs de réquisition similaires dévolus aux ministres de l'intérieur et de la défense pour l'application de « l'exception hertzienne » censurée par le Conseil constitutionnel[62]. Dans sa délibération du 9 juin 2017 relative aux dispositions du projet de loi tirant les conséquences de cette censure[63], la CNCTR a proposé que soit également abrogé le pouvoir de réquisition du Premier ministre évoqué ci-dessus. Le Gouvernement a ajouté cette abrogation dans le texte déposé au Parlement. La loi du 30 octobre 2017 l'a rendue effective.

62 - Voir le point 1.2. du présent rapport.

63 - Voir la délibération de la CNCTR n° 4/2017 du 9 juin 2017, publiée en annexe n° 5 au présent rapport et sur le site internet de la commission.

1.6. Une précision du règlement intérieur de la CNCTR

La loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes[64] a entraîné la modification du règlement intérieur de la CNCTR sur deux points :

- en ce qui concerne la prévention des conflits d'intérêts, il est désormais prévu que la déclaration d'intérêts de chaque membre de la CNCTR soit mise, de façon permanente, à la disposition des autres membres dans les locaux de la commission[65];
- en ce qui concerne les délibérations que devrait tenir le collège de la CNCTR sur la suspension du mandat, la fin des fonctions ou la démission d'un membre[66], la procédure a été mise en conformité avec les exigences de la loi en matière de délais comme de modalités de défense de l'intéressé.

La création récente de la CNCTR explique le caractère limité de ces ajouts. Les dispositions la régissant au titre III du livre VIII du code de la sécurité intérieure contenaient déjà l'essentiel des règles de déontologie et de fonctionnement que le législateur a souhaité généraliser et rationnaliser en 2017 en les inscrivant dans un statut commun à toutes les autorités administratives indépendantes.

De plus, indépendamment de la loi du 20 janvier 2017, le règlement intérieur de la CNCTR a été complété sur deux autres points :

64 - Cette loi sera désormais mentionnée comme « la loi du 20 janvier 2017 ».

65 - Par ailleurs, depuis l'entrée en vigueur de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (voir son article 29), les secrétaires généraux des autorités administratives indépendantes sont tenus de remplir une déclaration de situation patrimoniale et une déclaration d'intérêts. Le règlement intérieur de la CNCTR a donc également été modifié en ce sens.

66 - L'article 6 de la loi du 20 janvier 2017 envisage plusieurs cas, tels que l'empêchement d'un membre à exercer ses fonctions, un manquement grave à ses obligations légales, une incapacité définitive empêchant la poursuite de son mandat ou encore une incompatibilité avec les fonctions de membre auquel l'intéressé n'aurait pas mis fin de lui-même.

- les modalités selon lesquelles, dans des cas exceptionnels, le collège de la CNCTR peut délibérer par moyens de communication électronique sécurisés ont été précisées pour s'inspirer des prescriptions de l'ordonnance n° 2014-1329 du 6 novembre 2014 relative aux délibérations à distance des instances administratives à caractère collégial[67] ;
- la présentation au Président de la République du rapport annuel d'activité de la CNCTR a été inscrite dans le nouveau règlement intérieur pour tenir compte de la pratique observée lors de la première année de fonctionnement de la commission.

Conformément à l'article 14 de la loi du 20 janvier 2017, le règlement intérieur de la CNCTR modifié[68] a été publié au *Journal officiel* de la République française.

67 - Voir également le texte d'application de cette ordonnance, le décret n° 2014-1627 du 26 décembre 2014 relatif aux modalités d'organisation des délibérations à distance des instances administratives à caractère collégial.

68 - Voir la délibération de la CNCTR n° 2/2017 du 23 mars 2017 portant règlement intérieur de la commission, publiée en annexe n° 3 au présent rapport et sur le site internet de la commission.

2. Le contrôle de la mise en œuvre des techniques de renseignement : une consolidation du contrôle *a priori* et un approfondissement du contrôle *a posteriori* menés par la CNCTR

Aux termes de l'article L. 833-1 du code de la sécurité intérieure, la CNCTR veille à ce que les techniques de renseignement soient mises en œuvre sur le territoire national conformément au cadre légal qui les régit. Cette mission de contrôle porte également sur les mesures de surveillance des communications électroniques internationales, en vertu de l'article L. 854-9 du même code.

Le contrôle préalable qu'effectue la CNCTR sur les demandes tendant à la mise en œuvre de techniques de renseignement a connu une légère augmentation en 2017, mais la croissance de l'activité de la CNCTR est due, pour l'essentiel, à une intensité accrue du contrôle *a posteriori*.

2.1. Une activité de contrôle *a priori* en légère augmentation, toujours marquée par la prédominance de la prévention du terrorisme

Grâce aux développements informatiques conduits par le GIC au cours des années 2016 et 2017, la dématérialisation et l'unification de la procédure régissant les demandes de mise en œuvre de techniques de renseignement ont beaucoup progressé. La construction d'un outil fournissant de manière automatisée des chiffres consolidés est cependant encore en cours. Les éléments statistiques figurant dans le présent rapport demeurent le produit d'un travail d'extraction et d'agrégation de données mené par la CNCTR conjointement avec le GIC, puis de fiabilisation des résultats.

Après avoir publié, dans son premier rapport d'activité, les chiffres concernant sa première année de fonctionnement, soit du 3 octobre 2015 au 2 octobre 2016, la CNCTR présentera désormais ses éléments statistiques par année civile. Les évolutions d'une année à l'autre seront retracées à compter du 1er janvier 2016.

2.1.1. Le nombre d'avis préalables rendus par la CNCTR en valeur absolue : des évolutions contrastées selon les techniques de renseignement

Les avis préalables rendus par la CNCTR[69], dont le nombre est égal à celui des demandes soumises à la commission, se répartissent comme indiqué dans le tableau général ci-dessous.

Ces chiffres incluent l'ensemble des demandes formées par les services de renseignement en 2016 et 2017. Aucune demande n'a en effet été présentée, au cours de ces deux années, selon la procédure d'urgence absolue prévue

69 - Ce chiffre n'inclut pas les avis préalables émis par la CNCTR en matière de surveillance des communications électroniques internationales.

à l'article L. 821-5 du code de la sécurité intérieure, qui dispense le Gouvernement, dans des cas exceptionnels, de consulter la CNCTR avant de mettre en œuvre certaines techniques[70].

	2016	2017	Évolution
Accès aux données de connexion en temps différé (identifications d'abonnés ou recensements de numéros d'abonnement) (article L. 851-1 du code de la sécurité intérieure)	32 096	30 116	-6,2%
Accès aux données de connexion en temps différé (autres demandes, dont celles de « factures détaillées »[71]) (article L. 851-1 du code de la sécurité intérieure)	15 021	18 512	+23,2%
Géolocalisations en temps réel (article L. 851-4 du code de la sécurité intérieure)	2 426	3 751	+54,6%
Interceptions de sécurité *via* le GIC (I de l'article L. 852-1 du code de la sécurité intérieure)	8 137	8 758	+7,6%
Autres techniques de renseignement[72]	9 408	9 295	-1,2%
Ensemble des techniques de renseignement	**67 088**	**70 432**	**+5%**

70 - Pour mémoire, le Gouvernement n'a recouru qu'une seule fois, en décembre 2015, aux dispositions de cet article, comme l'expliquait le point 2.2.2. du premier rapport d'activité 2015/2016 de la CNCTR.

71 - Il s'agit d'obtenir la liste des communications d'une personne, ce qui peut révéler la date, la durée, le lieu de ces communications ainsi que le numéro ou l'identifiant technique du correspondant.

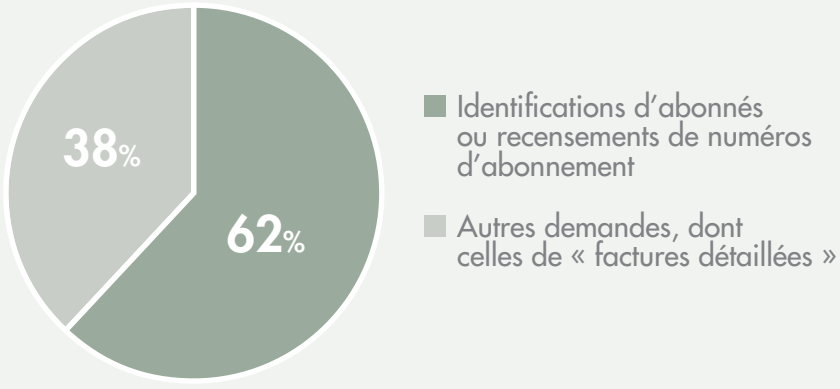
72 - Sont incluses les demandes d'accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure), celles de mise en œuvre de traitements automatisés sur des données de connexion (article L. 851-3 du code), celles de balisage (article L. 851-5 du code), celles de recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code), celles d'interception de sécurité par *IMSI catcher* (II de l'article L. 852-1 du code), celles d'interception de sécurité sur un réseau empruntant exclusivement la voie hertzienne (article L. 852-2 du code), celles de captation de paroles prononcées à titre privé ou celles de captation d'images dans un lieu privé (article L. 853-1 du code), celles de recueil et de captation de données informatiques (article L. 853-2 du code) et celles d'introduction dans un lieu privé (article L. 853-3 du code).

Si le nombre total de demandes tendant à la mise en œuvre de techniques de renseignement a légèrement augmenté de près de 5% au cours de l'année 2017, cette moyenne est le résultat d'évolutions différentes.

En premier lieu, l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) demeure, de très loin, la technique de renseignement la plus utilisée, tout en étant la moins intrusive de toutes celles prévues au livre VIII du code de la sécurité intérieure. Les demandes, en hausse de 3,4% en 2017, ont connu une augmentation moins importante qu'en 2016, année au cours de laquelle elles avaient crû de 14%.

Cette hausse modérée s'explique en partie par des phénomènes conjoncturels. Les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement ont diminué de plus de 6% en 2017 grâce à la résolution de problèmes techniques qui obligeaient auparavant les services à présenter plusieurs demandes identiques, ce qui gonflait artificiellement les données statistiques[73]. L'accès aux « factures détaillées » est, quant à lui, en progression d'environ 23% et représente désormais plus du tiers des accès aux données de connexion en temps différé.

La répartition des demandes d'accès aux données de connexion en temps différé en 2017



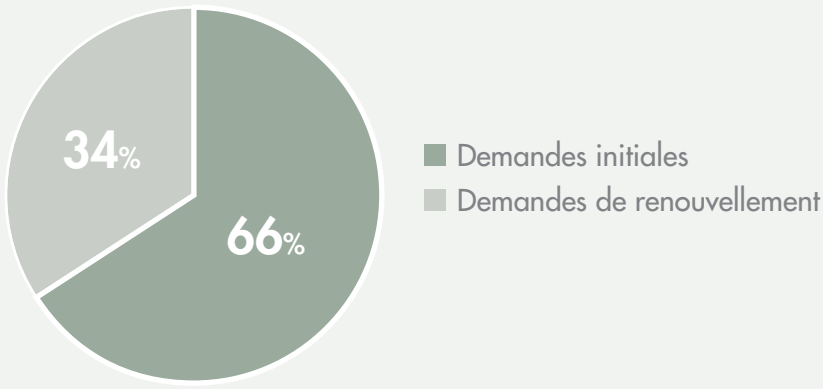
73 - Par exemple, lorsque l'accès à des données de connexion en temps différé était sollicité auprès d'un opérateur de communications électroniques qui se révélait ne pas être celui de la personne surveillée, il fallait présenter une nouvelle demande pour obtenir les données de l'opérateur effectivement concerné. Cette formalité n'est désormais plus nécessaire.

En deuxième lieu, la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) a poursuivi en 2017 sa forte progression, qui avait commencé dès l'autorisation de cette technique par la loi au 1er janvier 2015[74]. L'augmentation d'environ 55% en 2017 est toutefois inférieure à celle de 87% observée durant la première année de fonctionnement de la CNCTR.

En troisième lieu, le recours aux interceptions de sécurité *via* le GIC (I de l'article L. 852-1 du code de la sécurité intérieure) a crû, en 2017 comme en 2016, de façon maîtrisée dans un contexte marqué par une menace terroriste persistante. Les taux d'augmentation sont comparables pour ces deux années (5,6% en 2016 et 7,6% en 2017).

La répartition entre demandes initiales et demandes de renouvellement d'une autorisation déjà accordée n'évolue pas. Les premières représentent toujours 66% des demandes d'interceptions de sécurité et les secondes 34%.

La répartition des demandes d'interceptions de sécurité *via* le GIC en 2017



En quatrième lieu, les demandes portant sur les autres techniques de renseignement prévues aux chapitres Ier à III du titre V du livre VIII du code de la sécurité intérieure sont demeurées à peu près stables en 2017, la très légère diminution d'environ 1% ne pouvant s'interpréter comme une désaffection des services à l'égard des techniques concernées mais plutôt

74 - Voir le point 3.2.2. du premier rapport d'activité 2015/2016 de la CNCTR.

comme l'indication que certaines de ces techniques parfois très intrusives, dont la mise en œuvre nécessite une expertise forte, ne sont pas d'un usage banal et supposent une période significative d'appropriation.

Comme dans son premier rapport d'activité, la CNCTR a fait le choix d'indiquer le nombre de ces demandes de façon consolidée afin de respecter l'article L. 833-9 du code de la sécurité intérieure, qui prévoit que le présent rapport ne peut contenir d'informations couvertes par le secret de la défense nationale ni révéler des procédures ou des méthodes opérationnelles des services de renseignement.

Les avis défavorables rendus par la CNCTR

En 2017, la CNCTR a rendu, hors demandes d'accès aux données de connexion en temps différé prévues à l'article L. 851-1 du code de la sécurité intérieure, 786 avis défavorables, soit 3,6% du nombre d'avis rendus.

Ce taux, moins élevé que celui de 6,9% observé en 2016, s'explique principalement par la volonté manifestée par les services demandeurs de se conformer à la doctrine de la CNCTR, soit en présentant des demandes mieux proportionnées à la défense ou à la promotion des intérêts fondamentaux de la Nation justifiant le recours aux techniques de renseignement, soit en renonçant à présenter des demandes vouées à la désapprobation de la commission.

La diminution du nombre d'avis défavorables est, pour la CNCTR, une évolution positive, qui témoigne de la qualité du dialogue mené entre la commission et les services de renseignement, en particulier sur les questions nouvelles ou sérieuses.

La CNCTR a, en outre, rendu 125 avis défavorables sur les demandes d'accès aux données de connexion en temps différé, soit près de 0,3% du nombre d'avis rendus sur des demandes concernant cette technique.

En 2017, le Premier ministre n'a accordé aucune autorisation après un avis défavorable de la commission. Les avis défavorables de la CNCTR ont toujours été suivis par le Premier ministre depuis l'entrée en vigueur du nouveau cadre légal le 3 octobre 2015.

2.1.2. Les finalités invoquées dans les demandes de techniques de renseignement : la prédominance persistante de la prévention du terrorisme

Les techniques de renseignement ne peuvent être mises en œuvre que pour la défense ou la promotion d'intérêts fondamentaux de la Nation limitativement énumérés à l'article L. 811-3 du code de la sécurité intérieure.

Dans son premier rapport d'activité[75], la CNCTR présentait trois groupes de finalités fondant les seules demandes d'interceptions de sécurité *via* le GIC, afin d'assurer une continuité avec les éléments statistiques publiés par la CNCIS. La commission distinguait, parmi ces demandes, celles motivées par la prévention du terrorisme, celles motivées soit par la prévention de la criminalité et de la délinquance organisées, soit par la prévention des violences collectives de nature à porter gravement atteinte à la paix publique et, enfin, celles motivées par toute autre finalité mentionnée à l'article L. 811-3 du code de la sécurité intérieure.

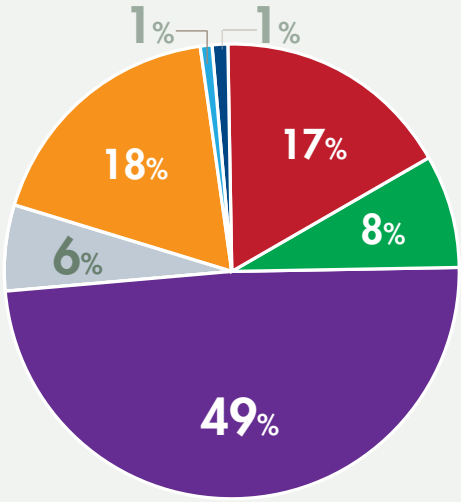
Pour l'année 2017, la commission a décidé d'élargir le périmètre des informations rendues publiques et de présenter, pour l'ensemble des demandes tendant à la mise en œuvre de techniques de renseignement, la proportion de chacune des sept finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure.

Le premier schéma indique la répartition des finalités invoquées à l'appui des demandes portant sur l'ensemble des techniques de renseignement prévues aux chapitres Ier à III du titre V du livre VIII du code de la sécurité intérieure. Le second n'inclut pas les demandes d'accès aux données de connexion prévues au deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure, c'est-à-dire les identifications d'abonnés et les recensements de numéros d'abonnement.

Les grandes tendances varient peu d'un schéma à l'autre.

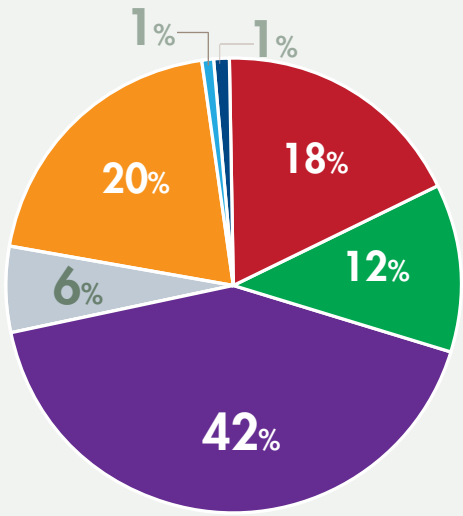
75 - Voir le point 3.2.3. du premier rapport d'activité 2015/2016 de la CNCTR.

Les finalités fondant toutes les demandes de techniques de renseignement en 2017



- 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

Les finalités fondant les demandes de techniques de renseignement en 2017, hors identifications d'abonnés ou recensements de numéros d'abonnement



- 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

La prévention du terrorisme, dont le premier rapport d'activité de la CNCTR montrait qu'elle était devenue en janvier 2015 le fondement légal le plus invoqué à l'appui des demandes d'interceptions de sécurité, est très nettement prédominante lorsque l'on considère l'ensemble des demandes. Cette finalité a motivé en 2017 la moitié des demandes soumises à la CNCTR.

Suivent en deuxième position, invoqués chacun dans environ 20% des demandes, d'une part la prévention de la criminalité et de la délinquance organisées, d'autre part le groupe de finalités relevant des intérêts géostratégiques de la France (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).

En troisième et dernière position, viennent deux finalités dont le contexte sécuritaire et international atténue l'importance relative mais qui motivent une partie significative de l'activité des services de renseignement. Il s'agit, d'un côté, de la défense et de la promotion des intérêts économiques, industriels et scientifiques majeurs de la France et, de l'autre, de 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.

