Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CNCTR

3e Rapport d'activité 2018

Commission nationale de contrôle des techniques de renseignement

SOMMAIRE

ANNEXES 119

Avant-propos

Les deux précédents rapports d'activité de la Commission nationale de contrôle des techniques de renseignement (CNCTR) ont décrit le cadre juridique créé par la loi du 24 juillet 2015 relative au renseignement et celle du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales. Ils ont aussi rendu compte des évolutions de ce cadre, intervenues à plusieurs reprises depuis 2015.

Une nouvelle modification, touchant la surveillance des communications électroniques internationales et l'articulation entre celle-ci et les mesures de surveillance intérieure, a été adoptée par le Parlement en 2018. Elle confie désormais à la CNCTR un pouvoir de contrôle *a priori* sur les demandes d'exploitation des informations recueillies par les moyens de surveillance des communications électroniques internationales. Le troisième rapport d'activité de la commission, qui couvre l'année 2018, rend compte de cette évolution, techniquement complexe, d'une manière qu'il s'efforce de rendre accessible au plus grand nombre.

Pour la première fois, le rapport de la CNCTR va au-delà du constat des modifications réalisées et formule des réflexions et des recommandations pour améliorer le cadre légal.

Cette initiative s'appuie sur l'expérience des trois années de fonctionnement de la commission. Elle s'inscrit dans la perspective de l'examen par le Parlement, en 2020, de certaines dispositions de la loi du 24 juillet 2015 relatives à la lutte contre le terrorisme qui doivent, selon cette loi, faire l'objet d'une évaluation par le Parlement.

Le rapport évoque la possibilité, pour des personnes qui estiment faire indûment l'objet d'une surveillance de leurs communications électroniques internationales, de saisir le juge, en l'occurrence le Conseil d'État, d'un recours. Cette possibilité existe déjà pour les techniques de renseignement prévues par la loi du 24 juillet 2015. Elle n'a initialement pas été instituée pour les mesures de surveillance prévues par la loi du 30 novembre 2015. Le législateur a cependant, par la modification de cette loi intervenue en 2018,

ouvert un droit au recours contre une des mesures de surveillance internationale. La commission estime souhaitable d'aller plus loin en alignant l'accès au recours en matière de surveillance des communications électroniques internationales sur celui prévu pour les techniques de renseignement relevant de la surveillance intérieure.

La commission suggère également des modifications plus techniques, susceptibles d'améliorer la cohérence du cadre légal et l'utilisation optimale de ses capacités de contrôle.

Elle s'interroge enfin sur la question des échanges de données entre services de renseignement français et étrangers. La loi n'a pas prévu d'encadrement juridique en ce domaine ; elle fait interdiction à la CNCTR d'avoir accès aux données communiquées par des services étrangers. La commission n'ignore pas l'importance de ces échanges pour l'efficacité de nos services de renseignement. Elle estime cependant qu'à l'instar de ce qui existe dans d'autres pays, notamment en Europe, un encadrement juridique est souhaitable.

Comme dans les précédents rapports, le lecteur trouvera des indications chiffrées sur l'activité de contrôle de la CNCTR. Elles s'étendent cette année au contrôle de la surveillance des communications électroniques internationales puisque la commission est, depuis 2018, légalement chargée d'exercer un contrôle *a priori* en ce domaine. Elles font apparaître une croissance de l'ordre de 4 % des demandes de techniques de renseignement et une évolution contrastée du recours aux différentes techniques. La prévention du terrorisme demeure le principal motif de recours à des mesures de surveillance par les services de renseignement, suivi de la prévention de la criminalité organisée et de la prévention de l'ingérence étrangère. La part des demandes invoquant la prévention des violences collectives de nature à porter gravement atteinte à la paix publique est en progression, son poids relatif passant de 6 à 9 %.

La CNCTR continue à calculer et à publier le nombre de personnes surveillées. Il était de 22 308 en 2018, soit une progression de 3 % par rapport à 2017.

Le taux d'avis défavorables de la CNCTR en 2018 s'établit à 2,1 %, en recul par rapport à 2017. Cette évolution témoigne de la qualité du dialogue mené entre la commission et les services de renseignement, qui conduit ceux-ci à mieux se conformer à la doctrine de la commission en renonçant notamment à présenter des demandes vouées à la désapprobation de celle-ci.

L'activité de contrôle *a posteriori* de la commission s'est maintenue à un rythme soutenu de deux à trois contrôles sur pièces et sur place par semaine. Grâce aux progrès réalisés en matière de centralisation des renseignements recueillis et de traçabilité des exploitations de données, la CNCTR est en mesure de réaliser son contrôle *a posteriori* depuis ses locaux sur un plus grand nombre de techniques mises en œuvre. S'ils progressent, le chantier de la centralisation et celui de la traçabilité demeurent inachevés. La CNCTR suit attentivement leur avancement dans les services et au sein du groupement interministériel de contrôle (GIC).

En 2018, la CNCTR a fait usage, pour la première fois, de son pouvoir de recommander à un service l'interruption d'une technique de renseignement ainsi que la destruction immédiate des renseignements collectés, en vertu de l'article L. 833-6 du code de la sécurité intérieure. Cette recommandation, justifiée par la découverte d'une irrégularité à l'occasion d'un contrôle *a posteriori* sur pièces et sur place, a été immédiatement mise en œuvre par le service concerné.

La commission a pris en 2018 l'initiative de deux événements destinés à ouvrir le débat sur le renseignement et son contrôle. Un colloque international s'est tenu en avril 2018 au Conseil d'État. Une conférence internationale des organes contrôlant la légalité des activités de renseignement en Europe s'est réunie à Paris en décembre 2018. Elle a permis aux participants de mieux connaître les dispositifs de contrôle, d'une grande variété, en place dans certains pays européens et de s'entendre sur le partage de bonnes pratiques. La conférence de Paris sera prolongée par une nouvelle réunion prévue aux Pays-Bas en décembre 2019.

Le lecteur trouvera enfin dans le rapport une étude portant sur les principaux éléments de jurisprudence européenne relatifs au droit au respect de la vie privée en matière de renseignement.

J'espère que ce troisième rapport d'activité de la CNCTR contribuera à une meilleure information du public sur le droit du renseignement et sur la façon dont les activités des services de renseignement sont contrôlées.

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 mettre en œuvre une technique ou, s'agissant de la surveillance des communications électroniques internationales, sur toutes les demandes tendant à exploiter des communications interceptées. La CNCTR vérifie également *a posteriori* que les prescriptions légales ont été respectées, en contrôlant l'exécution des autorisations accordées et en vérifiant qu'aucun recueil ou qu'aucune exploitation soumis à autorisation n'ont été irrégulièrement mis en œuvre. 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.

En matière de surveillance intérieure, c'est-à-dire visant le territoire national, 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 service 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 (article L. 853-3 du code de la sécurité intérieure), qui ne constitue pas à proprement parler une technique de renseignement mais 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.

En matière de surveillance des communications électroniques internationales, l'interception de ces communications ainsi que différentes mesures d'exploitation portant sur des communications entières ou des seules données de connexion peuvent être autorisées (articles L. 854-1 et suivants 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 que la commission 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 rapport 2017 et à celle du présent rapport.

Une modification de la composition de la CNCTR

Le collège de la CNCTR a connu deux renouvellements en 2018.

Le 29 mars 2018, madame Catherine DI FOLCO, sénatrice du Rhône, a été désignée par le Sénat comme membre de la CNCTR, en remplacement de madame Catherine TROENDLÉ, qui avait démissionné.

Le 3 octobre 2018, madame Martine JODEAU, conseillère d'État honoraire, et monsieur Gérard POIROTTE, conseiller honoraire à la Cour de cassation, ont été nommés membres de la CNCTR, la première par le vice-président du Conseil d'État et le second conjointement par le premier président de la Cour de cassation et le procureur général près la cour. Ils ont remplacé respectivement madame Jacqueline DE GUILLENCHMIDT et monsieur Franck TERRIER, dont les mandats avaient pris fin le 2 octobre 2018.

À la fin de l'année 2018, le collège de la CNCTR était composé des neufs membres suivants :

- monsieur Francis DELON, conseiller d'État honoraire, président ;
- madame Catherine DI FOLCO, sénatrice du Rhône ;
- monsieur Michel BOUTANT, sénateur de la Charente ;
- madame Constance LE GRIP, députée des Hauts-de-Seine ;
- monsieur Jean-Michel CLÉMENT, député de la Vienne ;
- madame Martine JODEAU, conseillère d'État honoraire ;
- madame Christine PÉNICHON, avocate générale près la Cour de cassation ;
- monsieur Gérard POIROTTE, conseiller honoraire à la Cour de cassation ;
- monsieur Patrick PUGES, personnalité qualifiée en matière de communications électroniques.

Le secrétariat général de la CNCTR se composait, à la même date, d'un secrétaire général, d'un conseiller placé auprès du président de la commission, de onze chargés de mission et de quatre agents exerçant des missions de soutien.

Compte-rendu de l'activité de la CNCTR

1. Les modifications du cadre juridique en 2018 et ses perspectives d'évolution à moyen terme : la CNCTR entre vigilance exigeante et force de proposition dans le cadre de sa mission de conseil auprès du Gouvernement et du Parlement

Les dispositions législatives applicables aux techniques de renseignement, codifiées au livre VIII du code de la sécurité intérieure, ont connu en 2018 leur sixième modification depuis leur entrée en vigueur en 2015.