2.1.3. Le nombre de personnes surveillées : une légère augmentation cohérente avec celle des demandes de techniques de renseignement

La CNCTR a repris l'indicateur qu'elle avait créé à l'occasion de son premier rapport d'activité[76] et a calculé le nombre de personnes ayant fait l'objet, en 2017, d'au moins une technique de renseignement prévue aux chapitres Ier à III du titre V du livre VIII du code de la sécurité intérieure. Il est rappelé que ce chiffre ne comprend pas les accès aux données de connexion en temps différé prévus au deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure, c'est-à-dire les identifications d'abonnés ou les recensements de numéros d'abonnement[77].

76 - Voir le point 3.3. du premier rapport d'activité 2015/2016 de la CNCTR.

77 - La CNCTR considère en effet que les identifications d'abonnés et les recensements de numéros d'abonnement constituent moins une mesure de surveillance qu'un acte préparatoire à des mesures de surveillance. De telles mesures commencent, pour la CNCTR, dès l'obtention de « factures détaillées » de la personne concernée en application du même article L. 851-1 du code de la sécurité intérieure.

Les éléments de calcul utilisés comportent une marge d'erreur, évaluée à moins de 10%, dès lors que les demandes tendant à la mise en œuvre de techniques de renseignement sont présentées par technique et non par personne, que le traitement informatisé des demandes n'a pas encore été entièrement harmonisé et, enfin, que certaines personnes ne sont pas nommément identifiées. Cependant, grâce aux développements informatiques conduits par le GIC et à l'amélioration des outils conçus par la commission en 2016, la fiabilité du calcul a été renforcée.

	2016	2017	Évolution
Nombre de personnes surveillées	20 360	21 386	+5%
Dont, au titre de la **prévention du terrorisme**	9 475 (46,5% du total)	9 157 (42,8% du total)	-3,4%
Dont, au titre de la **prévention de la criminalité et de la délinquance organisées**	4 969 (24,4% du total)	5 528 (25,8% du total)	+11,2%

Le nombre de personnes surveillées, en augmentation de 5% en 2017, a connu une évolution du même ordre que celle des demandes de techniques de renseignement.

De manière cohérente avec les schémas indiquant la répartition des finalités invoquées dans les demandes de techniques de renseignement, la proportion de personnes surveillées au titre de la prévention du terrorisme, qui s'élève à près de 43% en 2017, est nettement majoritaire, devant les quelque 26% de personnes surveillées au titre de la prévention de la criminalité et de la délinquance organisées. Ce rapport a peu évolué entre 2016 et 2017.

2.2. Une activité très soutenue de contrôle *a posteriori*, confirmant la nécessité de continuer à renforcer la centralisation des données recueillies et la traçabilité de leur exploitation

Dans son premier rapport d'activité[78], la CNCTR indiquait avoir recours à deux méthodes pour contrôler la mise en œuvre des techniques de renseignement, en particulier pour vérifier la conformité du recueil, de la transcription, de l'extraction et de la conservation des renseignements aux dispositions du livre VIII du code de la sécurité intérieure. La première méthode conduit la commission à mener des vérifications depuis ses locaux, grâce aux applications informatiques mises à sa disposition par le GIC. La seconde méthode consiste à effectuer des contrôles sur pièces et sur place au sein des services de renseignement.

Le premier type de contrôle, exercé depuis les locaux de la commission, est d'application quotidienne. Lors de l'entrée en vigueur du nouveau cadre légal, le 3 octobre 2015, il pouvait porter sur les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), les géolocalisations en temps réel (article L. 851-4 du code) et les interceptions de sécurité *via* le GIC (I de l'article L. 852-1 du code). Depuis janvier 2017, il concerne également le balisage (article L. 851-5 du code), le GIC fournissant désormais à tous les services de renseignement[79], sauf exception due à de rares contraintes opérationnelles, une prestation de stockage centralisé des données émises par balise ainsi qu'un outil de consultation de ces données à distance. La CNCTR dispose, depuis ses locaux, d'un accès immédiat à l'ensemble de ces données.

78 - Voir les points 4.1. et 4.2. du premier rapport d'activité 2015/2016 de la CNCTR.

79 - Hormis la direction générale de la sécurité intérieure et la direction générale de la sécurité extérieure, qui ont la faculté de stocker dans leurs propres locaux les données recueillies par balise, les services de renseignement sont tenus de recourir au dispositif de centralisation géré par le GIC.

Le second type de contrôle, conduit sur pièces et sur place au sein des services de renseignement, peut porter sur l'ensemble des techniques relevant de la compétence de la CNCTR. Il a connu un fort développement au cours de l'année 2017 grâce aux recrutements venus renforcer le secrétariat général de la CNCTR depuis l'installation de la commission le 3 octobre 2015. Désormais composée de onze chargés de mission aux compétences tant juridiques que techniques, l'équipe accomplissant les contrôles observe un rythme de deux, parfois trois déplacements par semaine. Le nombre de contrôles sur pièces et sur place est ainsi passé d'environ 60 en 2016 à plus de 130 en 2017. Un membre du collège de la CNCTR participe, dans la plupart des cas, aux contrôles.

Par ailleurs, le président de la CNCTR, généralement accompagné d'un autre membre du collège et d'un chargé de mission, s'est rendu dans douze centres territoriaux relevant du GIC en 2017. Ces déplacements sont principalement destinés à rencontrer les chefs des services de renseignement déconcentrés[80], afin de diffuser la doctrine de la commission et de répondre aux interrogations propres à ces services.

Les contrôles sur pièces et sur place offrant le plus d'enseignements sur la mise en œuvre du cadre légal, la CNCTR a fait le choix d'en présenter plus précisément, dans le présent rapport, les modalités comme les principales conclusions non couvertes par le secret de la défense nationale.

2.2.1. Les contrôles sur pièces et sur place : un vecteur essentiel pour la diffusion de la doctrine de la CNCTR et la régularisation rapide des quelques anomalies constatées

Les contrôles sur pièces et sur place font l'objet d'une préparation rigoureuse. Leur programme général est arrêté plusieurs mois à l'avance et approuvé par le président de la CNCTR : il s'agit de répartir les contrôles entre les services en fonction de leur usage des techniques de renseignement. Les services les plus importants que sont la direction générale de la sécurité

80 - Il peut s'agir des services déconcentrés de la sécurité intérieure, de la police judiciaire, du renseignement territorial, de la gendarmerie nationale et des enquêtes douanières.

intérieure (DGSI) et la direction générale de la sécurité extérieure (DGSE) sont, en règle générale, soumis à deux contrôles par mois, mais cette fréquence a pu être portée à un contrôle par semaine au cours de l'année 2017. Les services dont le recours aux techniques de renseignement est le plus limité ne nécessitent pas plus de quelques contrôles par an.

Les services sont avisés de la date à laquelle ils feront l'objet d'un contrôle sur pièces et sur place. Si la loi permet à la CNCTR d'effectuer des contrôles inopinés, la commission n'a pas estimé utile, en 2017, d'user de cette faculté, qu'elle réserve à des cas précis d'urgence ou d'irrégularité manifeste qui ne se sont pas présentés. La CNCTR considère que la réussite d'un contrôle dépend de la coopération constructive entre le service concerné et la commission. Dans cet état d'esprit, les affaires et sujets particuliers abordés au cours de chaque contrôle sont communiqués au service quelques jours à l'avance, ce qui lui permet de réunir les informations nécessaires et de prévoir la présence des agents pertinents.

Les contrôles sur pièces et sur place ont pour but d'aborder des dossiers précis et d'expliquer des points de doctrine de la commission. Les contrôles peuvent susciter des questions nouvelles qui ne sont pas immédiatement tranchées car elles nécessitent un travail d'instruction, dont les conclusions sont soumises *in fine* au collège de la CNCTR pour décision. Parmi les dossiers inscrits au programme des contrôles figurent des autorisations sur la mise en œuvre desquelles la commission, lors de l'examen de la demande, a souhaité que soit effectué un suivi étroit, par exemple en raison du caractère particulièrement intrusif de la technique. Les contrôles permettent en outre de préparer l'examen de futures demandes, soit qu'ils fournissent l'occasion de recueillir des éclaircissements sur des thématiques structurant l'action du service, soit qu'ils offrent la possibilité de mieux comprendre les raisons motivant l'emploi de certaines techniques et, partant, de mieux apprécier la proportionnalité, voire la subsidiarité[81] de leur mise en œuvre.

81 - Toutes les techniques de renseignement doivent être mises en œuvre, en vertu de l'article L. 801-1 du code de la sécurité intérieure, en respectant un principe de proportionnalité entre les atteintes portées à la vie privée et les menaces affectant les intérêts fondamentaux de la Nation. En outre, les techniques les plus intrusives ne peuvent être utilisées que lorsque les renseignements espérés ne peuvent être recueillis par un autre moyen légal : il s'agit des captations de paroles prononcées à titre privé ou des captations d'images dans un lieu privé (article L. 853-1 du code), des recueils et des captations de données informatiques (article L. 853-2 du code) et, enfin, des introductions dans un lieu privé (article L. 853-3 du code).

Deux référents par service ont été désignés parmi les chargés de mission de la CNCTR. En retour, les services ont également mis en place des points de contacts pour la commission. L'organisation des contrôles sur pièces et sur place ainsi que l'échange d'informations utiles s'en trouvent facilités. D'une manière générale, la CNCTR est satisfaite des conditions dans lesquelles elle est accueillie au sein des services de renseignement. Aucune difficulté particulière ne lui paraît devoir être signalée.

Les contrôles sur pièces et sur place s'étendent, dans la plupart des cas, sur une demi-journée. La CNCTR accède à toutes les données collectées dont elle a sollicité l'examen et commence par vérifier le respect des durées de conservation prévues à l'article L. 822-2 du code de la sécurité intérieure[82]. Elle se fait présenter les dispositifs techniques utilisés pour le recueil et la conservation des données. Elle demande que lui soient ouvertes les applications permettant d'exploiter les données et de tracer les actions effectuées. Le service expose les circuits de mise en œuvre des autorisations concernées et apporte toutes précisions sur les méthodes de travail des analystes chargés de trier, dans les données collectées, celles qu'il est pertinent de communiquer aux enquêteurs responsables des dossiers ou des thématiques. La CNCTR précise qu'elle n'impose pas aux services de conserver des données pour le seul besoin du contrôle, au-delà de la durée nécessaire pour les exploiter. Elle estime au contraire que le respect de la vie privée est renforcé par une destruction la plus rapide possible des données collectées. Les transcriptions et extractions des renseignements recueillis demeurent évidemment accessibles à la commission après la destruction des données brutes ayant servi à leur réalisation.

Pour tirer le meilleur parti des informations auxquelles elle a accès, la CNCTR a entrepris un travail de « cartographie », consistant, pour chaque service, à recenser les types de matériels utilisés, les méthodes employées, les procédures suivies et les contrôles internes mis en place. Ce travail permet

82 - Lorsqu'un dispositif permet de recueillir des données soumises à des durées de conservation différentes, la CNCTR considère que le régime le plus strict doit s'appliquer, au cas où les données ne peuvent être dissociées. Par exemple, les enregistrements d'une caméra captant à la fois des images et des paroles ne peuvent être conservés au-delà de trente jours, la durée de cent-vingt jours n'étant applicable qu'aux images sans le son. En outre, la CNCTR rappelle que le point de départ de toutes les durées maximales de conservation prévues à l'article L. 822-2 du code de la sécurité intérieure est la date de recueil des données et non celle de leur première exploitation.

à la commission d'identifier plus facilement les difficultés rencontrées par le service pour appliquer le cadre légal d'une manière à la fois exacte et efficiente. Il peut conduire à des préconisations formulées par la CNCTR lors de contrôles ultérieurs, mais contribue aussi à repérer des bonnes pratiques méritant d'être reproduites.

Tous les contrôles sur pièces et sur place donnent lieu à la rédaction d'un compte-rendu. Ce document, d'usage interne, est mis à la disposition de tous les membres de la CNCTR et suscite, le cas échéant, des débats sur des points de doctrine à fixer.

Les contrôles sur pièces et sur place menés en 2017 n'ont révélé aucune irrégularité sérieuse justifiant que la CNCTR fasse usage de son pouvoir de recommander formellement que la mise en œuvre d'une technique de renseignement soit interrompue et que les renseignements collectés soient détruits, en application de l'article L. 833-6 du code de la sécurité intérieure.

Les anomalies constatées ont pu être corrigées après un rappel de la règle de droit au moment du contrôle sur pièces et sur place. Le caractère satisfaisant de cette correction a été vérifié lors du contrôle suivant. Il a pu s'agir de données irrégulièrement conservées au-delà de la durée légale qui leur était applicable, car elles avaient été qualifiées, de manière erronée, de données chiffrées soumises à des délais de destruction différents. Dans d'autres cas, une procédure judiciaire ayant été ouverte à l'encontre d'une personne jusqu'alors surveillée par des techniques de renseignement, la CNCTR a demandé au service de cesser immédiatement la mise en œuvre de ces techniques afin de garantir la primauté de l'action judiciaire sur la police administrative. La CNCTR veille en effet à ce que les services portent une attention scrupuleuse aux éventuelles interférences entre procédure judiciaire et surveillance administrative.

La CNCTR privilégie, dans la mesure du possible, une gestion des anomalies concertée avec les services. Lorsqu'une irrégularité est détectée, la commission fait connaître informellement sa position, lors d'un contrôle sur pièces et sur place ou en prenant contact avec la cellule juridique du service concerné. Cette étape a jusqu'à présent toujours été suffisante pour mettre un terme aux irrégularités peu nombreuses qui sont apparues. Dans l'hypothèse où l'étape informelle serait infructueuse, la CNCTR commencerait

par envoyer un courrier au chef du service concerné ainsi qu'au ministre dont il relève. Ce n'est qu'en cas d'échec de cette nouvelle tentative que la commission interviendrait auprès du Premier ministre, auquel elle adresserait, en dernier recours, une recommandation tendant à ce qu'il soit mis fin à l'irrégularité constatée. Faute de mise en conformité avec le cadre légal après cette ultime démarche, la voie du recours contentieux devant le Conseil d'État serait ouverte à la CNCTR.

La CNCTR dresse un bilan positif des contrôles sur pièces et sur place qu'elle a menés en 2017. En permettant aux services d'interroger régulièrement la commission sur des difficultés d'interprétation du cadre légal, ces contrôles, dont la fréquence peut paraître exigeante, ont renforcé la sécurité juridique des activités de renseignement en rendant, pour les services, la doctrine de la CNCTR plus prévisible et en précisant, pour la commission, les besoins opérationnels des services.

Les recommandations et observations émises par la CNCTR

En 2017, la CNCTR, dont les avis défavorables ont toujours été suivis par le Premier ministre et dont les contrôles *a posteriori* n'ont pas révélé d'irrégularité qui n'ait été rapidement rectifiée, n'a pas eu à faire usage de son pouvoir de recommander formellement que la mise en œuvre d'une technique de renseignement soit interrompue et que les renseignements collectés soient détruits, en application de l'article L. 833-6 du code de la sécurité intérieure. En conséquence, la CNCTR ne s'est pas non plus trouvée dans la situation de devoir saisir le Conseil d'État d'un recours contentieux sur le fondement de l'article L. 833-8 du code, cette voie de recours étant ouverte lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission.

La CNCTR a en revanche émis des recommandations de portée générale depuis la publication de son premier rapport d'activité.

La première recommandation, qui a pris la forme d'une délibération classifiée adoptée en formation plénière le 8 décembre 2016, a été adressée au

Premier ministre et portait sur le régime transitoire applicable aux mesures de surveillance des transmissions empruntant la voie hertzienne, dans l'attente de l'adoption du nouveau cadre légal qu'appelait la censure par le Conseil constitutionnel des dispositions jusqu'alors en vigueur[83]. Il s'agissait en particulier de garantir que, durant la période transitoire, aucune technique de renseignement soumise à autorisation préalable sous le contrôle de la CNCTR, conformément au titre II et au chapitre IV du titre V du livre VIII du code de la sécurité intérieure, ne serait mise en œuvre sur le fondement des dispositions censurées.

Le second groupe de recommandations, de nature technique, portait sur la distinction entre données de connexion et contenu des correspondances ou des informations consultées. Dans une délibération adoptée en formation plénière le 14 janvier 2016[84], la CNCTR avait énoncé les principes généraux fondant la séparation entre ces deux types de données. Elle avait souligné que les développements contenus dans sa délibération constituaient une analyse non exhaustive, qui avait vocation à être approfondie en fonction des évolutions techniques. Elle avait en conséquence demandé que les nouveaux types de données qui pourraient être regardées comme faisant partie des données de connexion fassent l'objet d'un avis de sa part avant toute autorisation de recueil, afin qu'elle puisse s'assurer qu'aucun contenu de communications ne serait indûment collecté dans ce cadre.

En application de cette doctrine, la CNCTR a conduit en 2016 et en 2017 des échanges à la fois écrits et oraux avec les services de renseignement concernés. Au terme de cette instruction, la CNCTR a formalisé sa position sur plusieurs types de données dans des courriers classifiés, que le président de la CNCTR, après les avoir soumis à la commission réunie en formation collégiale, a adressés aux chefs des services de renseignement. Toutes les recommandations ont été appliquées.

83 - Pour un développement complet de ce sujet, voir le point 1.2. du présent rapport.

84 - Voir la délibération de la CNCTR n° 1/2016 du 14 janvier 2016, publiée sur le site internet de la commission.

2.2.2. La centralisation des données recueillies et la traçabilité de leur exploitation : un lourd chantier essentiel au contrôle, qui progresse mais demeure inachevé

Lors de l'examen en première lecture du projet de loi relatif au renseignement par l'Assemblée nationale en avril 2015, le ministre de l'intérieur avait déclaré : « *Le Gouvernement prend devant vous l'engagement de réfléchir ensemble aux moyens de minimiser l'éparpillement tout en tenant compte des techniques utilisées et des risques opérationnels adossés au transfert de telle ou telle donnée vers un lieu centralisé. Limiter au maximum le nombre de sites pour permettre que le contrôle soit effectif est une préoccupation majeure et convergente du Gouvernement et du Parlement* »[85].

Aux termes de l'article L. 822-1 du code de la sécurité intérieure, « *le Premier ministre organise la traçabilité de l'exécution des techniques autorisées (...) et définit les modalités de la centralisation des renseignements collectés* ». La surveillance des communications électroniques internationales est également concernée puisque l'article L. 854-4 du code de la sécurité prévoit que « *l'interception et l'exploitation des communications en application du présent chapitre font l'objet de dispositifs de traçabilité organisés par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement* » et que « *le Premier ministre définit les modalités de la centralisation des renseignements collectés* ».

Les dispositions légales citées ci-dessus contiennent deux exigences distinctes mais liées, qui conditionnent, selon la CNCTR, la pertinence et la précision des contrôles *a posteriori* dont la loi l'a chargée. Il s'agit, d'une part, de la centralisation des renseignements collectés et, d'autre part, de la traçabilité des mesures d'exploitation de ces renseignements.