Les modifications intervenues en 2016 et en 2017, analysées dans les précédents rapports d'activité de la CNCTR[3], avaient concerné les techniques de renseignement relevant de la surveillance intérieure, destinées à surveiller des personnes situées sur le territoire national[4]. Ces modifications avaient consisté notamment à :

- **permettre au service du ministère de la justice chargé du renseignement pénitentiaire de solliciter la mise en œuvre de certaines techniques de renseignement pour prévenir le terrorisme, prévenir la criminalité et la délinquance organisées ou, finalité propre à ce service, prévenir les évasions et assurer la sécurité et le bon ordre au sein des établissements pénitentiaires ;**
- **étendre à l'entourage des personnes surveillées à titre principal et, en contrepartie, contingenter le champ d'application du recueil de données de connexion en**

3 - Voir notamment les points 2.1.3 et 2.1.4.1 du premier rapport d'activité 2015/2016 de la CNCTR ainsi que les points 1.2, 1.4 et 1.6 du deuxième rapport d'activité 2017 de la CNCTR.

4 - Ces techniques sont celles prévues au titre V du livre VIII du code de la sécurité intérieure, sauf les mesures de surveillance des communications électroniques internationales ainsi que les mesures de surveillance de certaines communications hertziennes, dites « exception hertzienne ».

temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure ;

- intégrer dans le droit commun des techniques de renseignement l'essentiel des mesures de surveillance des communications empruntant la voie hertzienne ;
- prolonger jusqu'au 31 décembre 2020 la période expérimentale durant laquelle peuvent être mis en œuvre, en application de l'article L. 851-3 du code de la sécurité intérieure, des algorithmes sur des données de connexion à la seule fin de détecter des menaces terroristes.

En 2018, les dispositions relatives aux mesures de surveillance des communications électroniques internationales ont été modifiées pour la première fois pour améliorer l'articulation de ces mesures avec les techniques de surveillance intérieure. Les dispositifs de contrôle ont été renforcés en conséquence. Ainsi la consultation *a priori* de la CNCTR sur toutes les demandes d'exploitation de communications internationales interceptées est désormais rendue obligatoire par la loi.

Des évolutions de niveau réglementaire ont également eu lieu en 2018. Elles ont essentiellement concerné les services de renseignement dits du « second cercle ». L'une a intégré un nouveau service au sein de ce « second cercle ». Une autre a consisté à désigner les services pouvant être autorisés à recourir à une nouvelle technique de renseignement créée en 2017, l'interception de communications échangées au sein d'un réseau privatif empruntant exclusivement la voie hertzienne.

1.1 Les modifications du cadre juridique en 2018 : des évolutions maintenant l'équilibre entre la prise en compte des besoins opérationnels des services de renseignement et la nécessité d'un encadrement rigoureux

1.1.1 En matière de surveillance intérieure, deux adaptations du périmètre et des prérogatives des services de renseignement du « second cercle » en accord avec la doctrine de la CNCTR

1.1.1.1 L'intégration de la nouvelle sous-direction de la lutte contre l'immigration irrégulière de la préfecture de police de Paris parmi les services de renseignement du « second cercle »

Pour lutter contre des flux d'immigration irrégulière de grande ampleur et renforcer la coordination entre les services de police chargés de cette lutte à Paris et dans les départements des Hauts-de-Seine, de la Seine-Saint-Denis et du Val-de-Marne, une sous-direction de lutte contre l'immigration irrégulière (SDLII) a été créée à la préfecture de police de Paris par un arrêté du 15 mai 2017[5]. Cette sous-direction, née du rapprochement de différentes unités précédemment rattachées à plusieurs directions, comprend un département de lutte contre la criminalité organisée, qui a pour mission le démantèlement de filières d'acheminement illégal, de traite d'êtres humains et d'aide au maintien irrégulier sur le territoire national. Si ce département diligente essentiellement des enquêtes judiciaires, il peut exercer sa mission à titre préventif, dans un cadre de police administrative. Il est alors susceptible de rechercher du renseignement intéressant sa mission, ce qui peut justifier la mise en œuvre de techniques de renseignement.

5 - Voir l'arrêté n° 2017/559 du 15 mai 2017 relatif aux missions et à l'organisation de la direction de la sécurité de proximité de l'agglomération parisienne.

Pour que le département de la criminalité organisée de la SDLII puisse utiliser des techniques de renseignement, une mesure réglementaire était nécessaire, en application de l'article L. 811-4 du code de la sécurité intérieure, qui prévoit que les services de renseignement du « second cercle », qui peuvent être autorisés à recourir à de telles techniques, sont désignés par décret en Conseil d'État pris après avis de la CNCTR.

Le 8 novembre 2017, le ministre de l'intérieur a saisi la CNCTR pour avis d'un projet de décret désignant le département de la criminalité organisée de la SDLII comme service de renseignement du « second cercle » et prévoyant les techniques de renseignement auxquelles ce service pourrait demander à recourir ainsi que la finalité légale qu'il pourrait invoquer.

Dans une délibération adoptée en formation plénière le 7 décembre 2017[6], la CNCTR a rendu son avis sur le projet de décret.

Après avoir étudié les missions, l'organisation, les besoins opérationnels et les moyens techniques du département de la criminalité organisée de la SDLII, la CNCTR n'a pas émis d'objection à son intégration dans le « second cercle » des services de renseignement et a considéré que la prévention de la criminalité et de la délinquance organisée, prévue au 6° de l'article L. 811-3 du code de la sécurité intérieure, était la finalité légale adaptée à son action.

S'agissant des techniques de renseignement auxquelles le département de la criminalité organisée de la SDLII pourrait être autorisé à recourir, la CNCTR a émis un avis partiellement favorable, en s'appuyant sur sa doctrine énoncée dans toutes ses délibérations relatives aux services du « second cercle »[7]. Selon cette doctrine, la nature et le nombre de techniques auxquelles peuvent avoir accès les services du « second cercle » doit dépendre de la part qu'occupe le renseignement au sein de leurs missions ainsi que de l'expertise technique nécessaire pour mettre en œuvre les techniques de manière sûre.

6 - Voir la délibération de la CNCTR n° 5/2017 du 7 décembre 2007, publiée en annexe n° 1 au présent rapport et sur le site internet de la commission.

7 - Voir, pour la première formulation de cette doctrine, la délibération de la CNCTR n° 2/2015 du 12 novembre 2015, publiée sur le site internet de la commission.

La CNCTR a tout d'abord émis un avis favorable à ce que le département de lutte contre la criminalité organisée de la SDLII puisse être autorisé à recourir aux techniques de renseignement suivantes :

- l'accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) ;
- la géolocalisation en temps réel (article L. 851-4 du même code) ;
- le balisage (article L. 851-5 du même code) ;
- l'interception de sécurité réalisée *via* le GIC (I de l'article L. 852-1 du même code) ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé (article L. 853-1 du même code).

La CNCTR s'est également prononcée en faveur de la possibilité pour le service d'être spécialement autorisé à s'introduire dans un lieu privé (article L. 853-3 du code de la sécurité intérieure) pour y mettre en place, utiliser ou retirer une balise ou un dispositif de captation de paroles ou d'images. Le projet de décret n'incluait pas les lieux à usage d'habitation parmi les lieux privés dans lesquels le service pourrait être autorisé à s'introduire.

La CNCTR s'est ensuite écartée du projet du Gouvernement sur deux points :

- après avoir constaté que la SDLII n'avait ni les compétences techniques ni même le besoin opérationnel de recueillir des données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure), la CNCTR s'est montrée défavorable à ce que le département de lutte contre la criminalité organisée de la SDLII puisse avoir recours à cette technique de renseignement ;
- s'agissant du recueil et de la captation de données informatiques (article L. 853-2 du code de la sécurité intérieure), la CNCTR a d'abord rappelé qu'elle avait estimé, dans une précédente délibération[8], que le recours, à des fins de renseignement, à ces techniques particulièrement complexes et intrusives, qui peuvent être mises en œuvre dans un cadre judiciaire sur le fondement du

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

code de procédure pénale, n'était pas justifié pour un service[9] de la direction centrale de la police aux frontières exerçant une mission similaire à celle du service concerné par le projet de décret ; constatant de surcroît que la SDLII ne disposait pas de compétences techniques en la matière, la commission a, en conséquence, émis un avis défavorable à ce que le département de lutte contre la criminalité organisée de la SDLII, service de police essentiellement judiciaire, puisse être autorisé à recueillir ou capter des données informatiques dans un cadre administratif.

Dans le décret finalement adopté[10], le Gouvernement a suivi les recommandations de la CNCTR et limité l'accès du département de lutte contre la criminalité organisée de la SDLII aux techniques de renseignement qui avaient fait l'objet d'un avis favorable de la commission.

9 - Il s'agissait en l'espèce de l'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre (OCRIEST).

10 - Voir le décret n° 2018-543 du 29 juin 2018 relatif à la désignation de certains services 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, notamment son article 1er.

1.1.1.2 La désignation des services du « second cercle » pouvant être autorisés à recourir à l'interception de sécurité hertzienne

Créé en 2017, lors de la redéfinition par le législateur des mesures de surveillance des communications empruntant la voie hertzienne[11], l'article L. 852-2 du code de la sécurité intérieure a ajouté une technique de renseignement au cadre légal entré en vigueur en 2015. Sur le fondement de cet article, « *peuvent être autorisées les interceptions de correspondances 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, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs* ».