Plus de deux ans après l'entrée en vigueur du nouveau cadre légal, la CNCTR constate que des progrès ont été accomplis en matière de centralisation des

85 - Voir, sur le site internet de l'Assemblée nationale, le compte-rendu de l'examen du texte par la commission des lois de l'Assemblée nationale au cours de la réunion du 1er avril 2015 à 16h30.

renseignements collectés mais que l'organisation définitive n'est pas encore atteinte. La traçabilité de l'exploitation de ces renseignements est, quant à elle, tributaire de développements informatiques qui demeurent à conduire.

En ce qui concerne la centralisation des données, la CNCTR indiquait, dans son premier rapport d'activité[86], que, pour que la commission puisse réellement disposer, comme la loi le prévoit[87], d'un accès permanent, complet et direct aux renseignements collectés ainsi qu'aux extractions et transcriptions réalisées et, partant, pour qu'elle puisse effectivement contrôler la mise en œuvre des techniques autorisées, la centralisation des données recueillies était indispensable.

La CNCTR estimait également que la centralisation ne pouvait être réussie qu'à trois conditions :

- la mise en place de systèmes d'information et de réseaux de communication solides et sécurisés ;
- la possibilité de consulter et d'exploiter à distance les données collectées, pour éviter que ne soient centralisées des données brutes alors que l'exploitation s'effectuerait sur des copies conservées de façon décentralisée ;
- la limitation et le regroupement des lieux de stockage, consistant à faire du GIC l'organe de centralisation des renseignements collectés par les services du « second cercle » ainsi que par les services du « premier cercle » qui le souhaiteraient, tandis que la DGSI et la DGSE centraliseraient les renseignements recueillis pour leur propre compte ou celui des services du « premier cercle » associés.

Au regard de ces critères, la CNCTR estime achevé le dispositif de centralisation pour l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), l'accès aux données de connexion en temps réel (article L. 851-2 du code), la mise en œuvre de traitements automatisés sur des données de connexion (article L. 851-3 du code), la géolocalisation en temps réel (article L. 851-4 du code), le balisage (article

86 - Voir le point 4.2.1. du premier rapport d'activité 2015/2016 de la CNCTR.
87 - Voir notamment les articles L. 833-2 et L. 854-9 du code de la sécurité intérieure.

L. 851-5 du code) et les interceptions de sécurité *via* le GIC (I de l'article L. 852-1 du code). Il en va de même des mesures de surveillance des communications électroniques internationales (articles L. 854-1 à L. 854-9 du code).

En revanche, pour les autres techniques, caractérisées par une collecte décentralisée du renseignement, les modalités de stockage des données recueillies demeurent très disparates. Sont concernés le recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure), la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du code), enfin le recueil et la captation de données informatiques (article L. 853-2 du code). Si certains services sont parvenus à construire des dispositifs permettant la centralisation des renseignements au niveau de leur administration centrale, d'autres ont maintenu un stockage décentralisé au sein de leurs échelons territoriaux, faute de pouvoir concevoir et financer un réseau informatique susceptible d'acheminer de manière sûre des données volumineuses. La CNCTR a donc mené en 2017 plusieurs contrôles sur pièces et sur place dans des unités territoriales des services de renseignement. Au reste, même les dispositifs de stockage des administrations centrales ou des grands services souffrent parfois de dispersion, en l'absence d'application informatique unifiée et cohérente pour conserver et traiter les données.

Dans ce contexte, le GIC travaille depuis 2016 à la construction d'un dispositif technique permettant à tous les services de renseignement[88] de centraliser dans son système d'information les paroles ou les images captées sur le fondement de l'article L. 853-1 du code de la sécurité intérieure, puis d'exploiter ces données dans ses centres territoriaux. Les travaux pourraient aboutir au cours de l'année 2018. Ces développements constitueront, du point de vue de la CNCTR, un net progrès pour l'accomplissement de sa mission de contrôle puisque la commission aura désormais la possibilité de contrôler depuis ses locaux, qui sont reliés au système d'information du GIC, le respect des durées de conservation et la conformité des exploitations de données à la finalité fondant l'autorisation de recueil. À terme, les services devraient également pouvoir consulter et exploiter les données depuis leurs propres locaux, *via* un réseau relié à celui du GIC.

88 - Comme pour le balisage, tous les services de renseignement seraient tenus de recourir au dispositif géré par le GIC, hormis la DGSI et la DGSE, qui en auraient la faculté mais non l'obligation. Ces deux services disposent en effet d'un dispositif propre de centralisation des renseignements recueillis.

Consciente du temps et des ressources que réclame la mise en place de la centralisation prévue par la loi, la CNCTR reconnaît les évolutions positives intervenues en 2017 et invite le Gouvernement à poursuivre les différents développements nécessaires, tant par le biais du GIC qu'au sein des grands services.

En ce qui concerne la traçabilité de l'exploitation des données, la CNCTR rappelle tout d'abord que chaque mise en œuvre d'une technique doit, conformément à l'article L. 822-1 du code de la sécurité intérieure, faire l'objet d'un relevé mentionnant les dates de début et de fin de la mise en œuvre ainsi que la nature des renseignements collectés. En outre, l'article L. 822-3 du code prévoit que « *les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités* » que la défense et la promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code.

L'ensemble de ces opérations s'effectue sous le contrôle de la CNCTR. La loi confie ainsi à celle-ci une mission de contrôle sur toutes les étapes de la production du renseignement, afin de s'assurer que les autorisations de mettre en œuvre les techniques sont régulièrement exécutées. En prévoyant à l'article L. 833-2 du code de la sécurité intérieure que la commission « *dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions (...) ainsi qu'aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements* », la loi lui garantit un accès à tous documents et supports comportant des éléments obtenus grâce à la mise en œuvre d'une technique de renseignement[89].

La CNCTR a constaté que la rédaction des relevés de mise en œuvre, également dénommés « fiches de traçabilité », s'était améliorée au cours de l'année 2017, mais estime encore perfectibles les pratiques des services. Comme la commission le leur a rappelé plusieurs fois, l'accomplissement de cette exigence légale dans les meilleurs délais est nécessaire pour un exercice fluide et régulier du contrôle.

89 - La circonstance que certains documents comportent des éléments de provenances différentes, incluant des sources exclues à ce jour de la compétence de la commission comme les transmissions effectuées par des services étrangers, ne saurait, selon la CNCTR, faire obstacle au contrôle sur les éléments issus de techniques de renseignement.

Le chantier le plus substantiel et le moins avancé demeure cependant celui de la traçabilité des consultations, transcriptions et extractions des données recueillies. Il est lié à celui de la centralisation des renseignements, puisque la traçabilité est d'autant plus aisée que les conditions de stockage et d'exploitation des données sont étroitement définies.

Lors de ses contrôles sur pièces et sur place, la CNCTR est souvent confrontée à des dispositifs ne lui permettant pas d'apprécier de façon satisfaisante la régularité des exploitations du renseignement, soit que fasse défaut une fonction traçant tous les accès aux données stockées, soit qu'il ne soit pas encore possible de savoir quelles actions, transcriptions ou extractions, ont subi ces données. Le contrôle de l'existence même des transcriptions et extractions et, partant, celui de leur bien-fondé et de leur conformité aux finalités légales peuvent s'en trouver fragilisés. Ces remarques concernent toutes les techniques de renseignement, y compris les mesures de surveillance des communications électroniques internationales.

La CNCTR invite donc les services de renseignement à développer, en concertation avec la commission, des dispositifs de traçabilité complets et fiables, permettant de contrôler la régularité de l'exploitation des données recueillies. Une traçabilité rigoureuse est en effet essentielle pour parer tout risque de diffusion non maîtrisée, au sein des services de renseignement, d'informations concernant la vie privée des personnes.

Le dialogue institutionnel avec le Parlement, les relations internationales et l'information du public

Approfondissant les contacts qu'elle avait noués lors de sa première année de fonctionnement[90], la CNCTR a poursuivi le dialogue institutionnel avec le Parlement ainsi que les échanges avec les autorités de contrôle étrangères, dans le respect du secret de la défense nationale qui couvre les travaux de la commission en vertu de l'article L. 832-5 du code de la sécurité intérieure.

90 - Voir la 6e partie du premier rapport d'activité 2015/2016 de la CNCTR.

En novembre et décembre 2016, le président de la CNCTR a été reçu par le président de l'Assemblée nationale et par le président du Sénat afin de leur présenter le premier rapport d'activité de la commission. Au cours de l'année 2017, il a été auditionné, à l'Assemblée nationale et au Sénat, par les rapporteurs des commissions compétentes au fond ou saisies pour avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme. Lors de l'examen par le Sénat du projet de loi de finances pour 2018, le président de la CNCTR a été entendu par le rapporteur de la commission des lois saisie pour avis.

Le 22 mars 2017, la CNCTR et la délégation parlementaire au renseignement ont organisé conjointement un colloque intitulé « *Le contrôle et l'évaluation de la politique publique du renseignement* », en présence notamment de parlementaires, de magistrats, de représentants d'autorités administratives indépendantes, d'universitaires et de journalistes. Ce colloque a permis de dresser un premier bilan du nouveau cadre juridique applicable au renseignement et d'en faire mieux connaître l'architecture générale.

Le président de la CNCTR a par ailleurs participé, le 13 novembre 2017, à un colloque organisé par l'université de Grenoble Alpes[91] et par l'Institut national de recherche en informatique et en automatique, avec pour thème « *Le contrôle du renseignement : comment concilier surveillance et respect des droits de l'homme* ». Il y a présenté la refonte du cadre juridique applicable au renseignement en 2015, appréciée à la lumière de deux ans de mise en œuvre de cette nouvelle législation.

S'agissant des relations internationales, la CNCTR s'est déplacée à Berlin en juin 2017 pour y rencontrer des institutions chargées de contrôler les services de renseignement, la *G10-Kommission* et le *Parlamentarisches Kontrollgremium*[92]. Elle a accueilli à Paris en juillet 2017 la commission de contrôle suédoise dénommée *Säkerhets- och integritetsskyddsnämnden*[93]. Elle a rencontré à Paris en novembre 2017 le rapporteur spécial des Nations unies pour le droit à la vie privée. En outre, un représentant de la CNCTR a

91 - Il s'agissait plus précisément, au sein de l'université, du *Grenoble Alpes Data Institute* et du centre d'études sur la sécurité internationale et les coopérations européennes.

92 - Pour une présentation de ces deux institutions, voir l'étude figurant dans le présent rapport.

93 - Commission pour la sécurité et la protection de l'intégrité.

participé à une réunion de travail sur la protection des données personnelles, organisée à Vienne en février 2017 par l'Agence des droits fondamentaux de l'Union européenne, et à une conférence sur le contrôle du renseignement, organisée à Bruxelles en novembre 2017 par le rapporteur spécial des Nations unies pour le droit à la vie privée.

Enfin, comme elle l'annonçait dans son premier rapport d'activité, la CNCTR a mis en ligne un site, www.cnctr.fr, qui présente le cadre juridique applicable aux techniques de renseignement et met à la disposition du public les délibérations et rapports de la commission non couverts par le secret de la défense nationale.

3. Les recours contre la mise en œuvre des techniques de renseignement : une stabilité globale dans l'utilisation des voies de recours

Ni la voie de recours administrative que constitue la faculté de saisir la CNCTR d'une réclamation, ni la voie de recours contentieuse auprès du Conseil d'État n'ont connu d'évolution déterminante en 2017 par rapport à 2016.

3.1. Une hausse mesurée du nombre de réclamations adressées à la CNCTR

Toute personne peut saisir la CNCTR, conformément à l'article L. 883-4 du code de la sécurité intérieure, d'une réclamation tendant à ce que la commission vérifie qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard. Une faculté de réclamation similaire est prévue à l'article L. 854-9 du même code à l'égard des mesures de surveillance des communications électroniques internationales.

Comme la CNCTR l'indiquait dans son premier rapport d'activité[94], le pouvoir de vérification que lui confie la loi porte sur les seules techniques de renseignement prévues au livre VIII du code de la sécurité intérieure, à savoir des techniques mises en œuvre par des services de renseignement pour des finalités administratives. Cette compétence n'inclut donc ni les mesures de surveillance ordonnées par l'autorité judiciaire ni celles, au demeurant illégales, que pratiqueraient des personnes privées.

La CNCTR mène les vérifications sur réclamation de la même manière et en utilisant les mêmes outils que lorsqu'elle effectue un contrôle *a posteriori* de sa propre initiative.

94 - Voir le point 5.1.1. du premier rapport d'activité 2015/2016 de la CNCTR.

Le nombre de réclamations reçues par la CNCTR en 2017 est en augmentation par rapport à 2016. En valeur absolue, celle-ci demeure néanmoins mesurée.

	2016	2017	Évolution
Nombre de réclamations reçues par la CNCTR	49	54	+10,2%

Trois de ces réclamations ont été présentées par des personnes ayant déjà saisi la CNCTR et souhaitant que des vérifications soient à nouveau conduites à leur sujet.

Comme en 2016, la CNCTR s'était fixée en 2017 l'objectif de répondre aux réclamations contenant toutes les informations nécessaires à leur traitement dans un délai inférieur à deux mois. Cet objectif a toujours été respecté.

Aucune réclamation n'a conduit la CNCTR à envoyer une recommandation au chef du service concerné, au ministre dont il relève ou au Premier ministre pour que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits, conformément à l'article L. 833-6 du code de la sécurité intérieure. En conséquence, la CNCTR ne s'est pas non plus trouvée dans la situation de devoir saisir le Conseil d'État d'un recours contentieux sur le fondement de l'article L. 833-8 du code, cette voie de recours étant ouverte lorsque le Premier ministre ne donne pas suite aux recommandations de la commission.

Le dispositif propre aux « lanceurs d'alerte »

Pour garantir qu'il soit mis fin aux éventuelles violations manifestes du cadre juridique applicable aux techniques de renseignement, l'article L. 861-3 du code de la sécurité intérieure prévoit que les agents des services de renseignement ayant connaissance, dans l'exercice de leurs fonctions, d'une telle violation, peuvent porter ces faits à la connaissance de la seule CNCTR. Il appartient alors à la commission, au vu des éléments qui lui ont été transmis, de faire usage le cas échéant des pouvoirs de contrôle que lui attribue la loi.

En 2017, la CNCTR n'a pas été saisie sur le fondement de l'article L. 861-3 du code de la sécurité intérieure. Ces dispositions n'ont pas reçu application depuis l'entrée en vigueur du nouveau cadre légal en 2015.

3.2. Une légère diminution du nombre de recours formés devant le Conseil d'État

La procédure contentieuse spéciale prévue aux articles L. 773-1 et suivants du code de justice administrative permet de demander à une formation spécialisée du Conseil d'État de vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à l'encontre d'une personne. Les membres et le rapporteur public de la formation spécialisée sont habilités ès qualités à connaître d'informations couvertes par le secret de la défense nationale.

La formation spécialisée du Conseil d'État peut être saisie, sur le fondement de l'article L. 841-1 du code de la sécurité intérieure, par toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR. Toutefois, en matière de surveillance des communications électroniques internationales, seul le président ou trois membres au moins de la commission peuvent présenter une requête au Conseil d'État.

En 2016, le Conseil d'État avait été saisi de 9 requêtes concernant la mise en œuvre de techniques de renseignement. En 2017, 6 requêtes ont été présentées. Le Conseil d'État a rendu 6 décisions en 2016 et 3 en 2017. Au 31 décembre 2017, 5 affaires demeuraient en instance.

En 2017, la CNCTR a produit des observations sur tous les recours qui lui ont été communiqués par le Conseil d'État.

Dans une décision du 6 novembre 2017[95], le Conseil d'État a, pour la première fois, eu à se prononcer sur des moyens tirés de la violation d'articles de la convention de sauvegarde des droits de l'homme et des libertés fondamentales. Il a jugé que les modalités d'examen des recours par la formation spécialisée prévue à l'article L. 773-2 du code de justice administrative « *garantissent le respect de l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés*

95 - Voir la décision du Conseil d'État du 6 novembre 2017 n° 408495, reproduite en annexe n° 7 au présent rapport, notamment son paragraphe n° 7.

fondamentales », à savoir le droit d'exercer un recours effectif devant une instance nationale en cas de violation de droits et libertés reconnus par la convention. En outre, le juge administratif a indiqué avoir pu, en l'espèce, « *s'assurer notamment de l'absence de violation par l'administration des exigences de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* », qui protège le droit de toute personne au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

Étude

La notification aux personnes concernées des mesures de surveillance mises en œuvre à leur encontre par le passé

Garantir, dans la mesure du possible, que toute personne légalement surveillée ignore qu'elle fait l'objet d'une surveillance paraît une évidence pour les services de renseignement, qui font du secret l'une des conditions de l'efficacité de leur action. Si une personne se sait surveillée, les techniques de renseignement mises en œuvre à son encontre se heurteront, selon toute vraisemblance, à des efforts redoublés de dissimulation, et les informations espérées n'en seront que plus difficiles à obtenir.

Ce besoin de secret doit être cependant concilié, dans une société démocratique protégeant l'État de droit, avec la faculté ouverte à toute personne de s'assurer que sa vie privée a été respectée et, dans les cas où l'autorité publique y a porté atteinte, que les mesures intrusives étaient légales, en particulier qu'elles étaient proportionnées aux motifs poursuivis.

La conciliation entre le secret des activités de renseignement et le droit reconnu à toute personne d'exercer un recours contre des mesures de surveillance peut prendre la forme de vérifications intermédiées : la personne se tourne vers un tiers, organisme de contrôle spécifique ou juridiction, pour que cette institution indépendante tierce, habilitée à connaître des secrets du renseignement, effectue toutes vérifications nécessaires au nom du requérant.

Une autre forme de conciliation consiste à prévoir qu'une personne puisse, dans certains cas et selon certaines modalités, être informée qu'elle a fait l'objet d'une surveillance. Cette information, dénommée ci-après « notification », est destinée, en renforçant la transparence sur des mesures administratives

attentatoires à la vie privée, à permettre aux personnes concernées de s'en défendre le cas échéant en connaissance de cause.

Dans le présent rapport, la CNCTR a souhaité examiner la question de cette notification, afin de contribuer à la réflexion sur les meilleures garanties pouvant être apportées au respect de la vie privée dans le cadre des activités de renseignement.

1. La jurisprudence développée par les juges européens sur la notification

La Cour européenne des droits de l'homme (CEDH) s'est prononcée par plusieurs arrêts sur la conformité de la mise en œuvre de techniques de renseignement à la convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Au regard de la convention, la question de la notification de ces mesures aux personnes surveillées concerne plus particulièrement le respect des articles 8 et 13. Le premier protège le droit de toute personne au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Le second reconnaît à toute personne dont les droits et libertés auraient été méconnus le droit d'exercer un recours effectif devant une instance nationale. La CEDH a dégagé plusieurs principes concernant la notification, selon les législations en cause.