La technique constitue un nouveau type d'interception de sécurité, c'est-à-dire d'interception de communications incluant aussi bien le contenu de celles-ci que les données de connexion qui leur sont associées. Les communications concernées sont celles échangées sur des réseaux exclusivement hertziens, conçus pour une utilisation privative. L'interception ne peut être mise en œuvre sans autorisation du Premier ministre prise après avis de la CNCTR.

Comme pour la plupart des autres techniques, les services spécialisés de renseignement, dits du « premier cercle », tiennent de la loi elle-même la faculté de solliciter l'autorisation de mettre en œuvre l'interception de sécurité hertzienne pour l'exercice de leurs missions respectives et la poursuite des finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure. Pour être autorisés à mettre en œuvre la technique, les services du « second cercle » doivent, quant à eux, être désignés, en application de l'article L. 811-4 du même code, par un décret en Conseil d'État pris après avis de la CNCTR. Ce décret détermine également celles des finalités légales que les services du « second cercle » peuvent invoquer à l'appui de leurs demandes.

---

11 - Cette redéfinition était commandée par la déclaration d'inconstitutionnalité contenue dans la décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016. Les mesures de surveillance des communications empruntant la voie hertzienne ont été rénovées par les articles 15 et 18 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Pour une présentation détaillée des différentes étapes de la réforme, voir le point 2.1.6 du premier rapport d'activité 2015-2016 de la CNCTR et le point 1.2 du deuxième rapport d'activité 2017 de la CNCTR.

Le 19 avril 2018, le ministre de l'intérieur a saisi la CNCTR d'un projet de décret désignant les services du « second cercle » qui pourraient être autorisés à recourir à l'interception de sécurité hertzienne ainsi que les finalités sur lesquelles ces services pourraient fonder leurs demandes.

Dans une délibération adoptée en formation plénière le 17 mai 2018[12], la CNCTR a rendu son avis sur le projet de décret.

La commission a tout d'abord examiné, de manière générale, les finalités invocables. Elle a émis un avis favorable, eu égard aux usages susceptibles d'être faits des réseaux de communication hertziens privatifs, à ce que les services du « second cercle » puissent invoquer, en fonction de leurs missions respectives, la défense et la promotion des intérêts fondamentaux de la Nation mentionnés aux 1°, 4°, 5° et 6° de l'article L. 811-3 du code de la sécurité intérieure, à savoir :

- l'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- 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, 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 CNCTR s'est ensuite prononcée sur les services du « second cercle » susceptibles d'être autorisés à mettre en œuvre la technique. Elle a, à cet égard, constaté que la nouvelle interception de sécurité visait des correspondances échangées au sein de réseaux et au moyen de matériels spécifiques et que leur mise en œuvre nécessitait l'acquisition de dispositifs lourds et onéreux dont l'usage supposait des compétences techniques

12 - Voir la délibération de la CNCTR n° 2/2018 du 17 mai 2018, publiée en annexe n° 3 au présent rapport et sur le site internet de la commission.

particulières. Elle a également relevé que le traitement des données recueillies se heurtait à des contraintes techniques. La CNCTR a en conséquence estimé que la mise en œuvre de l'interception de sécurité hertzienne devait être réservée aux services du « second cercle » attestant un besoin réel et disposant de capacités opérationnelles adaptées.

La CNCTR s'est ainsi déclarée favorable à la désignation des services suivants, en tenant compte de l'étendue de leurs compétences en matière de renseignement, de leurs besoins opérationnels particuliers ou des enjeux de sécurité nationale s'attachant à leurs missions :

- à la direction générale de la police nationale :
  - au sein de la direction centrale de la police judiciaire : la sous-direction de la lutte contre la criminalité organisée et la délinquance financière, la sous-direction antiterroriste et la sous-direction de la lutte contre la cybercriminalité ;
  - au sein de la direction centrale de la sécurité publique : l'unité nationale de recherche et d'appui du service central du renseignement territorial ;
- à la direction générale de la gendarmerie nationale, au sein de la direction des opérations et de l'emploi : la sous-direction de l'anticipation opérationnelle et la sous-direction de la police judiciaire ;
- à la préfecture de police de Paris, au sein de la direction du renseignement : la sous-direction de la sécurité intérieure et la sous-direction du renseignement territorial ;
- parmi les services placés sous l'autorité d'emploi du ministère de la défense : les sections de recherches de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement ;
- à la direction de l'administration pénitentiaire : le bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire.

La CNCTR a en revanche émis un avis défavorable à la désignation des services suivants, en se fondant sur la nature de leurs missions, sur les contraintes techniques, opérationnelles et financières caractérisant l'interception de sécurité hertzienne ainsi que sur le constat du faible nombre de demandes présentées jusqu'alors par ces services pour mettre en œuvre des techniques de renseignement complexes :

- à la direction générale de la police nationale :
  - au sein de la direction centrale de la police judiciaire : le service central des courses et jeux ainsi que les services territoriaux de la police judiciaire ;
  - au sein de la direction centrale de la police aux frontières : l'office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre ;
  - au sein de la direction centrale de la sécurité publique : les échelons territoriaux du service central du renseignement territorial ;
- à la direction générale de la gendarmerie nationale : les sections de recherches.

Dans le décret finalement adopté[13], le Gouvernement a suivi les recommandations de la CNCTR et limité aux services ayant fait l'objet d'un avis favorable de la commission la faculté de solliciter la mise en œuvre de l'interception de sécurité hertzienne.

13 - Voir le décret n° 2018-543 du 29 juin 2018 relatif à la désignation de certains services 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, notamment son article 2.

1.1.2 En matière de surveillance internationale, une modification législative destinée à améliorer l'articulation avec la surveillance intérieure, sous le contrôle renforcé de la CNCTR

Au début de l'année 2018, le Gouvernement a estimé nécessaire de proposer au législateur une modification des dispositions légales régissant les mesures de surveillance des communications électroniques internationales[14] pour prendre en compte les besoins opérationnels des services de renseignement. Un amendement en ce sens a été introduit dans le projet de loi relatif à la programmation militaire pour les années 2019 à 2025, alors en cours de discussion au Parlement[15]. Consultée le 4 mai 2018 par le Gouvernement préalablement au dépôt de cet amendement, la CNCTR, réunie en formation plénière le 9 mai suivant, a adopté une délibération[16] constituant son avis sur le projet d'amendement qui lui était soumis.

La modification législative projetée avait pour objet de prévoir les conditions et les limites dans lesquelles les services de renseignement, dans le cadre de la surveillance des communications électroniques internationales, pourraient être autorisés à vérifier ponctuellement et, le cas échéant, à exploiter de manière suivie des données de connexion, voire des correspondances de personnes communiquant au moyen d'identifiants techniques rattachables au territoire national. Un identifiant technique peut être notamment un numéro de téléphone, un numéro de carte à puce dite « *IMSI*[17] », une adresse dite « *IP*[18] » ou une adresse de messagerie électronique. Est considéré comme rattachable au territoire national un identifiant technique qui présente une caractéristique[19] permettant de l'associer à ce territoire ou qui est utilisé par une personne résidant en France.

---

14 - Ces dispositions, créées par la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, sont celles des articles L. 854-1 à L. 854-9 du code de la sécurité intérieure, qui forment le chapitre IV du titre V du livre VIII de ce code.

15 - Voir l'amendement n° 91 au projet de loi, présenté par le Gouvernement en séance publique le 22 mai 2018 lors de la première lecture du texte par le Sénat. Adopté, l'amendement est devenu l'article 22 bis A du projet de loi puis l'article 37 de la loi finalement votée et promulguée.

16 - Voir la délibération de la CNCTR n° 1/2018 du 9 mai 2018, publiée en annexe n° 2 au présent rapport et sur le site internet de la commission.

17 - *International mobile subscriber identity.*

18 - *Internet protocol.*

19 - Il s'agit par exemple, pour un numéro de téléphone, d'un indicatif français ou, pour une adresse *IP*, de sa localisation en France.

Le cadre juridique en vigueur depuis 2015 prohibait la surveillance individuelle des communications électroniques internationales de personnes utilisant des identifiants techniques rattachables au territoire national. Deux exceptions à cette interdiction de principe étaient prévues, sous réserve que la personne communique depuis l'étranger[20].

Le projet de texte soumis à la CNCTR maintenait l'interdiction et ses deux exceptions, tout en complétant le champ des mesures de surveillance internationale pouvant être prises à l'égard des personnes utilisant des identifiants techniques rattachables au territoire national. Trois mesures étaient envisagées :

- des vérifications ponctuelles, ne constituant pas des mesures de surveillance individuelle, pourraient être effectuées dans des conditions et des limites prévues par la loi (IV de l'article L. 854-2 du code de la sécurité intérieure) ;
- une nouvelle mesure de surveillance individuelle, par exception au principe prohibant ce type de surveillance, serait créée et légalement encadrée (V de l'article L. 854-2 du même code) ;
- des autorisations individuelles délivrées sous le régime de la surveillance intérieure pourraient valoir, à condition qu'elles le prévoient, autorisation d'exploiter des communications internationales entrant dans leur champ d'application (quatrième alinéa de l'article L. 854-1 du même code).

La CNCTR n'a pas émis d'objection au principe d'une telle évolution législative. Elle a en effet estimé que, près de deux ans et demi après l'entrée en vigueur des dispositions régissant les mesures de surveillance des communications électroniques internationales, l'expérience avait montré que ce cadre légal comportait des dispositions pouvant paraître inadaptées au regard de la conciliation à effectuer entre la protection de la vie privée et la préservation des intérêts fondamentaux de la Nation.

20 - Voir le troisième alinéa de l'article L. 854-1 du code de la sécurité intérieure, dans sa rédaction issue de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales. En vertu de ces deux exceptions, ne pouvaient être surveillées que les communications de personnes situées à l'étranger et soit faisant l'objet d'une interception de sécurité prévue à l'article L. 852-1 du code de la sécurité intérieure à la date de leur sortie du territoire national, soit identifiées comme présentant une menace pour les intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code.

La CNCTR a ensuite formulé des observations détaillées, comportant des propositions de modification du projet d'amendement ainsi que des réserves d'interprétation.

En premier lieu, s'agissant des vérifications ponctuelles, la CNCTR a considéré que leur réalisation sur des communications de personnes utilisant des identifiants rattachables au territoire national ne serait pas disproportionnée au regard des intérêts fondamentaux de la Nation poursuivis.

Réservées aux services spécialisés de renseignement, dits du « premier cercle », les vérifications ponctuelles prévues par le projet d'amendement étaient conçues comme permettant d'accéder aux données de connexion, voire aux communications de personnes utilisant des identifiants techniques rattachables au territoire national, sans toutefois, du fait de leur caractère limité, constituer des mesures aussi intrusives qu'une surveillance individuelle. Elles pourraient donc être conduites sans méconnaître l'interdiction de principe énoncée par la loi, selon laquelle les mesures de surveillance internationale ne peuvent avoir pour objet la surveillance individuelle des communications de personnes utilisant des identifiants techniques rattachables au territoire national.

En contrepartie, la loi entourait la réalisation des vérifications ponctuelles de conditions destinées, d'une part, à garantir leur caractère limité et, d'autre part, à les soumettre à un contrôle adapté :

- le caractère ponctuel des vérifications supposait une limitation étroite dans le temps de leur réalisation ;
- les vérifications ponctuelles ne pourraient être effectuées que dans le cadre d'une autorisation prévue au III de l'article L. 854-2 du code de la sécurité intérieure en cours de validité ; ce type d'autorisation, délivré par le Premier ministre après avis de la CNCTR, permet d'exploiter des communications internationales émises ou reçues dans une zone géographique, par une organisation, par un groupe de personnes ou par une personne ;
- les vérifications ponctuelles ne pourraient avoir qu'un seul but, la détection d'une menace affectant les intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure ; il ne pourrait s'agir que d'une menace liée aux relations

entre l'identifiant technique concerné et la zone géographique, l'organisation, le groupe de personnes ou la personne objet de l'autorisation ; ainsi les vérifications ponctuelles se limiteraient à une « levée de doute », destinée à déterminer si la personne utilisant l'identifiant technique doit, le cas échéant, faire l'objet d'une surveillance individuelle ;

- les vérifications ponctuelles ne pourraient porter que sur des données de connexion ; aux seules fins de détecter en urgence une menace terroriste ou de prévenir une attaque informatique susceptible d'affecter l'indépendance nationale, l'intégrité du territoire ou la défense nationale, des vérifications ponctuelles pourraient, par exception, porter sur des communications tout entières, incluant le contenu des échanges ;
- lorsque les vérifications ponctuelles révèleraient l'existence d'une menace, l'exploitation des communications de la personne concernée ne pourrait être poursuivie que dans le cadre d'une surveillance individuelle, subordonnée à l'obtention d'une autorisation *ad hoc*.

La CNCTR a proposé une modification concernant la dernière des garanties rappelées ci-dessus. Le projet de texte soumis à la commission n'imposait le passage à une mesure de surveillance individuelle que pour « *l'exploitation des communications* » des personnes concernées. La CNCTR a cependant relevé que l'exploitation de seules données de connexion pouvait également constituer une mesure de surveillance individuelle et ne pourrait donc se poursuivre sans autorisation spécifique. Elle a en conséquence préconisé de remplacer les mots : « *l'exploitation des communications* » par les mots : « *l'exploitation des communications ou des seules données de connexion interceptées* », au dernier alinéa du projet de IV de l'article L. 854-2 du code de la sécurité intérieure.

Le Gouvernement a suivi cette préconisation dans l'amendement déposé au Parlement.

En deuxième lieu, s'agissant de la nouvelle mesure de surveillance individuelle, la CNCTR n'a pas émis d'objection de principe à sa création.

Réservée aux services spécialisés de renseignement, dits du « premier cercle », la nouvelle mesure, en permettant d'exploiter les communications d'une personne utilisant un identifiant technique rattachable au territoire français, alors même que cette personne communique depuis la France, constituait une exception à l'interdiction d'utiliser des mesures de surveillance internationale pour assurer la surveillance individuelle de personnes utilisant de tels identifiants.

Le projet du Gouvernement prévoyait deux garanties destinées à limiter le recours à cette mesure dérogatoire :

- la surveillance individuelle ne pourrait être réalisée que sur le fondement d'une autorisation ciblée du Premier ministre, prise après avis de la CNCTR ; contrairement au régime de droit commun en matière de surveillance internationale, la loi faisait ainsi obligation de recourir à une autorisation portant sur une seule personne à la fois ;

- l'autorisation ne pourrait être accordée pour toutes les finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure ; étaient exclues, d'une part, la défense et la promotion des intérêts économiques, industriels et scientifiques majeurs de la France et, d'autre part, 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 CNCTR a estimé que deux garanties supplémentaires devaient être prévues :

- la commission a relevé que la nouvelle mesure était similaire, dans son principe, aux interceptions de sécurité prévues à l'article L. 852-1 du code de la sécurité intérieure ; or ces interceptions sont soumises à un contingentement, décidé après avis de la CNCTR par le Premier ministre, qui limite le nombre d'autorisations simultanément en vigueur ; par cohérence avec les garanties entourant les interceptions

de sécurité et pour limiter au strict nécessaire la surveillance individuelle des communications de personnes utilisant des identifiants techniques rattachables au territoire national, la CNCTR a donc recommandé d'instituer un contingentement des autorisations d'exploitation prévues au projet de V de l'article L. 854-2 du code de la sécurité intérieure et de faire fixer le chiffre du contingent par le Premier ministre après avis de la commission ;

- en outre, pour les mêmes raisons que celles exposées plus haut à propos des vérifications ponctuelles, la CNCTR a considéré qu'une autorisation devait être rendue obligatoire aussi bien pour assurer la surveillance individuelle de communications, contenu des échanges compris, que pour assurer celle de seules données de connexion de personnes utilisant des identifiants techniques rattachables au territoire national ; la commission a ainsi préconisé de remplacer, dans la définition de la portée de l'autorisation, les mots : « *exploitation de communications* » par les mots : « *exploitation de communications ou de seules données de connexion interceptées* ».

Le Gouvernement a suivi les recommandations de la CNCTR sur ces deux points dans l'amendement déposé au Parlement. Il a cependant limité le contingentement des autorisations à celles permettant l'exploitation des communications, contenu des échanges compris, les autorisations d'exploitation de seules données de connexion se trouvant ainsi exclues du contingentement[21].

En troisième lieu, s'agissant des autorisations délivrées sous le régime de la surveillance intérieure qui pourraient valoir, à condition qu'elles le prévoient, autorisation d'exploiter des communications internationales entrant dans leur champ d'application, la CNCTR n'a pas émis d'objection à ce que de telles autorisations puissent être complétées par le recueil et l'exploitation de données équivalentes issues de communications électroniques internationales, sous réserve que cette nouvelle faculté ne soit applicable qu'aux autorisations accordées postérieurement à la modification de la loi.

21 - Le chiffre du contingent, c'est-à-dire le nombre maximal d'autorisations simultanément en vigueur, n'était pas encore fixé à la date de rédaction du présent rapport.

Les autorisations concernées étaient celles des accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), des accès aux données de connexion en temps réel pour la seule prévention du terrorisme (article L. 851-2 du même code) et des interceptions de sécurité (I de l'article L. 852-1 du même code).

La CNCTR a précisé que les mesures de surveillance des communications électroniques internationales prises dans ce cadre ne pourraient excéder la portée des autorisations accordées au titre de la surveillance intérieure et devraient respecter les garanties propres à ces autorisations.

Cela signifiait, pour la CNCTR, que les autorisations ne pourraient permettre, en matière internationale, que l'exploitation de données équivalentes, soumises aux mêmes durées de conservation. Plus généralement, les conditions d'exploitation seraient identiques à celles prévues pour la surveillance intérieure. L'exécution des interceptions de sécurité étant centralisée par un service du Premier ministre, le GIC, l'exploitation des communications internationales devrait également avoir lieu au sein de ce service.

En quatrième lieu, s'agissant des pouvoirs de contrôle attribués à la CNCTR par le projet d'amendement, la commission a tout d'abord émis un avis favorable à l'inscription dans la loi de l'obligation pour le Premier ministre de recueillir un avis *a priori* de la CNCTR avant d'accorder toute autorisation d'exploitation de communications ou de seules données de connexion interceptées, sur le fondement du III ou du projet de V de l'article L. 854-2 du code de la sécurité intérieure.

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

La CNCTR s'est également montrée favorable aux modifications législatives prévues pour renforcer ses moyens de contrôle *a posteriori*.