Dans un arrêt du 6 septembre 1978[96], la CEDH, après avoir relevé que « *si on ne l'avise pas des mesures prises à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice* », s'est interrogée « *sur la possibilité pratique d'exiger une notification ultérieure dans tous les cas* ». Elle a estimé que « *l'activité ou le danger qu'un ensemble de mesures de surveillance tend à combattre peut subsister pendant des*

96 - Voir l'arrêt de la CEDH du 6 septembre 1978, n° 5029/71, affaire Klass et autres contre Allemagne, notamment les paragraphes n° 57, n° 58 et n° 68.

années, voire des décennies, après leur levée », qu'« *une notification ultérieure à chaque individu touché par une mesure désormais levée pourrait bien compromettre le but à long terme qui motivait à l'origine la surveillance* » et que « *pareille notification risquerait de contribuer à révéler les méthodes de travail des services de renseignements, leurs champs d'observation et même, le cas échéant, l'identité de leurs agents* ». En conséquence, la cour a jugé que, dès lors que la mesure de surveillance était justifiée au regard de l'article 8 de la convention, « *il ne saurait être incompatible avec cette disposition de ne pas informer l'intéressé dès la fin de la surveillance, car c'est précisément cette abstention qui assure l'efficacité de l'"ingérence"* ».

La CEDH admet donc que la notification ne soit pas systématique, même après la fin de la surveillance. Dans une décision du 29 juin 2006[97], la cour a néanmoins considéré « *souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction* ».

L'existence de procédures de notification et les conditions dans lesquelles cette notification peut être effectuée demeurent un élément d'appréciation parmi tous ceux composant la législation applicable. Aussi la CEDH n'a-t-elle pas jugé, dans ses arrêts les plus récents, qu'une procédure de notification était par elle-même obligatoire.

Dans des arrêts du 26 avril 2007[98], du 28 juin 2007[99] et du 4 décembre 2015[100], la CEDH a condamné les États concernés pour violation de l'article 8 ainsi que, dans la deuxième affaire, de l'article 13 de la convention en raison d'un ensemble de défaillances en matière de garanties légales, parmi lesquelles figurait l'absence de toute procédure de notification. En revanche, dans un arrêt du 18 mai 2010[101], la cour, après avoir analysé la voie de

97 - Voir la décision d'irrecevabilité de la CEDH du 29 juin 2006, n° 54934, affaire Weber et Saravia contre Allemagne, notamment le paragraphe n° 135.

98 - Voir l'arrêt de la CEDH du 26 avril 2007, n° 71525/01, affaire Dumitru Popescu contre Roumanie.

99 - Voir l'arrêt de la CEDH du 28 juin 2007, n° 62540/00, affaire Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev contre Bulgarie.

100 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 288, dans lequel la cour résume sa jurisprudence en matière de notification.

101 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 189.

recours que prévoit la législation britannique contre les mesures de surveillance menées par les services de renseignement devant une juridiction spécialisée dénommée *Investigatory Powers Tribunal*, a considéré que « *la politique gouvernementale de "non-confirmation et de non-dénégation" serait remise en cause si un recours (...) pouvait conduire à dévoiler aux plaignants la mise en œuvre d'une opération d'interception, raison pour laquelle elle estime que la [juridiction] peut à bon droit se borner à les informer qu'aucune décision n'a été rendue en leur faveur* ».

La Cour de justice de l'Union européenne (CJUE) s'est par ailleurs également prononcée sur la question de la notification dans un arrêt du 21 décembre 2016[102].

S'appuyant sur l'article 15 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, la cour s'est reconnue compétente pour apprécier la conformité à la Charte des droits fondamentaux de l'Union européenne de législations nationales destinées à lutter contre la criminalité. Les mesures prévues par ces législations incluaient la conservation généralisée de données de connexion acheminées par les opérateurs de communications électroniques et l'accès d'autorités publiques aux données conservées.

Selon la CJUE, « *il importe que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités* ». La cour a estimé en effet que « *cette information est, de fait, nécessaire pour permettre [aux personnes concernées] d'exercer, notamment, le droit de recours* » contre la surveillance décidée à leur encontre.

La CJUE, qui a introduit ces considérations dans la motivation de son arrêt, n'a toutefois pas statué sur le sujet de la notification dans le dispositif final.

102- Voir l'arrêt de la CJUE du 21 décembre 2016, affaires C 203/15 (Tele2 *Sverige* AB contre *Post- och telestyrelsen*) et C 698/15 (*Secretary of State for the Home Department* contre Tom Watson, Peter Brice et Geoffrey Lewis), notamment le paragraphe n° 121 de la motivation et l'article 2 du dispositif.

2. L'existence de procédures de notification dans certains États membres de l'Union européenne

La CNCTR n'a pas l'ambition de mener une étude exhaustive des types de notifications prévues par la loi dans d'autres États membres de l'Union européenne (UE), mais souhaite mentionner quelques exemples susceptibles de retenir l'attention.

En Allemagne, l'article 12 de la loi relative aux restrictions apportées au secret des correspondances, de la poste et des télécommunications[103] énonce, dans sa rédaction en vigueur fin 2017, un principe général de notification assorti de limites, conformément à l'article 10 de la loi fondamentale de la République fédérale d'Allemagne[104].

Toute personne ayant fait l'objet d'une mesure de surveillance ciblée doit en être informée, après que la surveillance a pris fin. Toutefois, la notification n'a pas lieu tant qu'il ne peut être exclu qu'elle mette en danger le but poursuivi par la surveillance ou tant qu'il demeure prévisible qu'elle nuise gravement au bien de la République fédérale ou d'un Land.

L'absence de notification ne peut se prolonger plus de douze mois après la fin de la surveillance sans l'accord de la commission indépendante, dénommée « *G10-Kommission* »[105], que la loi a chargée de contrôler la légalité et la nécessité des mesures de surveillance. La commission fixe alors

---

103 - Voir *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, § 12 Mitteilungen an Betroffene*. Initialement adoptée par le Bundestag le 13 août 1968, la loi a été intégralement récrite par une loi du 26 juin 2001 puis a connu plusieurs modifications jusqu'en août 2017.

104 - Voir *Grundgesetz für die Bundesrepublik Deutschland, Artikel 10*. Cet article reconnaît l'inviolabilité des correspondances, des envois postaux et des télécommunications, tout en prévoyant que des restrictions peuvent être apportées à ce secret dans des conditions prévues par la loi. Lorsque les restrictions tendent à protéger l'ordre public dans une société libre et démocratique ou l'intégrité ou la sûreté de la République fédérale ou d'un Land, la loi peut prévoir que la personne concernée n'est pas informée des mesures de surveillance dont elle a fait l'objet.

105 - Cette dénomination fait référence à l'article 10 de la loi fondamentale de la République fédérale d'Allemagne. Les modalités de nomination et les missions de la commission sont fixées à l'article 15 de la loi relative aux restrictions apportées au secret des correspondances, de la poste et des télécommunications. Les membres de la commission sont nommés pour la durée d'une législature par l'organe parlementaire dénommé *Parlamentarisches Kontrollgremium*, chargé du contrôle politique des activités de renseignement.

la durée au terme de laquelle la notification devra intervenir. Elle peut également décider, en se prononçant à l'unanimité, que la notification n'aura jamais lieu :

- si l'un des obstacles légaux mentionnés ci-dessus se présente encore cinq ans après la fin de la surveillance ;
- s'il existe une probabilité proche de la certitude que cet obstacle persiste à l'avenir ;
- et si les conditions sont réunies pour que les données concernant la personne soient détruites par le service qui les a recueillies ainsi que par celui auquel elles ont été le cas échéant transmises.

Ces dispositions sont applicables à la surveillance non ciblée des communications internationales. Le délai de cinq ans court alors à compter du recueil des données. Il n'y a toutefois pas lieu de procéder à une notification lorsque les données ont été détruites immédiatement après leur recueil.

La notification est effectuée par le service qui a recueilli les données, en concertation avec celui auquel il les a, le cas échéant, transmises.

Les ministres dont relèvent les services de renseignement rendent compte chaque mois à la *G10-Kommission* des notifications effectuées ou des raisons qui s'y opposent. Lorsque la commission estime nécessaire une notification, celle-ci doit être effectuée sans délai[106].

Dans son dernier rapport d'activité rendu public[107], la *G10-Kommission* a communiqué des éléments statistiques concernant l'année 2016 en matière de surveillance ciblée. Cette année-là, les cas de 519 personnes physiques et morales qui avaient cessé d'être surveillées ont été examinés, que la surveillance les ait concernées à titre principal ou de manière incidente :

- 139 personnes, soit près de 27% des cas examinés, ont fait l'objet d'une décision autorisant la notification de la mesure de surveillance passée (parmi elles se trouvaient 51 personnes surveillées à titre principal et 88 surveillées de manière incidente) ;

106 - Voir *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, § 15 G10-Kommission, Absatz 7.*

107 - *Voir Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 G 10 (Berichtszeitraum 1. Januar bis 31. Dezember 2016)*, III, 3.

- 347 personnes, soit près de 67% des cas examinés, n'ont pu se voir notifier la surveillance passée car il a été estimé que les conditions légales n'étaient pas encore réunies[108] (parmi elles se trouvaient 116 personnes surveillées à titre principal et 235 de manière incidente) ;
- 33 personnes, soit un peu plus de 6% des cas examinés, ont fait l'objet d'une décision unanime de la commission constatant que la notification ne pourrait jamais avoir lieu (parmi elles se trouvaient 18 personnes surveillées à titre principal et 15 surveillées de manière incidente)[109].

Les cas des 519 personnes concernées se regroupaient en 94 dossiers, dont 83 provenant de l'office fédéral de protection de la Constitution (*Bundesamt für Verfassungsschutz* – ses missions sont proches de celles de la DGSI), 10 du service fédéral de renseignement (*Bundesnachrichtendienst* – ses missions sont proches de celles de la DGSE) et un seul de l'office de contre-intelligence militaire (*Amt für den militärischen Abschirmdienst* – ses missions sont proches de celles de la direction du renseignement de la sécurité et de la défense).

Dans le même rapport d'activité, la *G10-Kommission* a également publié des éléments statistiques en matière de surveillance non ciblée des communications internationales. Sur 43 dossiers concernant le terrorisme international et 135 dossiers concernant des filières d'immigration illégale, elle indique n'avoir pris que des décisions différant la notification ou la déclarant définitivement impossible.

La notification revêt une importance particulière dans le cadre juridique allemand car elle conditionne l'accès au juge pour contester la légalité d'une mesure de surveillance. L'article 13 de la loi relative aux restrictions

108 - Les raisons fondant la majeure partie des décisions différant la notification ont été, selon la *G10-Kommission*, la possibilité que soit décidée la reprise de la surveillance ou la circonstance que se poursuivaient d'autres mesures de surveillance que celles prévues par la loi relative aux restrictions apportées au secret des correspondances, de la poste et des télécommunications. Il a été par ailleurs décidé, conformément à la jurisprudence de la Cour constitutionnelle fédérale (*Bundesverfassungsgericht*) que les cas de ces personnes seraient à nouveau examinés après deux ans.

109 - Par comparaison, sur 1 628 personnes physiques et morales dont les cas ont été examinés en 2015, 400 personnes, soit près de 25% des cas examinés, ont reçu une notification, 1 040 personnes, soit près de 64% des cas examinés, ont fait l'objet d'une décision repoussant l'échéance de la notification, enfin 188 personnes, soit un peu plus de 11% des cas examinés, ont été définitivement privées de notification.

apportées au secret des correspondances, de la poste et des télécommunications prévoit en effet que le recours juridictionnel contre l'autorisation et la mise en œuvre d'une surveillance ciblée n'est ouvert qu'après que la personne a reçu notification qu'une mesure avait été prise à son encontre. La *G10-Kommission* précise qu'au début de l'année 2016, six mesures de surveillance ayant été exécutées faisaient l'objet d'un recours juridictionnel.

Aux Pays-Bas, l'article 34 de la loi du 7 février 2002 relative aux services de renseignement et de sécurité prévoit, dans sa rédaction en vigueur fin 2017[110], une obligation d'examiner la possibilité d'informer une personne ayant fait l'objet de mesures de surveillance limitativement énumérées (ouverture de courriers postaux, interception de communications électroniques, interceptions de communications non acheminées par des câbles, introduction dans un lieu d'habitation sans l'accord de son occupant pour y mettre en œuvre des dispositifs de surveillance). L'examen, qui incombe aux ministres dont relèvent les services de renseignement, doit être conduit tous les ans à l'issue d'une période de cinq ans après la fin de la surveillance.

L'obligation d'examen disparaît lorsque la notification pourrait raisonnablement avoir les conséquences suivantes :

- révéler les sources d'un service, y compris celles de services étrangers ;
- nuire gravement aux relations des Pays-Bas avec d'autres pays ou des organisations internationales ;
- révéler l'utilisation spécifique d'une méthode par un service ou l'identité d'une personne qui a concouru à l'utilisation de cette méthode par le service.

110 - Voir *Wet op de inlichtingen- en veiligheidsdiensten 2002, Artikel 34*. Le cadre juridique en vigueur depuis 2002 devait être progressivement remplacé par la loi du 26 juillet 2017 (voir *Wet op de inlichtingen- en veiligheidsdiensten 2017*) mais à l'occasion d'un référendum consultatif, qui s'est tenu le 21 mars 2018, les électeurs hollandais ont majoritairement désapprouvé la nouvelle loi, ce qui pourrait conduire le Gouvernement à modifier le texte.

Lorsque la notification n'est pas possible, la commission indépendante instituée à l'article 64 de la loi du 7 février 2002 pour contrôler l'action des services de renseignement est tenue informée de cette impossibilité et de ses raisons. De sa propre initiative, la commission peut, aux termes du même article 64, rendre un avis aux ministres compétents sur l'application de l'article 34 de la loi.

La notification doit être écrite et ne peut contenir d'autres informations que :

- l'identité de la personne concernée ;
- la technique de renseignement mise en œuvre à l'encontre de cette personne ;
- l'autorité ayant accordé l'autorisation de mise en œuvre ;
- la date de l'autorisation ;
- la durée de la mise en œuvre et, le cas échéant, le lieu d'habitation où le service s'est introduit sans l'accord de son occupant.

Pour d'autres exemples, la CNCTR invite à consulter les deux études publiées par l'Agence des droits fondamentaux de l'Union européenne en novembre 2015[111] et en octobre 2017[112] sur les cadres légaux applicables aux activités de renseignement dans les pays membres de l'UE.

Selon les résultats de ces études, vingt États membres de l'UE ont adopté des dispositions légales comportant une obligation de notification ou, à défaut, la faculté pour toute personne de saisir un organe de contrôle chargé de vérifier la légalité d'éventuelles mesures de surveillance.

Lorsqu'une notification est prévue, les prescriptions légales décrites dans les études varient :

- en ce qui concerne le champ d'application : la notification peut être restreinte aux mesures de surveillance ciblée ou, de manière plus rare, étendue aux mesures de surveillance non ciblée, telles que

111 - Voir l'étude intitulée *Surveillance by intelligence services : fundamental rights safeguards and remedies in the European Union – Volume I : mapping Member States' legal frameworks.*

112 - Voir l'étude intitulée *Surveillance by intelligence services : fundamental rights safeguards and remedies in the European Union – Volume II : field perspectives and legal update.*

celles visant les communications internationales ; s'agissant de la surveillance ciblée, la notification peut n'être prévue que pour certaines techniques de renseignement ;

- en ce qui concerne l'autorité compétente pour décider d'effectuer, de différer ou d'empêcher la notification : il peut s'agir de l'autorité administrative dont relèvent les services de renseignement, d'une autorité indépendante de contrôle, soit spécifique aux activités de renseignement, soit chargée d'assurer la protection des données personnelles de manière générale, ou encore d'une juridiction ;
- en ce qui concerne le délai devant s'écouler entre la fin de la surveillance et la notification : ce délai est variable, de même que la périodicité selon laquelle une décision de différer une notification doit à nouveau être examinée ;
- en ce qui concerne les motifs ou les circonstances pouvant faire obstacle, temporairement ou définitivement, à la notification : il s'agit essentiellement de protéger les surveillances en cours, la sécurité nationale, la conduite des relations internationales ou les sources et les méthodes opérationnelles des services de renseignement.

3. La solution retenue par le législateur français

Lorsqu'il a rénové le cadre juridique applicable aux activités de renseignement en 2015, le législateur français a dû, au regard des principes constitutionnels nationaux, concilier des exigences parfois opposées. Comme le conseil constitutionnel l'a jugé[113], il devait favoriser « *la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle* » et ne pas porter atteinte au « *secret de la défense nationale, qui participe des exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* ». D'autre part, il devait favoriser « *l'exercice des droits et des libertés constitutionnellement garantis* », au nombre desquels « *figurent le droit au respect de la vie privée, l'inviolabilité du domicile et le secret des correspondances, protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789* » ainsi que « *le droit des personnes intéressées à exercer un recours juridictionnel effectif, le droit à un procès équitable ainsi que le principe du contradictoire* » découlant de l'article 16 de la même Déclaration.

Pour effectuer la conciliation entre ces exigences, la loi n'a pas prévu de mécanisme de notification mais a institué des voies de recours ouvertes à toute personne.

La loi dispose que la mise en œuvre des techniques de renseignement, dès lors qu'elle est couverte par le secret de la défense nationale, ne peut être portée à la connaissance des personnes surveillées ni par l'autorité de contrôle indépendante qu'est la CNCTR, ni par le juge administratif chargé d'apprécier la légalité des mesures de surveillance. L'article L. 833-4 du code de la sécurité intérieure défend ainsi à la CNCTR de « *confirmer ni infirmer* » la mise en œuvre d'une technique. Lorsqu'il constate qu'aucune illégalité n'a été commise, le Conseil d'État est soumis à la même interdiction, en vertu de l'article L. 773-6 du code de justice administrative.

113 - Voir la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015, notamment ses paragraphes n° 2 à n° 5 et n° 82.

En contrepartie, toute personne peut saisir la CNCTR d'une réclamation tendant à ce que la commission vérifie, sur le fondement des articles L. 833-4 ou L. 854-9 du code de la sécurité intérieure, qu'aucune technique de renseignement n'a été irrégulièrement mise en œuvre à son encontre, ce qui inclut les mesures de surveillance des communications électroniques internationales. Toute personne ayant exercé cette faculté de réclamation peut ensuite présenter, conformément à l'article L. 841-1 du code de la sécurité intérieure, un recours contentieux devant une formation spécialisée du Conseil d'État en matière de surveillance nationale. Si cette voie de recours n'est pas directement ouverte aux requérants pour les mesures de surveillance des communications électroniques internationales, la CNCTR peut contester de telles mesures devant le juge administratif lorsqu'elle estime qu'une illégalité a été commise.

Ainsi, si les personnes surveillées ne peuvent être informées des techniques de renseignement mises en œuvre à leur encontre, la loi leur offre la possibilité de faire vérifier la légalité de cette éventuelle mise en œuvre par une autorité administrative indépendante puis par la juridiction suprême de l'ordre administratif.

Au reste, l'impossibilité d'avoir connaissance des mesures de surveillance n'est pas absolue. L'article L. 773-7 du code de justice administrative prévoit que le Conseil d'État, lorsqu'il constate qu'une technique de renseignement a été irrégulièrement mise en œuvre, informe la personne concernée qu'une illégalité a été commise et peut, saisi de conclusions en ce sens, indemniser cette personne du préjudice qu'elle a éventuellement subi. Dans un tel cas, une forme de notification a donc lieu.

Enfin les documents relatifs à la mise en œuvre des techniques de renseignement sont soumis aux dispositions régissant la communication des archives publiques. En vertu de l'article L. 213-2 du code du patrimoine, les documents dont la communication porte atteinte au secret de la défense nationale, aux intérêts fondamentaux de l'État dans la conduite de la politique extérieure, à la sûreté de l'État et à la sécurité publique sont librement accessibles au terme d'une durée de cinquante ans[114]. L'article

114 - Le délai est toutefois porté à cent ans pour les documents couverts ou ayant été couverts par le secret de la défense nationale dont la communication est de nature à porter atteinte à la sécurité de personnes nommément désignées ou facilement identifiables.

L. 213-3 du même code prévoit également qu'une dérogation peut être accordée pour consulter les archives publiques avant l'expiration des délais légaux, « *dans la mesure où l'intérêt qui s'attache à la consultation de ces documents ne conduit pas à porter une atteinte excessive aux intérêts que la loi a entendu protéger* ».

Dans ce contexte, la CNCTR accomplit, de sa propre initiative ou sur réclamation de toute personne, la mission de contrôle dont la charge le cadre juridique en vigueur. Elle n'a pas constaté, à ce jour, de difficulté dans l'exercice du droit au recours, reconnu à toute personne par la loi, contre la mise en œuvre d'une technique de renseignement.

Annexes

Annexe n° 1

Délibération de la CNCTR n° 3/2016 du 8 décembre 2016

Saisie pour avis par le garde des sceaux, ministre de la justice[1], d'un projet de décret modifiant la partie réglementaire du code de la sécurité intérieure et relatif à la désignation des services relevant du ministère de la justice autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes :

I. Remarques de portée générale

La CNCTR relève que le projet de décret est pris pour l'application de l'article L. 811-4 du code de la sécurité intérieure, qui prévoit qu'un décret en Conseil d'État pris après avis de la CNCTR désigne les services, autres que les services spécialisés de renseignement, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code.

Un premier décret[2] a été pris le 11 décembre 2015 pour désigner ceux de ces services, dits du « second cercle », qui relèvent du ministre de l'intérieur ou sont placés sous l'autorité d'emploi du ministre de la défense. Préalablement, la CNCTR avait rendu un avis sur le projet de texte, dans sa délibération n° 2/2015 du 12 novembre 2015.

1 - Le ministre de la justice a adressé à la commission une saisine initiale, reçue le 8 novembre 2016, et une saisine rectificative, reçue le 29 novembre 2016.

2 - Il s'agit 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.

Modifié par 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, l'article L. 811-4 du code de la sécurité intérieure rend désormais possible la désignation de services du « second cercle » relevant du ministère de la justice. C'est l'objet du nouveau projet soumis à l'avis de la commission. Ce projet vise à inclure dans le « second cercle » les services du garde des sceaux chargés du renseignement pénitentiaire, à savoir le futur bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire.

a) La CNCTR reprend l'intégralité des remarques de portée générale qu'elle avait formulées dans sa délibération du 12 novembre 2015.

Elle rappelle notamment que la nature et le nombre de techniques auxquelles peuvent avoir accès les services du « second cercle » dépend, à ses yeux, de la part qu'occupe le renseignement au sein de leurs missions ainsi que de l'expertise technique requise pour mettre en œuvre les techniques de manière sûre. En l'espèce, la commission constate que le futur bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire, s'ils se consacreront exclusivement au recueil et à l'exploitation du renseignement, disposeront, eu égard à leur création récente, de moyens humains et matériels encore modestes.

La CNCTR rappelle également que l'exercice effectif de la mission de contrôle confiée à la commission par la loi nécessite qu'elle puisse, outre le contrôle *a priori* sur les demandes tendant à mettre en œuvre une technique, mener à bien un contrôle *a posteriori* sur les données recueillies. Ceci impose une centralisation des données recueillies, auxquelles la CNCTR doit avoir un accès permanent, complet et direct, conformément à l'article L. 833-2 du code de la sécurité intérieure. Pour les services du « second cercle », cette centralisation doit, du point de vue de la commission, être réalisée de préférence par le groupement interministériel de contrôle (GIC). Pendant une période transitoire qui doit être brève, la centralisation ne peut se concevoir qu'à un niveau élevé de l'administration centrale concernée. En l'espèce, la CNCTR estime que la centralisation à titre temporaire devrait s'effectuer au niveau de la direction de l'administration pénitentiaire du ministère de la justice.

b) La CNCTR constate que des techniques ont, jusqu'à présent, été mises en œuvre en milieu pénitentiaire par des services de renseignement autorisés à y recourir. Elle estime que l'ouverture, dans le projet de décret, de la faculté de mettre en œuvre des techniques aux services du ministère de la justice chargés du renseignement pénitentiaire n'exclut pas que tous les services de renseignement concernés par la surveillance du milieu pénitentiaire continuent à agir de façon coordonnée et complémentaire, en fonction de leurs missions, de leurs compétences et de leur expertise technique.

À cet égard, la CNCTR rappelle que les termes de l'article L. 811-4 du code de la sécurité intérieure permettent au service du « second cercle » demandeur soit de mettre en œuvre lui-même la technique, s'il en a la capacité, soit de faire réaliser l'opération par un opérateur technique ou par un autre service de renseignement disposant de l'expérience et des compétences requises.

c) La CNCTR relève que le projet de décret limite le recours aux techniques de renseignement par les services du ministère de la justice chargés du renseignement pénitentiaire aux finalités de prévention du terrorisme et de prévention de la délinquance et de la criminalité organisées, prévues respectivement au 4° et au 6° de l'article L. 811-3 du code de la sécurité intérieure. La commission estime ces finalités adaptées aux missions et aux besoins de l'administration pénitentiaire.

d) Dans le dernier état de sa saisine, le ministre de la justice précise que les techniques auxquelles ses services chargés du renseignement pénitentiaire souhaitent avoir recours pourraient être mises en œuvre « *en détention comme à l'extérieur des établissements* » pénitentiaires. Elles concerneraient ainsi « *les personnes détenues ainsi que leur entourage* », mais aussi, en lien avec les autres services de renseignement, « *les autres personnes confiées à l'administration pénitentiaire par l'autorité judiciaire ainsi que leur entourage* ».

Toutefois, pour des raisons d'efficacité et de spécialisation déjà évoquées ci-dessus au point b), la CNCTR recommande, en l'état, que les services du ministère de la justice chargés du renseignement pénitentiaire concentrent leur action sur les seules personnes détenues, qu'elles vivent intégralement en établissement pénitentiaire ou y soient seulement hébergées. Seraient ainsi concernées les personnes détenues au sens strict, y compris lorsqu'elles bénéficient d'une permission de sortir prévue à l'article 723-3 du code de

procédure pénale, mais aussi les personnes placées sous les régimes de la semi-liberté ou du placement à l'extérieur avec hébergement en établissement pénitentiaire, prévus à l'article 132-26 du code pénal. En revanche, la commission estime que les techniques de renseignement concernant les personnes placées sous main de justice en milieu ouvert et celles écrouées mais non hébergées en établissement pénitentiaire, telles que les personnes placées sous surveillance électronique en application de l'article 132-26-1 du code pénal, devraient être mises en œuvre par d'autres services de renseignement déjà structurés pour effectuer cette mission.

e) Enfin, la CNCTR note qu'en vertu de l'article 727-1 du code de procédure pénale[3], « *les agents individuellement désignés et habilités appartenant à l'administration pénitentiaire* » peuvent mettre en œuvre, « *sous le contrôle du procureur de la République territorialement compétent* », certaines techniques de renseignement « *aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues* ».

La plupart des techniques utilisables dans ce cadre juridique sont similaires à celles sollicitées dans le projet de décret soumis à l'avis de la CNCTR, par exemple les accès aux données de connexion, les interceptions de sécurité, l'utilisation d'*IMSI catchers* pour recueillir des données de connexion ou pratiquer des interceptions de correspondances, le recueil de données informatiques stockées ou encore la captation de flux de données informatiques. Ces techniques seraient dès lors susceptibles d'être mises en œuvre dans deux cadres juridiques différents, celui du code de la sécurité intérieure et celui du code de procédure pénale. Même si les finalités prévues dans le code de la sécurité intérieure sont distinctes de celles mentionnées dans le code de procédure pénale, la CNCTR n'écarte pas tout risque de recouvrement entre les deux régimes, qui relèvent l'un et l'autre de la police préventive. Or, dans ce cadre préventif, le premier régime prévoit une autorisation du Premier ministre, après avis de la CNCTR, pour mettre en œuvre toute technique, tandis que le second régime permettrait, en l'état du

3 - L'article 727-1 du code de procédure pénale a été créé par 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.

projet de décret pris pour l'application de l'article 727-1 du code de procédure pénale communiqué pour information à la commission, à des agents de l'administration pénitentiaire de mettre en œuvre ces mêmes techniques, à la condition que le procureur de la République en ait été préalablement informé et ne s'y soit pas opposé.

Eu égard à ce qui précède et sous réserve de l'appréciation que portera le Conseil d'État sur les garanties pour la protection de la vie privée et pour la sécurité de l'action de l'État qu'offrent respectivement les deux régimes, la CNCTR recommande au Gouvernement de privilégier l'application des dispositions du code de la sécurité intérieure dans le cas où l'un et l'autre des régimes seraient applicables.

II. Observations détaillées

1. Sur la répartition des compétences au sein des services de renseignement pénitentiaire

Le projet de décret soumis à l'avis de la CNCTR prévoit que, sous l'autorité du directeur de l'administration pénitentiaire, le bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire pourront être autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure.

En ce qui concerne l'échelon central, le garde des sceaux a indiqué à la CNCTR que le bureau central du renseignement pénitentiaire succèdera, au sein de la direction de l'administration pénitentiaire, à l'actuel bureau du renseignement pénitentiaire, créé en 2003. Le nouveau bureau central est destiné à centraliser et mettre en forme toutes les demandes tendant à la mise en œuvre de techniques de renseignement avant leur examen par le directeur de l'administration pénitentiaire puis par le ministre ou ses délégués.

En ce qui concerne l'échelon déconcentré, le garde des sceaux a fait savoir à la commission que les dix cellules interrégionales du renseignement pénitentiaire, situées au sein de chaque direction interrégionale, seront chargées, de mettre en œuvre les techniques au niveau territorial. Les

demandes d'autorisation ont vocation à être préparées par ces cellules ou à être visées par elles lorsqu'elles seront préparées par les délégués locaux au renseignement pénitentiaire présents dans les établissements.

La CNCTR considère l'organisation décrite ci-dessus adaptée pour assurer le contrôle interne et la coordination des demandes provenant des cellules interrégionales du renseignement pénitentiaire réparties sur l'ensemble du territoire.

2. Sur les techniques de renseignement autorisées

a) La CNCTR constate, à titre liminaire, que le ministre de la justice souhaite que ses services chargés du renseignement pénitentiaire puissent mettre en œuvre la plupart des techniques prévues au titre V du livre VIII du code de la sécurité intérieure, y compris celles portant sur les moyens de communication électronique des personnes concernées. Bien que l'introduction, la détention et l'usage de téléphones portables et de clefs USB ou 3G ne soient pas autorisés en détention[4], l'administration pénitentiaire rencontre en effet des difficultés à faire respecter cette interdiction.

b) Eu égard aux missions du bureau central du renseignement pénitentiaire et des cellules interrégionales du renseignement pénitentiaire ainsi qu'à la répartition de compétences entre le niveau central et le niveau déconcentré, la CNCTR émet un avis favorable à ce que les services mentionnés dans le projet de décret puissent être autorisés à mettre en œuvre les techniques suivantes :

- l'accès aux données de connexion en temps différé, prévu à l'article L. 851-1 du code de la sécurité intérieure (voir l'article 3 du projet de décret) ;
- la géolocalisation en temps réel, prévue à l'article L. 851-4 du code de la sécurité intérieure (voir l'article 4 du projet de décret) ;

4 - La méconnaissance de cette interdiction, énoncée dans les règlements intérieurs des établissements pénitentiaires (voir l'article 27 du règlement intérieur type des établissements pénitentiaires annexé à l'article R. 57-6-18 du code de procédure pénale), peut constituer le délit prévu à l'article 434-35 du code pénal, qui réprime le fait de faire parvenir un objet à une personne détenue ou de communiquer avec elle en dehors des cas autorisés par les règlements. Elle peut également constituer le délit prévu à l'article 321-1 du code pénal, qui sanctionne notamment le recel d'une chose provenant d'un délit (voir, à ce sujet, l'arrêt du 24 octobre 2007 de la Cour de cassation, chambre criminelle, n° 07-81583).

- le balisage, prévu à l'article L. 851-5 du code de la sécurité intérieure (voir l'article 5 du projet de décret) ;
- l'utilisation d'*IMSI catchers* pour capter des données de connexion et de localisation[5], prévue à l'article L. 851-6 du code de la sécurité intérieure (voir l'article 6 du projet de décret) ;
- l'interception de sécurité réalisée *via* le GIC[6], prévue au I de l'article L. 852-1 du code de la sécurité intérieure (voir l'article 7 du projet de décret) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé, prévues à l'article L. 853-1 (voir l'article 9 du projet de décret) ;
- le recueil et la captation de données informatiques, prévus aux 1° et 2° du I de l'article L. 853-2 du code de la sécurité intérieure (voir l'article 10 du projet de décret).

c) La CNCTR rappelle que le II de l'article L. 852-1 du code de la sécurité intérieure encadre de manière particulièrement restrictive l'utilisation d'*IMSI* catchers pour intercepter des correspondances.

La commission estime que le recours à cette technique doit être réservé à des services se consacrant exclusivement au renseignement, ce qui est le cas des services mentionnés dans le projet de décret. Toutefois, elle considère également que la mise en œuvre de la technique nécessite un niveau d'expérience et de technicité très élevé. À cet égard, la création récente des services du ministre de la justice chargés du renseignement pénitentiaire et leurs moyens tant humains que matériels encore modestes ne permettent pas de regarder comme adapté leur accès à cette technique. En conséquence, la CNCTR émet un avis défavorable, en l'état, à la possibilité pour ces services d'intercepter des correspondances par *IMSI catchers*.

---

5 - La CNCTR rappelle que, conformément au IV de l'article L. 851-6 du code de la sécurité intérieure, le Premier ministre a fixé le nombre maximal d'*IMSI catchers* pouvant être utilisés simultanément et réparti ce contingent entre les ministres concernés. Une modification de l'arrêté du Premier ministre est donc nécessaire, à tout le moins pour modifier la répartition du contingent.

6 - La CNCTR rappelle que, conformément au VI de l'article L. 852-1 du code de la sécurité intérieure, le Premier ministre a fixé le nombre maximal d'autorisations d'interceptions de sécurité simultanément en vigueur et réparti ce contingent entre les ministres concernés. Une modification de l'arrêté du Premier ministre est donc nécessaire, à tout le moins pour modifier la répartition du contingent.

Au reste, le recours à cette technique n'étant justifié que dans des circonstances caractérisées par une urgence et une gravité telles qu'une implication de services de renseignement du « premier cercle » serait nécessaire, la possibilité existe, en tout état de cause, *via* ces services de mettre en œuvre la technique en milieu pénitentiaire.

d) L'article 11 du projet de décret conduit enfin la CNCTR à apprécier la nature des lieux de détention au regard des dispositions du livre VIII du code de la sécurité intérieure.

La CNCTR estime que les lieux gérés par l'administration pénitentiaire ne peuvent être considérés comme des lieux publics pour l'application du livre VIII du code de la sécurité intérieure, dans la mesure où l'article D. 277 du code de procédure pénale prévoit qu'« *aucune personne étrangère au service ne peut être admise à visiter un établissement pénitentiaire qu'en vertu d'une autorisation spéciale délivrée par le chef d'établissement* ». La CNCTR en déduit qu'il s'agit de lieux privés au sens des articles L. 853-1 et L. 853-3 du code de la sécurité intérieure.

Dès lors que ces lieux privés sont mis à disposition et placés sous le contrôle de l'administration pénitentiaire, la CNCTR estime que, pour y mettre en œuvre les techniques de balisage (article L. 851-5 du code de la sécurité intérieure), de captation de paroles prononcées à titre privé (article L. 853-1 du même code), de captation d'images dans un lieu privé (article L. 853-1 du code), de recueil et de captation de données informatiques (article L. 853-2 du code), les services mentionnés dans le projet de décret devront solliciter les autorisations prévues à ces articles, sans être tenus de demander de surcroît une autorisation d'introduction dans un lieu privé sur le fondement de l'article L. 853-3 du code de la sécurité intérieure.

Cependant, la CNCTR considère que la cellule de détention, bien que faisant partie des lieux mis à disposition et placés sous le contrôle de l'administration pénitentiaire, doit bénéficier d'un statut particulier. Si le personnel de l'administration pénitentiaire peut pénétrer dans la cellule, la fouiller ou effectuer des contrôles à l'œilleton[7], il s'agit en effet d'un lieu dans lequel la

7 - L'article D. 269 du code de procédure pénale prévoit, par exemple, que « *les surveillants procèdent, en l'absence des détenus, à l'inspection fréquente et minutieuse des cellules et locaux divers où les détenus séjournent, travaillent ou ont accès* ». En outre, l'article D. 271 du même code dispose que « *la présence de chaque détenu doit être contrôlée au moment du lever et du coucher, ainsi que deux fois par jour au moins, à des heures variables* ».

personne détenue se voit reconnaître une protection particulière de son intimité[8].

La Cour européenne des droits de l'homme a jugé que le droit au respect de la vie privée, énoncé à l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, était applicable dans une cellule de détention[9]. Dans sa décision n° 2009-593 DC du 19 novembre 2009, le Conseil constitutionnel a considéré qu'il appartenait « *au législateur de garantir les droits et libertés dont [les personnes détenues] continuent de bénéficier dans les limites inhérentes aux contraintes de la détention* » (voir le considérant n° 4 de la décision). Le Conseil d'État[10] et la Cour de cassation[11] ont contrôlé la proportionnalité des atteintes portées au droit au respect de la vie privée par des mesures de surveillance mises en place dans des cellules de détention.

La CNCTR en conclut que la cellule de détention et les lieux assimilés tels que les unités de vie familiale[12], en ce qu'ils abritent une part essentielle de la vie privée des personnes détenues, doivent être soumis au régime le plus protecteur prévu par la loi et, partant, être regardés, pour l'application du livre VIII du code de la sécurité intérieure, comme des lieux d'habitation au sens de l'article L. 853-3 de ce code. Les techniques de balisage (article L. 851-5 du code de la sécurité intérieure), de captation de paroles prononcées à titre privé (article L. 853-1 du même code), de captation d'images dans un lieu privé (article L. 853-1 du code), de recueil et de captation de données informatiques (article L. 853-2 du code) ne pourront dès lors être mises en œuvre dans ces lieux sans que, outre l'autorisation d'y recourir, une autorisation d'introduction dans un lieu d'habitation ait été également accordée. Conformément au I de l'article L. 853-3 du code, la CNCTR examinera en formation collégiale la demande d'introduction et celles tendant à la mise en œuvre des techniques.