Le projet du Gouvernement prévoyait à cet effet :

- que les vérifications ponctuelles feraient l'objet d'une traçabilité organisée par le Premier ministre après avis de la CNCTR ;
- qu'en cas de vérifications ponctuelles portant, au titre de la prévention du terrorisme, sur des contenus de communications de personnes utilisant des identifiants techniques rattachables au territoire national, la CNCTR devrait se voir immédiatement transmettre les identifiants concernés.

Les mesures comparables lui paraissant devoir être entourées des mêmes garanties, la CNCTR, après avoir relevé que des vérifications ponctuelles pourraient également porter sur des contenus de communications afin de prévenir des attaques informatiques susceptibles d'affecter l'indépendance nationale, l'intégrité du territoire ou la défense nationale, a considéré qu'une transmission immédiate devrait être également prévue dans un tel cas.

Le Gouvernement n'a pas repris cette préconisation dans le projet d'amendement déposé au Parlement.

En cinquième lieu, s'agissant des voies de recours contentieux contre les nouvelles mesures, la CNCTR a approuvé le principe de l'extension des voies de recours contre les mesures de surveillance des communications électroniques internationales, mais a estimé encore inutilement restrictif le dispositif prévu par le projet d'amendement.

Dans le cadre légal en vigueur jusqu'alors, la CNCTR pouvait être saisie par toute personne souhaitant que la commission vérifie qu'aucune mesure de surveillance de ses communications électroniques internationales n'avait été irrégulièrement mise en œuvre à son encontre. En revanche, seul le président de la CNCTR ou trois de ses membres pouvaient saisir le Conseil d'État, sur le fondement de l'article L. 854-9 du code de la sécurité intérieure, d'un recours contentieux portant sur la légalité de mesures de surveillance des communications électroniques internationales.

Dans le projet de modification législative soumis à la CNCTR, le Gouvernement prévoyait d'ouvrir à toute personne la faculté de saisir le Conseil d'État d'un recours contentieux portant sur la légalité de la mise en

œuvre de la nouvelle mesure de surveillance individuelle de communications renvoyant à des identifiants techniques rattachables au territoire national, prévue au projet de V de l'article L. 854-2 du code de la sécurité intérieure.

Il a semblé cependant à la CNCTR que toutes les mesures de surveillance concernant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national devraient pouvoir être contestées devant le Conseil d'État, qu'il s'agisse de mesures de surveillance individuelle ou de vérifications ponctuelles, dès lors que toutes peuvent, le cas échéant, concerner aussi bien des données de connexion que des contenus de communications et, partant, porter une atteinte à la vie privée des personnes en cause.

Plus largement, la CNCTR s'est interrogée sur la pertinence de maintenir une inégalité en matière de droit au recours, qui ne se fonderait que sur le rattachement au territoire national des identifiants techniques concernés. La pratique des réclamations adressées à la CNCTR par des particuliers sur le fondement de l'article L. 854-9 du code de la sécurité intérieure depuis l'entrée en vigueur du cadre légal en 2015 n'a pas fourni de justification à l'absence de droit au recours direct en matière de surveillance des communications électroniques internationales.

Aussi la CNCTR a-t-elle recommandé au Gouvernement de permettre à toute personne de saisir le juge administratif de toute mesure susceptible de concerner ses communications électroniques internationales, sous réserve de justifier avoir préalablement saisi la CNCTR d'une réclamation.

Le Gouvernement n'a pas retenu ces recommandations d'extension du droit au recours dans le projet d'amendement déposé au Parlement.

Sur l'ensemble des sujets évoqués ci-dessus, le Parlement a approuvé sans modification le projet d'amendement présenté par le Gouvernement. Les trois nouvelles mesures et les moyens de leur contrôle ont été insérés aux articles L. 854-1, L. 854-2, L. 854-4 et L. 854-9 du code de la sécurité intérieure[22].

22 - Voir ces articles dans leur rédaction résultant de l'article 37 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

1.1.3 Un encadrement rénové des essais de matériels de renseignement par la direction générale de l'armement et certaines unités des armées

En 2018, à l'initiative du Gouvernement, le législateur a précisé et renforcé un dispositif entrant de façon marginale dans le champ de compétence de la CNCTR. Il s'agit des essais menés par la direction générale de l'armement et par certaines unités des armées sur des appareils ou des dispositifs permettant de mettre en œuvre des techniques de renseignement. Ces essais ne peuvent avoir pour objet que de tester les matériels concernés, à l'exclusion de toute exploitation des données recueillies.

Les matériels sont destinés à appuyer l'action des forces armées engagées dans des opérations à l'étranger, en leur donnant la maîtrise d'outils qui permettent le recueil hors du territoire national de renseignements d'intérêt militaire. Les essais pouvant être effectués en France, la loi prévoit une autorisation, sans laquelle ils constitueraient des infractions pénales dès lors qu'ils sont susceptibles d'entraîner l'interception résiduelle de communications privées.

Depuis 2017, l'article L. 2371-2 du code de la défense[23] prévoit la réalisation de tels essais sur des matériels permettant de réaliser des mesures de surveillance de certaines communications empruntant la voie hertzienne. Ces mesures sont celles relevant de « l'exception hertzienne » prévue aux articles L. 855-1 A à L. 855-1 C du code de la sécurité intérieure. Elles permettent d'intercepter 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[24].

23 - Voir cet article dans sa rédaction résultant de l'article 18 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

24 - Voir, pour une présentation détaillée de « l'exception hertzienne », le point 1.2.2 du deuxième rapport d'activité 2017 de la CNCTR.

Une autorisation légale limitée à ces mesures n'était pas adaptée aux besoins opérationnels des armées sur des théâtres d'intervention extérieure. La loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 a donc élargi la portée de l'autorisation, tout en renforçant les garanties entourant la réalisation des essais[25].

L'article L. 2371-2 du code de la défense prévoit désormais que la délégation générale de l'armement et certaines unités des armées sont autorisées à effectuer des essais sur des appareils et des dispositifs permettant de mettre en œuvre les techniques de renseignement suivantes :

- des recueils de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure) ;
- des interceptions de correspondances par *IMSI catcher* (II de l'article L. 852-1 du même code) ;
- des interceptions de correspondances empruntant exclusivement une voie hertzienne privative (article L. 852-2 du même code) ;
- des mesures de surveillance des communications électroniques internationales (article L. 854-1 du même code) ;
- des interceptions de communications empruntant exclusivement une voie hertzienne ouverte (article L. 855-1 A du même code).

En contrepartie de cet élargissement :

- une déclaration doit être adressée à la CNCTR préalablement à la réalisation des essais ;
- les données recueillies ne peuvent être conservées que pour la durée des essais ;
- la CNCTR est informée du champ et de la nature des essais effectués ; un registre rendant compte de ces opérations est tenu à sa disposition ;
- un arrêté du ministre de la défense, pris après avis de la CNCTR, précise les conditions d'application des dispositions légales.

25 - Voir l'article L. 2371-2 du code de la défense dans sa rédaction issue de l'article 36 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

Le 28 octobre 2018, la ministre des armées a saisi la CNCTR pour avis d'un projet d'arrêté pris pour l'application de l'article L. 2371-2 du code de la défense. Ce projet avait pour objet :

- de préciser la nature des essais autorisés par la loi, en les liant aux travaux de recherche et de développement, de vérification, de validation et de qualification des matériels concernés ;
- d'énumérer les informations que doivent comporter, d'une part, la déclaration adressée à la CNCTR avant tout essai et, d'autre part, le registre recensant les opérations réalisées.

Dans une délibération adoptée en formation plénière le 8 novembre 2018[26], la CNCTR a émis un avis favorable sur le projet d'arrêté qui lui était soumis, en précisant que, si le projet ne fixait pas de délai pour adresser à la commission la déclaration préalable, celle-ci devrait lui parvenir avec un délai suffisant pour que la CNCTR puisse utilement l'examiner et formuler, le cas échéant, les observations nécessaires pour garantir le respect de la loi.

Une fois l'avis de la CNCTR recueilli, l'arrêté a été édicté par la ministre des armées au début de l'année 2019[27].

26 - Voir la délibération de la CNCTR n° 4/2018 du 8 novembre 2018, publiée en annexe n° 5 au présent rapport et sur le site internet de la commission.

27 - Voir l'arrêté du 3 janvier 2019 relatif aux essais de matériels de renseignement réalisés en application de l'article L. 2371-2 du code de la défense.

Une augmentation du contingent des interceptions de sécurité

Les interceptions de sécurité prévues à l'article L. 852-1 du code de la sécurité intérieure sont soumises à un principe de contingentement, en vertu duquel le nombre d'autorisations simultanément en vigueur ne peut excéder un maximum fixé par le Premier ministre après avis de la CNCTR.

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, de manière générale, à ne recourir à la technique concernée 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 GIC, qui centralise les demandes de techniques de renseignement, s'assure quotidiennement du respect du contingent et en rend compte à la CNCTR.

Saisie par le Premier ministre en mai 2018 d'un projet d'augmentation de 18% du contingent applicable aux interceptions de sécurité, la CNCTR s'est prononcée par une délibération adoptée en formation plénière le 7 juin 2018[28]. Comme lors de la précédente augmentation du contingent en 2017, la CNCTR, après avoir constaté que le nombre maximal d'autorisations simultanément en vigueur n'était pas loin d'être atteint, a estimé avéré le besoin d'augmenter à nouveau le contingent eu égard à la persistance d'une menace terroriste élevée.