---

8 - L'article D. 270 du code de procédure pénale dispose, par exemple, que « *pendant la nuit (…) personne ne doit (…) pénétrer [dans les cellules] en l'absence de raisons graves ou de péril imminent* ». De plus, l'article 46 du règlement intérieur type des établissements pénitentiaires annexé à l'article R. 57-6-18 du code de procédure pénale autorise la personne détenue à « *aménager sa cellule d'une façon personnelle* ». Enfin, l'article 42 de la loi n° 2009-1436 du 24 novembre 2009 pénitentiaire dispose que « *toute personne détenue a droit à la confidentialité de ses documents personnels* ».

9 - Voir notamment l'arrêt du 5 novembre 2002, n° 48539/99, affaire Allan contre Royaume-Uni, ou la décision d'admissibilité du 1er juin 2004, n° 8704/03, Van der Graaf contre Pays-Bas.

10 - Voir l'ordonnance de référé du 28 juillet 2016 n° 401800.

11 - Voir l'arrêt du 17 mars 2015, chambre criminelle, n° 14-88351.

12 - Aux termes de l'article R. 57-8-14 du code de procédure pénale, « *les unités de vie familiale sont des locaux spécialement conçus afin de permettre aux personnes détenues de recevoir, sans surveillance continue et directe, des visites des membres majeurs de leur famille ou de proches majeurs (…)* ».

Annexe n° 2

Délibération de la CNCTR n° 1/2017 du 16 mars 2017

Saisie pour avis par le garde des sceaux, ministre de la justice[1], d'un projet de décret modifiant la partie réglementaire du code de la sécurité intérieure et relatif à la désignation des services relevant du ministère de la justice autorisés à recourir aux techniques mentionnées aux articles L. 851-1 (accès aux données de connexion en temps différé), L. 851-4 (géolocalisation en temps réel), L. 851-5 (balisage), L. 851-6 (recueil de données de connexion par *IMSI catcher*) et au I de l'article L. 852-1 (interception de sécurité) du code de la sécurité intérieure, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes :

I. Remarques de portée générale

La CNCTR relève que le projet de décret est pris pour l'application de l'article L. 855-1 du code de la sécurité intérieure[2], qui prévoit qu'un décret en Conseil d'État pris après avis de la CNCTR désigne les services de l'administration pénitentiaire qui peuvent être autorisés à recourir aux techniques de renseignement mentionnées ci-dessus, dans les conditions prévues aux titres II et V du livre VIII du code, à l'encontre des seules personnes détenues, 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.

1 - Voir le courrier du garde des sceaux, ministre de la justice, daté du 24 février 2017 et reçu le 7 mars suivant.

2 - L'article L. 855-1 du code de la sécurité intérieure a été créé par le II de l'article 35 de la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique.

a) À titre liminaire, la CNCTR s'interroge sur la nécessité de modifier, aux articles 2 à 8 du projet de décret, sept articles du code de la sécurité intérieure.

D'une part, aux termes de l'article L. 855-1 du code de la sécurité intérieure, le décret pris pour son application a pour seul objet de désigner les services de l'administration pénitentiaire autorisés à recourir à des techniques déjà mentionnées dans la loi, pour une finalité également déjà prévue par celle-ci.

D'autre part, les articles qu'envisage de modifier le projet de décret désignent les services du « second cercle » mentionnés à l'article L. 811-4 du code, à savoir ceux autorisés à recourir à des techniques pour des finalités prévues à l'article L. 811-3, distinctes de celle prévue à l'article L. 855-1.

La CNCTR suggère donc de remplacer les articles 2 à 8 du projet de décret par un article unique, qui pourrait être un article R. 855-1 au sein d'un titre V bis à créer au niveau réglementaire dans le livre VIII du code de la sécurité intérieure. Cette écriture simplifiée paraît plus à même de faire correspondre les dispositions réglementaires du code avec son architecture de niveau législatif.

b) La CNCTR rappelle qu'elle a déjà rendu deux avis sur des projets de décret[3] désignant des services, dits du « second cercle », autorisés à recourir aux techniques de renseignement mentionnées au titre V du livre VIII du code de la sécurité intérieure. La commission reprend l'intégralité des remarques de portée générale formulées dans ces deux précédents avis, que constituent sa délibération n° 2/2015 du 12 novembre 2015 et sa délibération n° 3/2016 du 8 décembre 2016.

En particulier, la CNCTR rappelle que la nature et le nombre de techniques auxquelles peuvent avoir accès les services du « second cercle » dépend, à ses yeux, de la part qu'occupe le renseignement au sein de leurs missions ainsi que de l'expertise technique requise pour mettre en œuvre les techniques de manière sûre.

---

3 - Le premier projet est devenu le 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. Le second projet est devenu le décret n° 2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la justice, 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.

En outre, dès lors que l'article L. 855-1 du code de la sécurité intérieure limite le recours aux techniques de renseignement qu'il mentionne à la surveillance des seules personnes détenues, la CNCTR renvoie à la définition de ces personnes qu'elle a énoncée dans sa délibération n° 3/2016 du 8 décembre 2016. Ne peuvent, selon la commission, être concernées que les personnes détenues au sens strict, qu'elles bénéficient ou non d'une permission de sortir prévue à l'article 723-3 du code de procédure pénale, ainsi que les personnes placées sous les régimes de la semi-liberté ou du placement à l'extérieur avec hébergement en établissement pénitentiaire, prévus à l'article 132-26 du code pénal. En revanche, la commission rappelle que cette définition exclut les personnes placées sous main de justice en milieu ouvert et celles écrouées mais non hébergées en établissement pénitentiaire, telles que les personnes placées sous surveillance électronique en application de l'article 132-26-1 du code pénal.

II. Observations détaillées

1. Sur les techniques de renseignement autorisées

La CNCTR relève qu'aux termes de l'article L. 855-1 du code de la sécurité intérieure, les services de l'administration pénitentiaire à désigner par décret sont autorisés à recourir à une liste limitative de techniques de renseignement.

L'article 8 du projet de décret prévoit, en outre, que les agents de ces services puissent être autorisés à s'introduire dans un véhicule ou dans un lieu privé, en application de l'article L. 853-3 du code de la sécurité intérieure, pour mettre en place, utiliser ou retirer un dispositif de localisation, communément dénommé « balise ».

La CNCTR constate, toutefois, que l'article L. 855-1 du code de la sécurité intérieure ne prévoit pas que les agents des services de l'administration pénitentiaire puissent être autorisés à s'introduire dans de tels lieux. De plus, l'article L. 853-3 du code dispose, au deuxième alinéa de son I, que seuls peuvent être autorisés à s'y introduire, parmi les agents des services du

« second cercle », ceux des services mentionnés à l'article L. 811-4 du code. Or si l'article L. 811-4 mentionne des services relevant du ministre de la justice, il restreint l'autorisation qui peut leur être accordée de recourir à des techniques aux seules finalités prévues à l'article L. 811-3, distinctes de celle prévue à l'article L. 855-1.

La CNCTR considère, en conséquence, qu'il n'existe pas de base légale permettant aux agents des services de l'administration pénitentiaire de s'introduire dans un véhicule ou dans un lieu privé pour recourir à une technique en application de l'article L. 855-1 du code de la sécurité intérieure. Elle émet donc un avis défavorable à cette faculté ouverte à l'article 8 du projet de décret.

2. Sur la répartition des compétences entre services de l'administration pénitentiaire

Le projet de décret soumis à l'avis de la CNCTR prévoit que, sous l'autorité du directeur de l'administration pénitentiaire, le bureau central du renseignement pénitentiaire, les cellules interrégionales du renseignement pénitentiaire et les délégations locales au renseignement pénitentiaire pourront être autorisés à recourir aux techniques mentionnées dans l'article L. 855-1 du code de la sécurité intérieure.

Le garde des sceaux a, par ailleurs, indiqué à la commission que le bureau central du renseignement pénitentiaire centraliserait et instruirait toutes les demandes de recours à des techniques avant leur examen par le directeur de l'administration pénitentiaire puis par le ministre ou ses délégués. Il a également précisé que les demandes avaient vocation à être préparées et les autorisations du Premier ministre mises en œuvre par les cellules interrégionales ou par les délégations locales au renseignement pénitentiaire.

La CNCTR, conformément à sa délibération n° 3/2016 du 8 décembre 2016, constate que le bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire se consacrent exclusivement à des missions de renseignement et développent leur expertise technique en la matière. Elle émet donc un avis favorable à ce que ces services puissent recourir aux techniques mentionnées à l'article L. 855-1 du code de la sécurité intérieure.

S'agissant des délégations locales au renseignement pénitentiaire, présentes au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues, le garde des sceaux a également fait valoir que, bien qu'elles ne consacrent, dans la plupart des cas, qu'une partie de leur activité au recueil du renseignement :

- les délégués locaux qui les composent se trouvent en contact quotidien avec les personnes à surveiller ou avec les sources de renseignement, ce qui peut les rendre plus à même de détecter les menaces motivant le recours à une technique mais aussi d'apprécier la pertinence des informations recueillies (un délégué pourra ainsi reconnaître plus facilement la voix de personnes dont les conversations téléphoniques seront écoutées ou mieux comprendre le contexte de ces conversations) ;
- ces délégués locaux ont vocation, en application de l'article 727-1 du code de procédure pénale, à être autorisés, pour la même finalité que celle prévue à l'article L. 855-1 du code de la sécurité intérieure, à intercepter et exploiter des données de connexion ou des conversations émises par des moyens de communications légaux ainsi qu'à recueillir les données stockées dans un équipement terminal ou un système informatique utilisé par une personne détenue.

Eu égard à ces éléments et au fait que la finalité prévue à l'article L. 855-1 du code de la sécurité intérieure touche au bon fonctionnement quotidien des établissements concernés, la CNCTR émet un avis favorable à ce que les délégations locales au renseignement pénitentiaire puissent être autorisées à préparer des demandes tendant à recourir aux techniques mentionnées dans cet article, sous réserve que les propositions de demandes ne soient transmises au bureau central du renseignement pénitentiaire qu'après avoir été validées par la cellule interrégionale du renseignement pénitentiaire compétente. Constituées, dans de nombreux établissements, d'un unique agent, les délégations locales devraient ainsi soumettre leurs propositions à un premier filtre avant instruction par le niveau central.

La CNCTR estime en outre que, nonobstant les actions de formation engagées, l'expertise technique et opérationnelle que requièrent une mise en œuvre sûre des techniques mentionnées aux articles L. 851-5 (balisage) et L. 851-6 (recueil de données de connexion par *IMSI catcher*) du code de la sécurité intérieure ainsi qu'une exploitation pertinente des données recueillies au moyen de cette dernière technique fait obstacle à ce que cette mise en œuvre et cette exploitation puissent être directement confiées aux délégations locales au renseignement pénitentiaire. Elle recommande donc que les agents des délégations locales ne soient pas autorisés à mettre en œuvre eux-mêmes les techniques mentionnées aux articles L. 851-5 (balisage) et L. 851-6 (recueil de données de connexion par *IMSI catcher*) du code de la sécurité intérieure. Elle recommande également que ces agents ne soient pas autorisés à exploiter directement les données recueillies au moyen de cette dernière technique.

3. Sur les dispositions applicables outre-mer

L'article d'application outre-mer étant vide dans la saisine du garde des sceaux, la CNCTR n'a pu délibérer ni rendre d'avis sur les dispositions projetées.

Annexe n° 3

Délibération de la CNCTR n° 2/2017 du 23 mars 2017

Règlement intérieur

La Commission nationale de contrôle des techniques de renseignement,

Sur la proposition de son président,

Vu le code de la sécurité intérieure, notamment son livre VIII ;

Vu le code de justice administrative ;

Vu la loi n° 83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires ;

Vu la loi n° 2013-907 du 11 octobre 2013 modifiée relative à la transparence de la vie publique, notamment son article 11 ;

Vu la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes ;

Vu l'ordonnance n° 2014-1329 du 6 novembre 2014 relative aux délibérations à distance des instances administratives à caractère collégial ;

Vu le décret n° 2014-90 du 31 janvier 2014 portant application de l'article 2 de la loi n° 2013 907 du 11 octobre 2013 relative à la transparence de la vie publique, notamment son chapitre Ier ;

Vu le décret n° 2015-1186 du 29 septembre 2015 relatif à l'organisation administrative et financière de la Commission nationale de contrôle des techniques de renseignement,

Adopte le règlement intérieur suivant :

I – Obligations des membres et des agents de la Commission nationale de contrôle des techniques de renseignement

Article 1er

Les membres et les agents de la Commission nationale de contrôle des techniques de renseignement, ci-après dénommée « la commission », s'abstiennent de tout comportement de nature à faire naître un doute sur l'indépendance de l'institution. Ils doivent prévenir toute situation de conflit d'intérêts.

Lorsqu'ils estiment que, pour une raison quelconque, de leur propre fait ou de celui d'autrui, leur indépendance n'est pas ou peut ne pas apparaître assurée, ils s'abstiennent de prendre part à la délibération ou au contrôle concerné et d'émettre un avis. Ils en informent le président préalablement à la délibération ou au contrôle.

Les membres et le secrétaire général adressent au président de la commission copie de la déclaration d'intérêts prévue au 6° de l'article 11 de la loi du 11 octobre 2013 susvisée. La déclaration d'intérêts de chaque membre est mise, de façon permanente, à la disposition des autres membres dans les locaux de la commission. Le président restitue aux membres et au secrétaire général leur déclaration d'intérêts dans un délai de six mois suivant la fin de leurs fonctions au sein de la commission.

Article 2

Les membres et les agents de la commission respectent une obligation générale de loyauté à l'égard de l'institution.

Les membres et les agents de la commission ne reçoivent ni ne sollicitent aucune instruction d'une quelconque autorité.

Article 3

Les membres et les agents de la commission observent le secret de la défense nationale, le secret professionnel et le devoir de discrétion professionnelle auxquels ils sont tenus par la loi.

Ces obligations se perpétuent après le terme du mandat de membre ou des fonctions d'agent de la commission.

Le secret de la défense nationale n'est pas opposable aux membres et aux agents de la commission entre eux. Ils se doivent mutuellement toute l'information utile au bon accomplissement de leurs missions.

Le partage du secret de la défense nationale avec un service ou un agent extérieur à la commission pour le traitement d'un dossier n'autorise pas la méconnaissance du secret couvrant une autre affaire.

Aucune affaire particulière ou générale couverte par le secret de la défense nationale ne peut être évoquée avec un service ou un agent qui n'a pas besoin d'en connaître et n'y est pas habilité.

Article 4

Les demandes soumises pour avis à la commission sont examinées avec impartialité et neutralité.

Investis d'une mission de contrôle des services autorisés à mettre en œuvre des techniques de renseignement, les membres et les agents de la commission ne peuvent avoir avec les agents de ces services que des relations conciliables avec l'exercice d'un tel contrôle.

Article 5

Les membres et les agents de la commission se soumettent, lors des contrôles dans les services de renseignement, aux règles de sécurité applicables aux personnes étrangères à ces services et à toutes celles qui leur seraient réglementairement imposées.

Ils ne se départissent jamais de la courtoisie requise.

Ils demandent aux responsables des lieux ainsi qu'aux agents exploitants de leur permettre l'accès aux données qui leur sont utiles et de leur fournir les documents nécessaires à l'accomplissement du contrôle. Ils consignent avec précision tout refus d'accès aux données, accidentel ou délibéré, et, plus généralement, tout refus de coopération qui risquerait de compromettre la conduite de leur mission.

Ils se gardent de tout jugement pendant le déroulement de la visite. Ils se bornent à recueillir les informations qui leur sont utiles, à établir leur véracité et à poser les questions requises par leur compréhension.

Ils veillent à ce que les questions qu'ils posent soient en lien direct avec les attributions de la commission. Ils précisent en tant que de besoin en quoi leurs demandes relèvent de ces attributions.

Dans leur rapport, ils veillent en toute objectivité à faire la part des faits établis et celle des hypothèses et mettent en lumière les considérations qui leur paraissent mériter un examen par les membres de la commission.

Article 6

Toute difficulté rencontrée par les membres et les agents de la commission dans l'exercice de leurs missions est portée à la connaissance du président, qui peut inviter la formation restreinte ou plénière de la commission à en débattre.

II – Formation plénière et formation restreinte

Article 7

Les formations plénière et restreinte fixent le calendrier de leurs réunions. Elles sont en outre réunies en tant que de besoin, à l'initiative du président.

Dans le cas prévu à l'article L. 821-7 du code de la sécurité intérieure, le président prend les dispositions nécessaires pour réunir la formation plénière dans les meilleurs délais.

Le président fixe l'ordre du jour des réunions en formations plénière et restreinte de la commission. Les membres de la commission peuvent demander l'inscription d'une question à cet ordre du jour.

Les documents utiles sont mis à la disposition des membres dans les locaux de la commission au plus tard vingt-quatre heures avant la séance.

Les formations plénière et restreinte de la commission statuent à la majorité des membres présents ou participant à la délibération, le président ayant voix prépondérante en cas de partage égal des voix.

En tant que de besoin, le président peut décider qu'une délibération sera organisée par tous moyens de communication électronique, dès lors que l'identification des participants et la confidentialité des débats sont assurées.

Le secrétaire général de la commission assure le secrétariat des séances et en établit le procès-verbal. Les procès-verbaux sont tenus à la disposition des membres dans les locaux de la commission.

Le président désigne les agents invités à assister aux séances des formations plénière et restreinte.

Article 8

S'il se trouve empêché, le président désigne celui des membres de la commission qui préside la formation plénière ou restreinte. Ce membre a voix prépondérante en cas de partage égal des voix.

Article 9

Les membres ont, dans les locaux de la commission, accès à tout moment aux avis émis sur les demandes soumises à la commission ainsi qu'aux suites données à ces avis par le Premier ministre.

Article 10

La formation plénière débat des principes régissant les avis rendus par la commission sur les demandes qui lui sont soumises ainsi que des contrôles effectués par la commission sur la mise en œuvre des techniques de renseignement.

Article 11

En concertation avec les membres de la commission, le président arrête le programme des visites de contrôle et les conditions dans lesquelles ces visites sont organisées. Il peut aussi décider de contrôles impromptus.

Les résultats des contrôles et les suites données par les services concernés sont portés à la connaissance des formations plénière ou restreinte de la commission.

Article 12

Lorsque le Premier ministre n'a pas donné suite à un avis de la commission sur une demande, la formation plénière en est informée dans les meilleurs délais et débat des suites à donner.

La formation plénière est informée des recommandations adressées au Premier ministre, tendant à ce que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits, en application des articles L. 833-6 ou L. 854-9 du code de la sécurité intérieure. Elle débat des suites données par le Premier ministre à ces recommandations.

La formation plénière décide des observations qu'elle juge utile d'adresser au Premier ministre en application de l'article L. 833-10 du code de la sécurité intérieure.

Article 13

La formation plénière débat de la réponse qui doit être apportée aux demandes d'avis que peuvent, en application de l'article L. 833-11 du code de la sécurité intérieure, adresser à la commission le Premier ministre, le président de l'Assemblée nationale, le président du Sénat et la délégation parlementaire au renseignement.

III – Secrétariat général et agents de la commission

Article 14

Les agents de la commission sont placés sous l'autorité du président. Ils assistent les membres de la commission dans la conduite de leurs missions.

Le secrétaire général anime et coordonne leur action.

IV – Traitement des demandes

Article 15

Le président fixe, en concertation avec les membres et les agents de la commission, les conditions dans lesquelles sont rendus les avis sur les demandes soumises à celle-ci.

Le président veille à ce que les délais impartis à la commission pour émettre ses avis soient respectés.

Article 16

L'appréciation de la légalité des demandes, en particulier celle de la proportionnalité des mesures envisagées, prend en compte les règles et principes posés par la loi, la jurisprudence, notamment celle du Conseil d'État statuant au contentieux, et la doctrine énoncée par les formations plénière et restreinte de la commission.

Article 17

Toutes les demandes soumises à la commission sont examinées à la lumière des informations communiquées, qui sont interprétées strictement, sans altération ni omission.

Lorsque toutes les informations nécessaires à l'examen de la demande n'ont pas été communiquées, la commission invite le service à l'origine de la demande à lui transmettre des informations complémentaires dans les meilleurs délais.

Le délai légal d'examen court à compter du moment où la commission estime que la demande est complète.

Article 18

Toute question nouvelle, toute difficulté sérieuse et toute incertitude sur la validité d'une demande sont, à l'initiative du président ou de l'un des membres de la commission, soumises, selon le cas, à la formation plénière ou à la formation restreinte de la commission.

V – Rapport public, communication et relations extérieures

Article 19

Dans les relations avec l'autorité politique, la commission est représentée par le président, qui rend compte à la formation plénière.

La communication publique de la commission est assurée par le président, en concertation avec les membres.

Les agents de la commission ne peuvent s'exprimer au nom de l'institution, sauf mandat exprès du président.

Article 20

Le rapport public d'activité, débattu et approuvé en formation plénière, est remis par le président au Président de la République, au Premier ministre et aux présidents des deux assemblées.

Le président invite les parlementaires membres de la commission à l'accompagner lors de la visite qu'il rend au président de l'assemblée dans laquelle ils siègent.

Article 21

Le président, en concertation avec les membres et les agents de la commission, prend toutes dispositions pour mener les échanges utiles dans les cadres européen et international et promouvoir le modèle français de contrôle des techniques de renseignement.

VI – Suspension du mandat, fin des fonctions ou démission d'un membre et vacance du poste de président

Article 22

La formation plénière de la commission délibère sur la suspension du mandat, la fin des fonctions ou la démission d'un membre pour l'un des motifs prévus à l'article 6 de la loi du 20 janvier 2017 susvisée.

La délibération se déroule une semaine au moins après que l'intéressé a été mis en mesure de présenter des observations écrites ou, à sa demande, d'être entendu par la formation plénière. Le vote a lieu à bulletin secret hors la présence de l'intéressé.

Article 23

Si le poste de président devient vacant pour quelque cause que ce soit, la fonction de président par intérim est exercée par le doyen d'âge des membres de la commission mentionnés aux 2° et 3° de l'article L. 831-1 du code de la sécurité intérieure, dans l'attente de l'entrée en fonctions du nouveau président.

VII – Dispositions finales

Article 24

Le présent règlement intérieur sera publié au Journal officiel de la République française.

Annexe n° 4

Délibération de la CNCTR n° 3/2017 du 26 avril 2017

Saisie pour avis par le Premier ministre[1], en application du VI de l'article L. 852-1 du code de la sécurité intérieure, d'un projet d'augmenter le nombre maximal des autorisations d'interceptions de sécurité pouvant être accordées simultanément, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

La CNCTR rappelle que le contingent des autorisations d'interceptions de sécurité simultanées avait été augmenté pour la dernière fois par une décision du Premier ministre du 27 avril 2015. Il avait alors été porté de 2 190 à 2 700. Le Premier ministre se propose désormais de l'élever à 3 040, soit une hausse d'environ 13%.

La CNCTR a constaté que le contingent actuel n'était pas loin d'être entièrement utilisé. Eu égard, d'une part, à l'aggravation de la menace terroriste et, d'autre part, à la faculté de recourir aux interceptions de sécurité désormais ouverte aux services du ministre de la justice chargés du renseignement pénitentiaire[2], la commission estime avéré le besoin d'accorder simultanément un nombre supérieur d'autorisations d'interception.

En conséquence, la CNCTR émet un avis favorable à l'augmentation du contingent envisagée et rappelle qu'en application du VI de l'article L. 852-1 du code de la sécurité intérieure, la décision du Premier ministre fixant ce contingent ainsi que sa répartition entre les ministres dont relèvent les services de renseignement doit être portée à sa connaissance.

1 - Voir le courrier du directeur du cabinet du Premier ministre, daté du 24 avril 2017.

2 - Voir, en premier lieu, les articles L. 811-4 et R. 852-1 modifiés du code de la sécurité intérieure. Voir, en second lieu, l'article L. 855-1 du code de la sécurité intérieure.

Annexe n° 5

Délibération de la CNCTR n° 4/2017 du 9 juin 2017

Saisie pour avis par le Premier ministre[1] en application de l'article L. 833-11 du code de la sécurité intérieure, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a examiné deux articles d'un projet de loi renforçant la lutte contre le terrorisme et la sécurité intérieure, qui concernent la surveillance des transmissions empruntant la voie hertzienne et sont destinés à se substituer à l'article L. 811-5 du code de la sécurité intérieure, déclaré contraire à la Constitution par le Conseil constitutionnel dans sa décision n° 2016-590 QPC du 21 octobre 2016.

À titre liminaire, la CNCTR rappelle que le Conseil constitutionnel, après avoir jugé que « l'exception hertzienne » prévue à l'article L. 811-5 du code de la sécurité intérieure, faute de garanties appropriées, portait une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances, avait fixé au 31 décembre 2017 la prise d'effet de son abrogation. Avant cette date et jusqu'à l'adoption éventuelle de nouvelles dispositions législatives, le Conseil constitutionnel avait exigé que la CNCTR fût régulièrement informée sur le champ et la nature des mesures prises en application de l'article censuré. Par une délibération du 10 novembre 2016, la CNCTR avait précisé le cadre de son contrôle en la matière.

En réponse à la saisine du Premier ministre, la CNCTR approuve l'économie générale du nouveau régime juridique, qui consiste, d'une part, à intégrer toutes les mesures de surveillance des transmissions hertziennes attentatoires

1 - Voir le courrier du secrétaire général du Gouvernement n° 1177/17/SG du 6 juin 2017. Des contacts informels préalables entre le Gouvernement et la CNCTR ont permis à la commission d'entreprendre son travail d'instruction avant cette saisine officielle.

à la vie privée dans le droit commun de la mise en œuvre des techniques de renseignement et, d'autre part, à rendre d'application résiduelle les mesures pouvant être prises sans autorisation spécifique préalable et constituant une nouvelle « exception hertzienne » d'ampleur nettement plus limitée que celle prévue à l'article L. 811-5 du code de la sécurité intérieure.

La CNCTR constate que les communications concernées par la nouvelle « exception hertzienne » sont celles empruntant **exclusivement** la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques. Il en résulte que les communications acheminées successivement par la voie hertzienne et la voie filaire ne pourront être légalement interceptées sur le fondement de ces dispositions, ce qui, de l'avis de la commission, lève définitivement l'ambiguïté que pouvait contenir la rédaction de l'article L. 811-5 du code de la sécurité intérieure.

La CNCTR formule en outre les observations suivantes, tendant à renforcer les mécanismes de contrôle sur l'ensemble des mesures prévues.

I. Sur l'encadrement des mesures de surveillance des transmissions hertziennes revêtant un caractère privé

a) La CNCTR constate que les transmissions hertziennes devant être regardées comme revêtant un caractère privé ne relèveront pas de la nouvelle « exception hertzienne ». Elles ne pourront être interceptées que sur le fondement d'une nouvelle technique de renseignement, prévue à un futur article L. 852-2 du code de la sécurité intérieure et soumise comme telle à autorisation préalable du Premier ministre accordée après avis de la commission ainsi qu'au contrôle *a posteriori* de sa mise en œuvre. Les correspondances interceptées ne pourront être conservées plus de trente jours à compter de leur recueil, à l'instar des correspondances recueillies lors des interceptions de sécurité prévues à l'article L. 852-1 du code.

D'accord avec ce principe, qui renforce la protection de la vie privée par rapport au droit existant, la CNCTR s'interroge toutefois sur la rédaction pertinente pour définir les réseaux de communications concernés. Si le projet de loi prévoit la possibilité d'intercepter un réseau hertzien « *lorsque*

ce réseau est réservé à l'usage d'un groupe fermé d'utilisateurs », la CNCTR propose l'expression : « *lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs* ». Cette rédaction, outre qu'elle fait clairement apparaître le lien entre atteinte à la vie privée et nécessité d'une autorisation, aurait l'avantage d'indiquer que le droit commun du renseignement ne s'applique pas uniquement aux communications par voie hertzienne impliquant plusieurs personnes, telles les communications par *private mobile radio* (PMR), mais aussi, le cas échéant, aux transmissions entre objets connectés qui peuvent n'appartenir qu'à une seule personne.

b) La CNCTR constate que le projet de loi prévoit également la suppression du terme « audiovisuels » au 2° du I de l'article L. 853-2 du code de la sécurité intérieure, ce qui a pour effet d'intégrer le recueil de certaines transmissions hertziennes dans le champ d'application d'une technique existante, la captation de données informatiques. Il peut s'agir de transmissions par protocoles de communication sans fil tel que le « wifi ».

La CNCTR estime que cette clarification de base légale constitue un progrès dans l'encadrement des techniques de renseignement, dans la mesure où le recueil des transmissions hertziennes concernées sera soumis au régime spécialement protecteur de la captation de données informatiques, qui ne peut notamment être autorisée sans respecter le principe de subsidiarité.

II. Sur l'encadrement de la nouvelle « exception hertzienne »

La CNCTR prend acte du fait que les nouveaux articles L. 854-9-1 à L. 854-9-3 du code de la sécurité intérieure, qui prévoient une faculté d'interception et d'exploitation des transmissions hertziennes par les services de renseignement sans autorisation spécifique préalable, auront un champ d'application résiduel puisque les transmissions concernées ne pourront être de celles qui entrent dans le champ d'application des techniques de renseignement de droit commun.

Pour la CNCTR, les interceptions résiduelles ne pourront concerner que les communications par réseaux hertziens ouverts, c'est-à-dire écoutables par toute

personne à la seule condition de régler un appareil de réception sur la fréquence utilisée. Il peut s'agir, d'une part, des fréquences pour radioamateurs ou pour *talkie-walkies* analogiques et, d'autre part, des communications internationales à longue distance.

Pour rendre la rédaction plus claire, la CNCTR suggère de remplacer la première phrase de l'article L. 854-9-1 du projet de loi par les dispositions suivantes : « *Les services de renseignement mentionnés aux articles L. 811-2 et L. 811-4 sont autorisés, aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, à intercepter et à exploiter les communications 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 technique de renseignement prévue aux chapitres I^er^ à IV* ».

Le projet de loi prévoit que les données ainsi recueillies dans le cadre de la nouvelle « exception hertzienne » ne pourront être conservées au-delà de délais qu'il fixe. Cette limitation, qui n'existait pas dans le cadre juridique résultant de l'article L. 811-5 du code de la sécurité intérieure, est bienvenue, selon la commission. Cependant la durée de conservation des renseignements recueillis non chiffrés, fixée à six ans par l'article L. 854-9-2, paraît trop longue et ne correspond à aucune durée existant dans le livre VIII du code de la sécurité intérieure pour des renseignements susceptibles de contenir le contenu de correspondances. La CNCTR recommande dès lors d'abaisser de six à quatre ans cette durée et de préciser qu'elle court à compter du recueil des communications, en s'inspirant des dispositions applicables aux correspondances internationales en application de l'article L. 854-5 du code.

L'article L. 854-9-3 prévoit que la CNCTR veillera au respect des champs d'application respectifs de la nouvelle « exception hertzienne » et des dispositions du code de la sécurité intérieure régissant les techniques de renseignement de droit commun. À cette fin, la commission disposera de capacités de contrôle des mesures prises par les services de renseignement dans le cadre de la nouvelle « exception hertzienne ». Ces dispositions sont également bienvenues, aux yeux de la CNCTR, car, nonobstant le caractère résiduel des articles L. 854-9-1 et suivants du code de la sécurité intérieure,

la commission doit, dans un cadre juridique rénové, avoir les moyens de s'assurer que ces dispositions ne sont pas utilisées à d'autres fins que celles très strictement limitées par la loi. Pour parfaire ce mécanisme de contrôle, la CNCTR recommande cependant de compléter le deuxième alinéa de l'article L. 854-9-3 en indiquant que la commission, « *peut, à sa demande, se faire présenter sur place les capacités d'interception mises en œuvre sur le fondement de cet article ainsi que les renseignements collectés et les transcriptions et extractions réalisées* ».

III. Sur l'encadrement des mesures mises en œuvre par les militaires des armées

La CNCTR constate que, par un nouvel article L. 2371-1 du code de la défense, les militaires des armées seront autorisés à mettre en œuvre la nouvelle « exception hertzienne », c'est-à-dire à pratiquer sans autorisation spécifique préalable les interceptions résiduelles prévues à l'article L. 854-9-1 du code de la sécurité intérieure.

La CNCTR estime légitime cette faculté dès lors qu'elle est limitée par la loi aux besoins de la défense militaire et de l'action de l'État en mer. Informée du champ et de la nature des mesures de surveillance mises en œuvre, la commission veillera au respect de ce champ d'application particulier.

Pour garantir la traçabilité des mesures prises, la CNCTR recommande en outre que la loi prévoie que ces mesures ne puissent être mises en œuvre que par des militaires individuellement désignés et habilités, comme c'est le cas au sein des services de renseignement.

Par ailleurs, la CNCTR relève qu'un nouvel article L. 2371-2 du code de la défense a pour but d'autoriser la direction générale de l'armement du ministère de la défense à utiliser des capacités d'interception de la nouvelle « exception hertzienne » à la seule fin d'effectuer des tests. Estimant que cette restriction n'apparaît pas suffisamment clairement dans le texte du projet de loi, la CNCTR propose de substituer à la fin de l'article L. 2371-2 les mots suivants : « *à la seule fin d'effectuer des tests et à l'exclusion de toute mesure d'exploitation des renseignements recueillis* ».

IV. Sur le pouvoir de réquisition prévu à l'article L. 871-2 du code de la sécurité intérieure

Par mesure de coordination, le projet de loi prévoit de supprimer de l'article L. 871-2 du code de la sécurité intérieure la possibilité ouverte aux ministres de la défense et de l'intérieur d'obtenir des données de connexion des opérateurs de communications électroniques et des fournisseurs de services au public en ligne, en vue de surveiller des transmissions hertziennes sur le fondement de l'article L. 811-5 du code de la sécurité intérieure censuré par le Conseil constitutionnel.

La CNCTR approuve cette modification et suggère de compléter la révision de l'article L. 871-2 du code en supprimant également le pouvoir de réquisition attribué au Premier ministre.

Dans une délibération classifiée du 28 avril 2016, la CNCTR avait constaté que ce pouvoir du Premier ministre, non soumis à l'avis préalable de la commission, était privé d'utilité par d'autres dispositions du code de la sécurité intérieure, telles que l'article L. 851-1 et le III de l'article L. 852-1, soumis quant à eux au contrôle de la CNCTR. Elle avait dès lors recommandé au Premier ministre de cesser tout recours à l'article L. 871-2, ce que celui-ci a décidé par une note du 20 mai 2016.

En conséquence, la CNCTR recommande que soient également supprimés de l'article L. 871-2 du code de la sécurité intérieure les mots : « *ainsi que le Premier ministre* ».

Annexe n° 6

Décision du Conseil constitutionnel n° 2017-648 QPC du 4 août 2017

La Quadrature du Net et autres [Accès administratif en temps réel aux données de connexion]

LE CONSEIL CONSTITUTIONNEL A ÉTÉ SAISI le 23 mai 2017 par le Conseil d'État (décision n° 405792 du 17 mai 2017), dans les conditions prévues à l'article 61-1 de la Constitution, d'une question prioritaire de constitutionnalité. Cette question a été posée pour les associations La Quadrature du Net, *French Data Network* et la Fédération des fournisseurs d'accès à internet associatifs, par la SCP Spinosi et Sureau, avocat au Conseil d'État et à la Cour de cassation. Elle a été enregistrée au secrétariat général du Conseil constitutionnel sous le n° 2017-648 QPC. Elle est relative à la conformité aux droits et libertés que la Constitution garantit de l'article L. 851-2 du code de la sécurité intérieure, dans sa rédaction résultant de la 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.

Au vu des textes suivants :

- la Constitution ;
- l'ordonnance n° 58-1067 du 7 novembre 1958 portant loi organique sur le Conseil constitutionnel ;
- le code de la sécurité intérieure ;
- la 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 ;

- le règlement du 4 février 2010 sur la procédure suivie devant le Conseil constitutionnel pour les questions prioritaires de constitutionnalité ;

Au vu des pièces suivantes :

- les observations présentées pour les associations requérantes par la SCP Spinosi et Sureau, enregistrées les 14 et 29 juin 2017 ;
- les observations présentées par le Premier ministre, enregistrées le 14 juin 2017 ;
- les observations en intervention présentées pour la Ligue des droits de l'homme, par la SCP Spinosi et Sureau, enregistrées le 14 juin 2017 ;
- les pièces produites et jointes au dossier ;

Après avoir entendu Me Patrice Spinosi, avocat au Conseil d'État et à la Cour de cassation, pour les associations requérantes et l'association intervenante, et M. Xavier Pottier, désigné par le Premier ministre, à l'audience publique du 25 juillet 2017 ;

Et après avoir entendu le rapporteur ;

LE CONSEIL CONSTITUTIONNEL S'EST FONDÉ SUR CE QUI SUIT :

1. L'article L. 851-2 du code de la sécurité intérieure, dans sa rédaction résultant de la loi du 21 juillet 2016 mentionnée ci-dessus, prévoit :

« *I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée susceptible d'être en lien avec une menace. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.*

« *II.- L'article L. 821-5 n'est pas applicable à une autorisation délivrée en application du présent article* ».

2. Les associations requérantes et l'association intervenante soutiennent que l'article L. 851-2, dans cette rédaction, porterait atteinte au droit au respect de la vie privée et au secret des correspondances dès lors, d'une part, que le champ des personnes dont les données de connexion sont susceptibles d'être ainsi recueillies en temps réel serait trop large et, d'autre part, que la durée de l'autorisation serait trop longue.

3. Par conséquent, la question prioritaire de constitutionnalité porte sur le paragraphe I de l'article L. 851-2 du code la sécurité intérieure.