Par une décision du 28 juin 2018, le Premier ministre a fixé à 3 600 autorisations simultanées le nouveau contingent et l'a réparti entre les différents ministères dont relèvent les services de renseignement.

Le tableau ci-contre rappelle l'évolution du contingent des interceptions de sécurité depuis son inscription dans la loi en 1991.

28 - Voir la délibération de la CNCTR n° 3/2018 du 7 juin 2018, publiée en annexe n° 4 au présent rapport et sur le site internet de la commission.

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

Pour mémoire, deux autres techniques de renseignement sont soumises à contingentement, le recueil de données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure et le recueil de données de connexion par *IMSI catcher* prévu à l'article L. 851-6 du même code. Fixés à 500 en janvier 2018 pour le premier et à 60 en janvier 2016 pour le second par deux décisions du Premier ministre prises après avis de la CNCTR, ces contingents n'ont pas évolué depuis lors[29].

29 - Voir l'encadré intitulé « Les techniques de renseignement soumises à contingentement » aux pages 37 à 39 du deuxième rapport d'activité 2017 de la CNCTR.

1.2 Les perspectives d'évolutions du cadre législatif : les propositions de la CNCTR pour approfondir le contrôle sur le recueil et l'exploitation du renseignement

En 2020, le Parlement débattra du devenir de la technique de renseignement consistant à mettre en œuvre des algorithmes sur des données de connexion issues des réseaux des opérateurs de communications électroniques, à la seule fin de détecter des menaces terroristes. Le recours à cette technique n'est actuellement autorisé que dans le cadre d'une expérimentation. L'article L. 851-3 du code de la sécurité intérieure, qui la prévoit, n'est en vigueur que jusqu'au 31 décembre 2020[30]. Avant cette date, le législateur devra donc, au vu notamment d'un rapport que le Gouvernement est tenu de lui présenter au plus tard le 30 juin 2020[31], décider s'il souhaite supprimer la technique, prolonger la période expérimentale ou pérenniser les dispositions concernées.

Ce débat au Parlement sur une question relevant du droit du renseignement pourrait, en outre, constituer une occasion pour faire un bilan plus général de l'application du cadre légal entré en vigueur en 2015. Certaines dispositions de procédure, dont la pratique a révélé les difficultés d'application, pourraient être rectifiées. Certains encadrements, trop souples ou trop rigoureux, pourraient nécessiter des ajustements. Des sujets d'une ampleur plus vaste, que la discussion parlementaire n'avait pu aborder en 2015 mais dont l'actualité a confirmé l'intérêt, pourraient également être soumis à l'examen du législateur.

Dans cette perspective, pour nourrir de futurs débats au sein du Gouvernement comme du Parlement, la CNCTR a souhaité livrer les réflexions suivantes.

---

30 - Initialement limitée au 31 décembre 2018 par l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, la validité de l'article L. 851-3 du code de la sécurité intérieure a été prolongée jusqu'au 31 décembre 2020 par l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

31 - Voir l'article 25 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement dans sa rédaction résultant de l'article 17 de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

1.2.1 Une extension du droit au recours contentieux en matière de surveillance internationale

Une modification législative pourrait consister à élargir, en matière de surveillance des communications électroniques internationales, le droit de toute personne de saisir le Conseil d'État d'un recours tendant à ce que le juge administratif vérifie qu'aucune mesure de surveillance n'a été irrégulièrement mise en œuvre à son encontre.

L'accès au juge administratif en matière de surveillance des communications électroniques internationales, prévu à l'article L. 854-9 du code de la sécurité intérieure, est aujourd'hui réservé au président de la CNCTR ou à trois de ses membres, au cas où la commission constaterait un manquement à la loi auquel le Gouvernement ne remédierait pas de façon satisfaisante. La seule exception à ce principe concerne les autorisations permettant d'exploiter les communications ou les seules données de connexion de personnes utilisant des identifiants techniques rattachables au territoire national, lorsque ces personnes communiquent depuis la France. Sous réserve d'avoir préalablement saisi la CNCTR d'une réclamation portant sur la légalité d'une telle autorisation, toute personne peut, dans ce cas, demander au juge administratif d'en vérifier également la légalité.

Comme elle l'a déjà indiqué au Gouvernement lors des travaux ayant conduit à modifier en 2018 les dispositions légales relatives à la surveillance des communications électroniques internationales[32], la CNCTR considère que l'accès direct au juge devrait, à tout le moins, pouvoir porter sur toutes les mesures tendant à exploiter des communications ou des seules données de connexion de personnes utilisant des identifiants techniques rattachables au territoire national.

Plus largement, la CNCTR doute, s'agissant du droit au recours, de la pertinence d'une distinction fondée sur le rattachement au territoire national des identifiants techniques concernés. Aussi recommande-t-elle de permettre à toute personne de saisir le juge administratif de toute mesure susceptible de concerner ses communications électroniques internationales, sous la seule réserve de justifier avoir préalablement saisi la commission d'une réclamation.

32 - Voir le point 1.1.2 du présent rapport.

1.2.2 Des ajustements législatifs pour renforcer la cohérence du cadre juridique applicable au renseignement

La CNCTR soumet à l'appréciation du Gouvernement et du Parlement quelques propositions de modifications législatives sur des sujets techniques ou de procédure. Ces propositions ont pour but une simplification et une amélioration de la cohérence générale du cadre légal.

Une première modification pourrait consister à prévoir une durée maximale de conservation unique pour les données collectées par les dispositifs de captation de paroles et ceux de captation d'images prévus à l'article L. 853-1 du code de la sécurité intérieure.

Les durées maximales de conservation en vigueur, fixées aux 1° et 2° de l'article L. 822-2 du code de la sécurité intérieure, sont à ce jour :

- trente jours à compter de leur recueil, pour les paroles prononcées à titre privé ;
- cent-vingt-jours à compter de leur recueil, pour les images captées dans un lieu privé.

La CNCTR considère que le caractère éventuellement plus intrusif d'une technique par rapport à l'autre ne justifie pas une distinction entre les durées maximales de conservation des données recueillies. Les débats parlementaires sur le projet de loi relatif au renseignement en 2015 n'apportent pas d'élément décisif à ce sujet. Par ailleurs, la distinction s'est révélée, à l'usage, problématique pour les services de renseignement, qui ont parfois recours à des caméras captant à la fois les images et les paroles. Une exploitation différenciée des deux types de données collectées paraît alors artificiellement contraignante.

Une deuxième modification pourrait consister à prévoir qu'une introduction dans un lieu d'habitation à la seule fin de retirer un dispositif ayant servi à recueillir des renseignements[33] puisse être autorisée par le

33 - Il peut s'agir, en application de l'article L. 853-3 du code de la sécurité intérieure, de dispositifs de balisage, de captation de paroles prononcées à titre privé, de captation d'images dans un lieu privé ou de recueil et de captation de données informatiques.

Premier ministre au vu d'un avis rendu par un membre de la CNCTR statuant seul et non plus uniquement par une formation collégiale de la commission.

L'introduction d'agents de services de renseignement dans un lieu privé pour y mettre en place, utiliser ou retirer certains dispositifs de surveillance doit, en vertu de l'article L. 853-3 du code de la sécurité intérieure, être spécialement autorisée par le Premier ministre après avis de la CNCTR. La loi prévoit en outre que l'avis de la commission doit être rendu en formation collégiale, restreinte ou plénière, lorsque le lieu concerné est à usage d'habitation.

Si la CNCTR estime justifié l'examen en formation collégiale des demandes d'introduction dans un lieu d'habitation pour y mettre en place ou y utiliser des dispositifs de surveillance, cette procédure lui paraît en revanche inadaptée aux demandes qui ont pour seul but le retrait de tels dispositifs. L'atteinte essentielle à la vie privée de la personne concernée a lieu au moment de l'installation d'un dispositif et doit, par conséquent, être appréciée par le collège de la CNCTR. Lorsque le service souhaite reprendre son matériel, la commission ne peut, dans les faits, qu'émettre un avis favorable, puisque le retrait du dispositif de surveillance bénéficie à la vie privée de la personne intéressée.

Si un membre de la CNCTR ayant la qualité de magistrat ou de membre du Conseil d'État pouvait, en l'espèce, émettre seul l'avis de la commission, selon le droit commun du traitement des demandes, la procédure gagnerait en rapidité. Un membre seul dispose en effet de vingt-quatre heures pour se prononcer, tandis que le collège de la commission peut statuer dans un délai de soixante-douze heures. En outre, les formations collégiales de la CNCTR pourraient se concentrer davantage sur les demandes nécessitant une réelle délibération pour apprécier la proportionnalité de l'atteinte portée à la vie privée.

1.2.3 Une réorganisation du contrôle *a priori* sur certains accès aux données de connexion en temps différé

L'article L. 851-1 du code de la sécurité intérieure ouvre aux services de renseignement la faculté, sur autorisation du Premier ministre accordée après avis de la CNCTR, d'accéder à des données de connexion conservées par des opérateurs de communications électroniques ou des fournisseurs de services au public en ligne. Cet accès a donc lieu en temps différé, à la différence d'autres recueils de données de connexion dont la loi prévoit qu'ils puissent avoir lieu en temps réel.

Deux types de données de connexion sont généralement distingués parmi celles que mentionne l'article L. 851-1 du code de la sécurité intérieure :

- les données relatives « *à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques* » ainsi que celles relatives « *au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée* » ;
- les données relatives « *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* ».

Dans le premier cas, les informations recherchées peuvent être soit l'identité d'un abonné ou d'une personne connectée à une ligne téléphonique, un accès à internet ou un service au public en ligne, soit les numéros d'abonnement ou de connexion d'une personne désignée à des services de communications électroniques. Par exemple, un service de renseignement disposant d'un numéro de téléphone peut demander à connaître l'identité du titulaire de la ligne. À l'inverse, s'il connaît l'identité d'une personne, il peut demander à connaître ses numéros de téléphone. Dans ces situations, la technique de renseignement prévue à l'article L. 851-1 du code de la sécurité intérieure remplit principalement une fonction d'annuaire.

Dans le second cas, les informations recherchées sont essentiellement des détails de communications téléphoniques ou internet. Il s'agit par exemple

de « factures détaillées » d'appels téléphoniques, dites « fadet », qui permettent de connaître le nombre, les numéros appelant et appelé, la durée, voire la localisation de tels appels.

La CNCTR ne propose pas de modifications concernant les demandes relevant du second cas, concernant pour l'essentiel des « factures détaillées ». Elle s'interroge en revanche sur la pertinence du niveau de contrôle exercé jusqu'à présent sur les demandes relevant du premier cas, c'est-à-dire les identifications d'abonnés ou les recensements de numéros d'abonnement.

Depuis l'entrée en vigueur de l'article L. 851-1 du code de la sécurité intérieure le 1er février 2016, les demandes fondées sur ces dispositions ont représenté environ deux tiers des quelque 70 000 demandes de techniques de renseignement présentées chaque année. En 2018, plus de 46 000 demandes portaient sur ces accès à des données de connexion en temps différé.

Au sein des demandes :

- environ les deux tiers concernent des identifications d'abonnés ou des recensements de numéros d'abonnement, soit autour de 30 000 demandes par an en moyenne ;
- le tiers restant concerne les demandes de « factures détaillées » et assimilées, soit un peu plus de 16 000 demandes par an en moyenne.

La CNCTR considère que le recueil d'identifications d'abonnés ou de numéros d'abonnement est conçu non tant comme une mesure de surveillance en soi que comme une mesure préparatoire à des mesures de surveillance à proprement parler. Un service de renseignement peut ainsi obtenir le numéro de téléphone d'une personne suspecte dans le but de solliciter ensuite une autorisation d'accès à une « facture détaillée » afférente à ce numéro ; il peut également chercher à préparer une demande d'interception des communications émises ou reçues par ce numéro. Les identifications d'abonnés ou les recensements de numéros d'abonnement peuvent aussi compléter des mesures de surveillance déjà autorisées, par exemple pour identifier les correspondants d'une personne, dont une « facture détaillée » fait apparaître les numéros. Dans tous les cas, pour la CNCTR, ce sont les techniques que les opérations d'identification préparent ou complètent qui portent atteinte à la vie privée, non ces opérations elles-mêmes.

La loi prévoit déjà un statut légèrement dérogatoire en matière de contrôle pour les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement. Contrairement à l'ensemble des autres demandes tendant à la mise en œuvre de techniques de renseignement, qui doivent être approuvées par le ministre dont relève le service à l'origine des demandes, celles qui concernent des opérations d'identification d'abonnés ou des recensements de numéros d'abonnement sont, en vertu du deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure, directement présentées à la CNCTR puis au Premier ministre par les agents des services de renseignement dont elles émanent.

Lorsqu'elle contrôle *a priori* les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement, la CNCTR, eu égard à leur caractère faiblement intrusif, exerce un contrôle de légalité réduit, qui se borne le plus souvent à vérifier que la motivation de la demande comporte des éléments concernant les intérêts fondamentaux de la Nation invoqués. Le contrôle de proportionnalité ne trouve pas matière à s'appliquer. Seul un contrôle de l'erreur manifeste d'appréciation est le cas échéant pratiqué.

Pour l'ensemble des raisons exposées ci-dessus, la CNCTR estime, après trois ans d'expérience, que le contrôle *a priori* qu'elle exerce sur les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement est d'une faible valeur ajoutée.

Si la commission ne conteste pas l'utilité d'un contrôle *a priori*, qui permet de détecter des erreurs manifestes d'appréciation, elle est d'avis que ce type de contrôle relève davantage de la compétence du GIC, service du Premier ministre auquel la loi confie la mission de recueillir de façon centralisée les données de connexion auprès des opérateurs de communications électroniques ou des fournisseurs de services au public en ligne. Ce service est également celui qui centralise toutes les demandes de techniques de renseignement et les met à disposition de la CNCTR et du Premier ministre pour traitement. Distinct des services de renseignement car constitué en service à compétence nationale relevant du Premier ministre, le GIC, qui dispose de compétences juridiques et d'effectifs exerçant des missions de contrôle, pourrait remplir de façon adaptée le rôle de conseiller de l'autorité décisionnaire pour les demandes d'identification d'abonnés ou de recensement de numéros d'abonnement.

Par exception, la CNCTR pourrait conserver sa compétence en matière de contrôle *a priori* lorsque la demande porte sur une personne exerçant une profession ou un mandat bénéficiant d'une protection particulière en vertu de la loi. Sont concernés les parlementaires, les magistrats, les avocats et les journalistes, pour lesquels l'article L. 821-7 du code de la sécurité intérieure impose notamment que la CNCTR rende un avis *a priori* en formation plénière lorsque des techniques de renseignement sont sollicitées à leur encontre.

Dans tous les cas, la CNCTR conserverait l'intégralité de sa compétence en matière de contrôle *a posteriori* et se réserverait la possibilité de vérifier la légalité de tout recueil de données de connexion au regard de l'autorisation accordée.

1.2.4 Une réflexion à mener sur l'encadrement légal des échanges de données entre les services de renseignement français et leurs partenaires étrangers

Lorsque le cadre légal applicable aux activités de renseignement a été entièrement rénové en 2015, le législateur a soumis à autorisation préalable du Premier ministre et au contrôle d'une autorité administrative indépendante, la CNCTR, un ensemble de techniques permettant aux services de renseignement de recueillir sur le territoire national des informations nécessaires à la défense et à la promotion des intérêts fondamentaux de la Nation.

N'ont pas été inclus dans cet encadrement légal les échanges de données avec des services de renseignement étrangers, qu'il s'agisse d'éléments que les services français transmettent à leurs partenaires ou de renseignements qu'ils reçoivent de ceux-ci.

Eu égard aux conséquences potentielles sur la vie privée des Français et, de manière générale, de toute personne résidant en France ainsi qu'aux évolutions du contexte juridique, en particulier international, la CNCTR estime qu'une réflexion doit être menée sur l'encadrement légal des échanges de données entre les services de renseignement français et leurs partenaires étrangers.

La prévention des menaces communes, notamment terroristes, auxquelles sont confrontés la France et ses alliés justifie l'existence d'une intense coopération entre services de renseignement de ces différents pays. Faute d'une telle coopération, les services verraient compromis l'accomplissement de certaines de leurs missions. Par nature très sensible et participant de la souveraineté de l'État dans la conduite de sa politique étrangère, la coopération internationale entre services de renseignement a vocation, comme le reste des activités de ces services, à demeurer couverte par le secret. Une gestion imprudente des données échangées pourraient entraîner notamment de graves complications diplomatiques ou une perte de crédibilité des services français nuisant à leur action. Une coutume, dite du « tiers service », est à cet égard souvent invoquée pour justifier qu'un service de renseignement recevant des données d'un partenaire étranger s'interdise, sauf autorisation de ce partenaire, de communiquer les données à un troisième organe.

L'éventualité que des échanges internationaux incluent des données sur des citoyens français ou sur toute personne résidant en France incite cependant la CNCTR à s'interroger sur la règle de droit qui pourrait s'appliquer en la matière et, partant, sur le niveau de protection dont devraient le cas échéant bénéficier ces données.

a) Tout d'abord, la CNCTR, en se fondant sur son champ de compétence prévu par la loi[34], s'interroge sur la possibilité que non seulement les éléments transmis par des services de renseignement français à des partenaires étrangers, désignés comme « flux sortants », mais aussi ceux communiqués par des services de renseignement étrangers à leurs partenaires français, désignés comme « flux entrants », soient susceptibles de comprendre des données dont le recueil, l'exploitation et la conservation entrent dans le champ d'application du livre VIII du code de la sécurité intérieure, c'est-à-dire du cadre légal institué en 2015.

S'agissant des « flux sortants », il ne peut être exclu qu'ils contiennent soit des données recueillies au moyen de techniques de renseignement régies par le livre VIII du code de la sécurité intérieure, soit des transcriptions et des extractions réalisées à partir de ces données et elles-mêmes soumises aux dispositions du code. La transmission éventuelle de tels éléments à des services de renseignement étrangers a pour conséquence implicite de les soustraire à l'application des dispositions légales françaises.

À titre d'exemple :

- les données recueillies au moyen de techniques de renseignement doivent, en vertu des articles L. 822-2, L. 854-5 et L. 854-8 du code de la sécurité intérieure, être détruites à l'expiration de durées fixées par la loi en fonction de la nature des données ; en cas de transmission à des partenaires étrangers, le respect de ces durées maximales de conservation ne peut être garanti ;

34 - L'article L. 833-1 du code de la sécurité intérieure définit de manière générale cette compétence en prévoyant que la CNCTR veille à ce que les techniques de recueil de renseignement soient mises en œuvre sur le territoire national conformément au livre VIII du même code.