Sur le fond :

4. En vertu de l'article 34 de la Constitution, il appartient au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis. Au nombre de ces derniers figurent le secret des correspondances et le droit au respect de la vie privée, protégés par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

5. Les dispositions contestées permettent à l'autorité administrative, pour la prévention du terrorisme, d'obtenir le recueil en temps réel des données de connexion relatives, d'une part, à une personne préalablement identifiée susceptible d'être en lien avec une menace et, d'autre part, aux personnes appartenant à l'entourage de la personne concernée par l'autorisation lorsqu'il y a des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation. Cette technique de recueil de renseignement est autorisée pour une durée de quatre mois renouvelable, conformément à l'article L. 821-4 du code de la sécurité intérieure.

6. En premier lieu, la procédure de réquisition administrative de données de connexion instituée par les dispositions contestées exclut l'accès au contenu des correspondances. Par suite, le grief tiré de la méconnaissance du droit au secret des correspondances doit être écarté.

7. En second lieu, d'une part, le recueil des données de connexion en temps réel ne peut être mis en œuvre que pour les besoins de la prévention du terrorisme. Ne peuvent, par ailleurs, être recueillis que les informations ou documents traités ou conservés par les opérateurs de télécommunication, les fournisseurs d'accès à un service de communication au public en ligne ou les hébergeurs de contenu sur un tel service.

8. D'autre part, cette technique de recueil de renseignement s'exerce dans les conditions prévues au chapitre Ier du titre II du livre VIII du code de la sécurité intérieure. En vertu de l'article L. 821-4 de ce code, elle est autorisée par le Premier ministre ou les collaborateurs directs auxquels il a délégué cette compétence, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, après avis préalable de la commission nationale de contrôle des techniques de renseignement. Elle est autorisée pour une durée de quatre mois renouvelable. En vertu du paragraphe II de l'article L. 851-2, la procédure d'urgence absolue prévue à l'article L. 821-5 de ce code n'est pas applicable. En application de l'article L. 871-6 du même code, les opérations matérielles nécessaires à la mise en place de la technique mentionnée à l'article L. 851-2 ne peuvent être exécutées, dans leurs réseaux respectifs, que par des agents qualifiés des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications.

9. Enfin, cette technique de renseignement est réalisée sous le contrôle de la commission nationale de contrôle des techniques de renseignement. La composition et l'organisation de cette autorité administrative indépendante sont définies aux articles L. 831-1 à L. 832-5 du code de la sécurité intérieure dans des conditions qui

assurent son indépendance. Ses missions sont définies aux articles L. 833-1 à L. 833-11 du même code dans des conditions qui assurent l'effectivité de son contrôle. Conformément aux dispositions de l'article L. 841-1 du même code, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la commission nationale de contrôle des techniques de renseignement.

10. Il résulte de ce qui précède que le législateur a assorti la procédure de réquisition des données de connexion, lorsqu'elle s'applique à une personne préalablement identifiée susceptible d'être en lien avec une menace, 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.

11. En revanche, en application des dispositions contestées, cette procédure de réquisition s'applique également aux personnes appartenant à l'entourage de la personne concernée par l'autorisation, dont il existe des raisons sérieuses de penser qu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation. Ce faisant, le législateur a permis que fasse l'objet de cette technique de renseignement un nombre élevé de personnes, sans que leur lien avec la menace soit nécessairement étroit. Ainsi, faute d'avoir prévu que le nombre d'autorisations simultanément en vigueur doive être limité, le législateur n'a pas opéré une conciliation équilibrée entre, d'une part, la prévention des atteintes à l'ordre public et des infractions et, d'autre part, le droit au respect de la vie privée.

12. Par suite, la seconde phrase du paragraphe I de l'article L. 851-2 du code de la sécurité intérieure doit être déclarée contraire à la Constitution. La première phrase du même paragraphe, qui ne méconnaît ni le droit au respect de la vie privée, ni aucun autre droit ou liberté que la Constitution garantit, doit être déclarée conforme à la Constitution.

Sur les effets de la déclaration d'inconstitutionnalité :

13. Selon le deuxième alinéa de l'article 62 de la Constitution : « *Une disposition déclarée inconstitutionnelle sur le fondement de l'article 61-1 est abrogée à compter de la publication de la décision du Conseil constitutionnel ou d'une date ultérieure fixée par cette décision. Le Conseil constitutionnel détermine les conditions et limites dans lesquelles les effets que la disposition a produits sont susceptibles d'être remis en cause* ». En principe, la déclaration d'inconstitutionnalité doit bénéficier à l'auteur de la question prioritaire de constitutionnalité et la disposition déclarée contraire à la Constitution ne peut être appliquée dans les instances en cours à la date de la publication de la décision du Conseil constitutionnel. Cependant, les dispositions de l'article 62 de la Constitution réservent à ce dernier le pouvoir tant de fixer la date de l'abrogation et de reporter dans le temps ses effets que de prévoir la remise en cause des effets que la disposition a produits avant l'intervention de cette déclaration.

14. L'abrogation immédiate de la seconde phrase du paragraphe I de l'article L. 851-2 du code de la sécurité intérieure entraînerait des conséquences manifestement excessives. Par suite, il y a lieu de reporter au 1er novembre 2017 la date de cette abrogation.

LE CONSEIL CONSTITUTIONNEL DÉCIDE :

Article 1er. - La seconde phrase du paragraphe I de l'article L. 851-2 du code de la sécurité intérieure dans sa rédaction résultant de la 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 est contraire à la Constitution.

Article 2. - La déclaration d'inconstitutionnalité de l'article 1er prend effet dans les conditions fixées au paragraphe 14 de cette décision.

Article 3. - La première phrase du paragraphe I de l'article L. 851-2 du code de la sécurité intérieure dans sa rédaction résultant de la 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 est conforme à la Constitution.

Article 4. - Cette décision sera publiée au Journal officiel de la République française et notifiée dans les conditions prévues à l'article 23-11 de l'ordonnance du 7 novembre 1958 susvisée.

Jugé par le Conseil constitutionnel dans sa séance du 3 août 2017, où siégeaient : M. Laurent FABIUS, Président, M^me^ Claire BAZY MALAURIE, MM. Michel CHARASSE, Jean-Jacques HYEST, Lionel JOSPIN, M^mes^ Corinne LUQUIENS, Nicole MAESTRACCI et M. Michel PINAULT.

Annexe n° 7

Décision du Conseil d'État statuant au contentieux

N° 408495

Inédit au recueil Lebon

Formation spécialisée

M^me^ Emmanuelle Prada Bordenave, rapporteur

M^me^ Emmanuelle Cortot-Boucher, rapporteur public

OCCHIPINTI, avocats

Lecture du lundi 6 novembre 2017

AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête et un mémoire complémentaire, enregistrés au secrétariat du contentieux du Conseil d'État les 28 février et 28 mai 2017, M. B... A... demande au Conseil d'État :

1°) d'annuler la décision par laquelle le Premier ministre a refusé de lui indiquer si des techniques de renseignement ont été mises en œuvre à son égard ;

2°) subsidiairement, de vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard.

Vu les autres pièces du dossier ;

Vu :

- la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;
- le code de la sécurité intérieure ;
- le code de justice administrative ;

Après avoir convoqué à une séance à huis-clos, d'une part, M. B... A..., et d'autre part, le Premier ministre et la Commission nationale de contrôle des techniques de renseignement, qui ont été mis à même de prendre la parole avant les conclusions ;

Et après avoir entendu en séance :

- le rapport de M^me^ Emmanuelle Prada Bordenave, conseillère d'État,
- et, hors la présence des parties, les conclusions de M^me^ Emmanuelle Cortot-Boucher, rapporteur public ;

Considérant ce qui suit :

1. Aux termes du premier alinéa de l'article L. 821-1 du code de la sécurité intérieure, issu de la loi 24 juillet 2015 relative au renseignement : « *La mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées au titre V du présent livre est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement* ». Aux termes de l'article L. 833-1 du même code : « *La Commission nationale de contrôle des techniques de renseignement veille à ce que les techniques de recueil de renseignement soient mises en œuvre sur le territoire national conformément au présent livre* ». L'article L. 833-4 du même code précise que : « *De sa propre initiative ou lorsqu'elle est saisie d'une réclamation de toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard, la commission procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect du présent livre. Elle*

notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer leur mise en œuvre ».

2. L'article L. 841-1 du code de la sécurité intérieure dispose que : « *Sous réserve des dispositions particulières prévues à l'article L. 854-9 du présent code, le Conseil d'État est compétent pour connaître, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, des requêtes concernant la mise en œuvre des techniques de renseignement mentionnées au titre V du présent livre./ Il peut être saisi par : / 1° Toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue à l'article L. 833-4 ; / 2° La Commission nationale de contrôle des techniques de renseignement, dans les conditions prévues à l'article L. 833-8. / Lorsqu'une juridiction administrative ou une autorité judiciaire est saisie 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, elle peut, d'office ou sur demande de l'une des parties, saisir le Conseil d'État à titre préjudiciel. Il statue dans le délai d'un mois à compter de sa saisine* ». Ces dispositions s'appliquent aux techniques de renseignement mises en œuvre à compter de la date de leur entrée en vigueur, soit le 3 octobre 2015, y compris celles qui, initiées avant cette date, ont continué à être mises en œuvre après.

3. L'article L. 773-6 du code de justice administrative, issu de la même loi, dispose que : « *Lorsque la formation de jugement constate l'absence d'illégalité dans la mise en œuvre d'une technique de recueil de renseignement, la décision indique au requérant ou à la juridiction de renvoi qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une technique* ». *Aux termes de l'article L. 773-7 de ce code :* « *Lorsque la formation de jugement constate qu'une technique de recueil de renseignement est ou a été mise en œuvre illégalement ou qu'un renseignement a été conservé illégalement, elle peut annuler l'autorisation et*

ordonner la destruction des renseignements irrégulièrement collectés./ Sans faire état d'aucun élément protégé par le secret de la défense nationale, elle informe la personne concernée ou la juridiction de renvoi qu'une illégalité a été commise. Saisie de conclusions en ce sens lors d'une requête concernant la mise en œuvre d'une technique de renseignement ou ultérieurement, elle peut condamner l'État à indemniser le préjudice subi (...) ». *L'article R. 773-20 du même code précise que :* « *Le défendeur indique au Conseil d'État, au moment du dépôt de ses mémoires et pièces, les passages de ses productions et, le cas échéant, de celles de la Commission nationale de contrôle des techniques de renseignement, qui sont protégés par le secret de la défense nationale. / Les mémoires et les pièces jointes produits par le défendeur et, le cas échéant, par la Commission nationale de contrôle des techniques de renseignement sont communiqués au requérant, à l'exception des passages des mémoires et des pièces qui, soit comportent des informations protégées par le secret de la défense nationale, soit confirment ou infirment la mise en œuvre d'une technique de renseignement à l'égard du requérant, soit divulguent des éléments contenus dans le traitement de données, soit révèlent que le requérant figure ou ne figure pas dans le traitement. / Lorsqu'une intervention est formée, le président de la formation spécialisée ordonne, s'il y a lieu, que le mémoire soit communiqué aux parties, et à la Commission nationale de contrôle des techniques de renseignement, dans les mêmes conditions et sous les mêmes réserves que celles mentionnées à l'alinéa précédent* ».

4. Il ressort des pièces du dossier que M. A... a saisi la Commission nationale de contrôle des techniques de renseignement (CNCTR) le 21 septembre 2016 afin de vérifier qu'aucune technique de renseignement n'était irrégulièrement mise en œuvre à son égard. Par lettre du 29 décembre 2016, le président de la commission a informé M. A... qu'il avait été procédé à l'ensemble des vérifications requises et que la procédure était terminée, sans apporter à l'intéressé d'autres informations. M. A... demande au Conseil d'État d'annuler le refus du Premier ministre de lui indiquer si des mesures

de surveillance ont été exercées à son égard, révélé par ce courrier, ou, subsidiairement de vérifier si des techniques de renseignement ont été mises en œuvre pour le surveiller et, le cas échéant, de constater qu'elles l'ont été illégalement.

5. Il appartient à la formation spécialisée, créée par l'article L. 773-2 du code de justice administrative, saisie de conclusions relatives à la mise en œuvre de technique de renseignement, de vérifier, au vu des éléments qui lui sont été communiqués hors la procédure contradictoire, si le requérant fait ou non l'objet d'une telle technique. Lorsqu'il apparaît soit qu'aucune technique de renseignement n'est mise en œuvre à l'égard du requérant, soit que cette mise en œuvre n'est entachée d'aucune illégalité, la formation de jugement informe le requérant de l'accomplissement de ces vérifications, sans indiquer si une technique de recueil de renseignement a été mise en œuvre à son égard. Dans le cas où une technique de renseignement est mise en œuvre dans des conditions entachées d'illégalité, elle en informe le requérant, sans faire état d'aucun élément protégé par le secret de la défense nationale. Elle peut, par ailleurs, annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés.

6. La lettre que le président de la CNCTR a adressée au requérant en réponse au recours préalable obligatoire qu'il a formé en application de l'article L. 833-4 du code de la sécurité intérieure ne révèle, contrairement à ce qu'il soutient, aucun refus du Premier ministre de lui indiquer si des mesures de surveillance ont été mise en œuvre à son égard. Ses conclusions dirigées contre un prétendu refus du Premier ministre ne peuvent donc qu'être écartées.

7. La formation spécialisée a, en revanche, examiné, selon les modalités décrites au point 5 qui garantissent le respect de l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, les éléments fournis par la Commission nationale de contrôle des techniques de renseignement, qui a précisé l'ensemble des vérifications auxquelles elle avait procédé, et par le Premier ministre. À l'issue de cet examen, qui a permis au Conseil d'État de s'assurer notamment de

l'absence de violation par l'administration des exigences de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, il y a lieu de répondre à M. A... que la vérification qu'il a sollicitée a été effectuée et n'appelle aucune mesure de la part du Conseil d'État.

D E C I D E :

Article 1er : Il a été procédé à la vérification demandée par M. A....

Article 2 : Les conclusions de M. A... dirigées contre le refus que lui aurait opposé le Premier ministre de lui indiquer si des techniques de renseignement ont été mises en œuvre à son égard sont rejetées.

Article 3 : La présente décision sera notifiée à M. B... A..., au Premier ministre et à la Commission nationale de contrôle des techniques de renseignement.

Annexe n° 8

Les modifications législatives du livre VIII du code de la sécurité intérieure

Le tableau ci-dessous dresse la liste des modifications de nature législative intervenues au livre VIII du code de la sécurité intérieure depuis l'entrée en vigueur de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement et de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
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 Voir les articles 14 et 119 de la loi (entrée en vigueur le 5 juin 2016)	Article L. 811-4 Article L. 821-2	Intégration des services chargés du renseignement pénitentiaire dans le « second cercle » des services de renseignement	Décret n° 2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la justice, 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	Délibération de la CNCTR n° 3/2016 du 8 décembre 2016 Voir l'annexe n° 1 au présent rapport
	Article L. 895-1 *Article L. 896-1* *Article L. 897-1* *Article L. 898-1*	*Application outre-mer*		

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
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 Voir les articles 15, 17 et 21 de la loi (entrée en vigueur le 22 juillet 2016)	Article L. 851-2	1. Recueil de données de connexion en temps réel pour la seule prévention du terrorisme : • Extension de la durée maximale d'autorisation à quatre mois • Extension du champ d'application aux personnes « *préalablement identifiée[s] susceptible[s] d'être en lien avec une menace* » et aux personnes appartenant à l'entourage de celles-ci lorsqu'elles sont « *susceptibles de fournir des informations au titre de la finalité* » de prévention du terrorisme		

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
	Article L. 852-1	2. Clarification de la nature des données de connexion pouvant être recueillies sur le fondement d'une autorisation d'interception de sécurité : les données « *associé[e]s à l'exécution de l'interception et à son exploitation* »		
	Article L. 863-2	3. Autorisation pour les services de renseignement de « *partager* » et non plus seulement « *échanger* » les informations utiles à l'accomplissement de leurs missions		
	Article L. 895-1 *Article L. 896-1* *Article L. 897-1* *Article L. 898-1*	*Application outre-mer*		

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
Loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes Voir les articles 36 et 39 de la loi (entrée en vigueur le 22 janvier 2017)	Article L. 831-1 Article L. 832-1 Article L. 832-2 Article L. 832-3 Article L. 832-4 Article L. 833-9 Article L. 861-3	Adaptation des dispositions relatives à la composition et au fonctionnement de la CNCTR au nouveau statut général des autorités administratives indépendantes		Délibération de la CNCTR n° 2/2017 du 23 mars 2017 Voir l'annexe n° 3 au présent rapport

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique Voir les articles 35 et 40 de la loi (entrée en vigueur le 2 mars 2017)	Article L. 855-1	Définition de finalités propres au service chargé du renseignement pénitentiaire, distinctes de celles énumérées à l'article L. 811-3 : possibilité d'autoriser la mise en œuvre de techniques de renseignement « *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* »	Décrets n° 2017-749 du 3 mai 2017 relatif à la désignation des services relevant du ministère de la justice pris en application de l'article L. 855-1 du code de la sécurité intérieure	Délibération de la CNCTR n° 1/2017 du 16 mars 2017 Voir l'annexe n° 2 au présent rapport
	Article L. 895-1 *Article L. 896-1* *Article L. 897-1* *Article L. 898-1*	*Application outre-mer*		

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme Voir les articles 15, 17, 18 et 20 de la loi (entrée en vigueur le 31 octobre 2017)	Article L. 821-1 Article L. 821-4 Article L. 821-7 Article L. 822-2 Article L. 852-2 Article L. 855-1 A Article L. 855-1 B Article L. 855-1 C (Articles L. 2371-1 et L. 2371-2 du code de la défense)	1. Surveillance des transmissions empruntant exclusivement la voie hertzienne (conséquences de l'abrogation de l'article L. 811-5 par la décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016) : • Création d'une nouvelle technique de renseignement (article L. 852-2), soumise au droit commun, pour intercepter les communications des réseaux privatifs • Réduction à un champ d'application marginal de l'« exception hertzienne » (articles L. 855-1 A à L. 855-1 C)		Délibération de la CNCTR n° 4/2017 du 9 juin 2017. Voir l'annexe n° 5 au présent rapport.

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
	Article L. 851-2	2. Recueil de données de connexion en temps réel (conséquences de l'abrogation partielle de l'article L. 851-2 par la décision du Conseil constitutionnel n° 2017-648 QPC du 4 août 2017) : instauration d'un contingent des autorisations de recueil simultanément en vigueur		
	Article L. 853-2	3. Élargissement du type d'équipements périphériques sur lesquels peut porter la captation de données informatiques, afin d'inclure notamment les transmissions par protocole « *wifi* »		

Loi	Dispositions créées ou modifiées	Objet	Décret d'application	Délibération de la CNCTR
	Article L. 871-2	4. Suppression d'un pouvoir résiduel de réquisition de données de connexion par le Premier ministre, le ministre de l'intérieur ou le ministre de la défense auprès des opérateurs de communications électroniques		
	Article L. 895-1 *Article L. 896-1* *Article L. 897-1* *Article L. 898-1*	*Application outre-mer*		