- les transcriptions et les extractions de données recueillies au moyen de techniques de renseignement doivent, en vertu des articles L. 822-3 et L. 854-6 du code de la sécurité intérieure, être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités qui ont motivé leur réalisation ; le respect de cette obligation de destruction ne peut pas non plus être assuré, en cas de partage de transcriptions et d'extractions avec des services étrangers.

S'agissant des « flux entrants », il ne peut être non plus exclu qu'ils contiennent des données dont le recueil, l'exploitation et la conservation auraient été soumis au livre VIII du code de la sécurité intérieure si les services de renseignement français les avaient collectées par eux-mêmes. Des telles données pourraient ainsi être privées des garanties légales dont elles auraient bénéficié si elles avaient été recueillies au moyen d'une technique de renseignement prévue par la loi. Parmi ces garanties figurent notamment la nécessité d'obtenir une autorisation préalable du Premier ministre pour les recueillir, l'obligation de les détruire au terme d'une durée légale et l'existence d'un contrôle de légalité par une autorité indépendante et, le cas échéant, par le juge administratif.

b) En l'état actuel du droit applicable en France, il n'existe pas de dispositif permettant de pallier les difficultés évoquées ci-dessus.

Le livre VIII du code de la sécurité intérieure ne mentionne pas les « flux sortants ». Il n'évoque les « flux entrants » que pour faire obstacle à la CNCTR d'accéder aux données qu'ils contiennent. L'article L. 833-2 du code de la sécurité intérieure prévoit en effet que la CNCTR « *(...) peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions (...) à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux (...)* ».

Lors de la discussion parlementaire sur le projet de loi relatif au renseignement en 2015, le sujet des échanges de données entre les services de renseignement français et leurs partenaires étrangers n'a presque pas été abordé.

La rédaction de l'article L. 833-2 du code de la sécurité intérieure, cité ci-dessus, résulte d'un amendement adopté en première lecture du projet de loi par l'Assemblée nationale, lors de l'examen du texte en commission des lois[35]. Conçu comme un élargissement des pouvoirs de la CNCTR, à laquelle était désormais attribuée une faculté de demander au Premier ministre communication de tous éléments nécessaires à ses missions, l'amendement n'a fait l'objet d'aucun débat sur l'exclusion des « flux entrants » de son champ d'application[36].

L'éventualité d'un encadrement spécifique des échanges internationaux de renseignements n'a pas non plus été réellement examinée[37]. Si, dans les faits, ces échanges sont vraisemblablement formalisés par des conventions liant les services de renseignement français à leurs partenaires étrangers, aucune disposition légale n'a fixé de cadre pour la conclusion et l'application de tels accords.

c) Dans ce contexte, la CNCTR constate que, sous réserve d'une étude comparative plus approfondie, le droit français paraît en retrait par rapport aux législations en vigueur dans d'autres États membres de l'Union européenne comparables à la France.

L'Agence des droits fondamentaux de l'Union européenne[38], dans une étude en deux parties portant sur les législations relatives au renseignement en vigueur dans les États membres[39], a indiqué que vingt-sept des vingt-huit États concernés ont défini, avec plus ou moins de précision, un cadre légal applicable à la coopération internationale entre services de renseignement.

35 - Voir l'amendement n° CL 238, adopté le 1er avril 2015 lors de l'examen du texte par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République.

36 - Ni le compte-rendu de la séance de la commission des lois du 1er avril 2015, ni le rapport fait au nom de cette commission (voir le point 6 du B du III du rapport n° 2697 enregistré le 2 avril 2015) ne discutent ce point.

37 - Un amendement ayant pour objet d'instituer une limitation de principe du volume des échanges, lorsqu'ils concernent des citoyens français, a été rejeté lors de la première lecture du projet de loi en séance publique au Sénat (voir l'amendement n° 26 rectifié ter, examiné lors de la séance publique du 4 juin 2015).

38 - L'Agence des droits fondamentaux de l'Union européenne est une agence spécialisée créée par le règlement (CE) n° 168/2007 du Conseil de l'Union du 15 février 2007. Elle a pour objectif de fournir aux institutions de l'Union ainsi qu'à ses États membres une assistance et des compétences en matière de droits fondamentaux.

39 - Voir notamment la seconde partie, publiée en 2017 et intitulée *Surveillance by intelligence services : fundamental rights safeguards and remedies in the European Union – Volume II : field perspectives and legal update*, pages 49 à 52 et 101 à 108.

À titre d'exemple, en Allemagne, plusieurs dispositions autorisent, en les encadrant, les échanges internationaux, en particulier les « flux sortants », selon le type de données concernées.

Les services de renseignement allemands peuvent ainsi transmettre des données à leurs partenaires étrangers sous certaines conditions, qui concernent le niveau de l'autorité décisionnaire en la matière, la formalisation de l'acte de transmission, la nature des finalités poursuivies, les garanties que doivent offrir les services étrangers bénéficiaires et le contrôle de ces échanges par une autorité indépendante. Les données concernées peuvent être issues de mesures de surveillance intérieure ciblées[40] ou avoir été recueillies par des mesures de surveillance internationale non ciblées, qu'il s'agisse de communications entre l'Allemagne et l'étranger[41] ou de communications émises et reçues hors d'Allemagne[42].

La CNCTR a noté, en outre, que l'existence, dans des pays européens, de législations prévoyant un encadrement des échanges internationaux de renseignement a permis à des organes de contrôle indépendants de mener,

---

40 - Effectuée par le *Bundesamt für Verfassungsschutz*, l'équivalent de la direction générale de la sécurité intérieure, la transmission des données doit faire l'objet d'un acte formalisé. Elle doit être nécessaire aux missions du service allemand ou à la protection d'intérêts de sécurité majeurs du partenaire étranger. Elle ne peut avoir lieu lorsqu'y font obstacle soit des intérêts de la politique étrangère allemande, soit des considérations tirées de la protection des personnes concernées par ces données. Le service destinataire des données ne peut les exploiter que pour les motifs pour lesquels il les a reçues. Voir les dispositions combinées de *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, §4 Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungen, Zweckbindung, Absatz 4 et de Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, §19 Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz, Absatz 3*.

41 - Effectuée par le *Bundesnachrichtendienst*, l'équivalent de la direction générale de la sécurité extérieure, la transmission des données doit être autorisée par la chancellerie fédérale sur initiative d'un agent du service de renseignement ayant la qualité de magistrat. Elle doit être nécessaire à la protection d'intérêts de sécurité ou de politique étrangère de l'Allemagne ou du pays partenaire. Elle ne peut avoir lieu si ce pays n'est pas en mesure d'assurer aux données un niveau de protection adapté ainsi qu'une exploitation selon les principes de l'État de droit. Le service destinataire des données ne peut les exploiter que pour les motifs pour lesquels il les a reçues et doit rendre compte de cette exploitation à la demande du service allemand. Un rapport sur ce type de transmission est adressé chaque mois à la commission indépendante, la *G10-Kommission*, qui contrôle les activités de renseignement. Voir *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, §7a Übermittlungen durch den Bundesnachrichtendienst an ausländische öffentliche Stellen*.

42 - La loi fédérale prévoit que les échanges doivent faire l'objet d'accords formalisés, approuvés par la chancellerie fédérale. La loi encadre le contenu et les finalités de telles conventions ainsi que les modalités des transmissions. Le service étranger destinataire des données doit notamment s'engager à les détruire au terme d'une durée fixée par les accords. Les échanges sont soumis au contrôle d'une autorité indépendante composée de magistrats et dénommée *Unabhängiges Gremium*. Voir *Gesetz über den Bundesnachrichtendienst, §13 Kooperation im Rahmen der Ausland-Ausland-Fernmeldeaufklärung*.

à ce sujet, une première expérience de coopération[43]. Les organes belge, danois, néerlandais, norvégien et suisse chargés de contrôler les activités de renseignement ont ainsi élaboré un programme de contrôle commun portant sur l'exploitation et le partage de données en matière de terrorisme. Pendant trois ans, ces organes ont conduit, chacun dans son pays, des contrôles au sein des services de renseignement concernés puis se sont retrouvés lors de séances de travail destinées à évoquer les méthodes utilisées et les difficultés rencontrées, sans faire état d'éléments classifiés. Les contrôles ont pu porter sur les données fournies par des services de renseignement étrangers à leur pays sans que la coutume du « tiers service » soit opposée aux contrôleurs. Comme d'autres organes de contrôle européens rencontrés par la CNCTR, les organes belge, danois, néerlandais, norvégien et suisse n'ont pas estimé que cette coutume leur fût applicable et pourrait faire obstacle aux compétences que leurs législations nationales respectives leur attribuent pour garantir la régularité des activités de renseignement. Au début de l'année 2019, l'organe de contrôle britannique a fait savoir qu'il rejoignait l'expérience de coopération conduite par ses cinq homologues et participerait à la prochaine réunion de travail prévue cette même année.

d) En matière jurisprudentielle, la CNCTR note que la Cour européenne des droits de l'homme (CEDH) a, dans un arrêt du 13 septembre 2018[44], examiné pour la première fois la compatibilité avec les stipulations de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, en l'espèce le droit au respect de la vie privée, de dispositions légales régissant le partage international de données entre services de renseignement. Cet arrêt de chambre n'est pas définitif, un renvoi en grande chambre ayant été accepté par la cour le 4 février 2019. Une formation de jugement élargie de la CEDH va donc à nouveau examiner l'affaire.

43 - Voir le communiqué de presse conjoint du 14 novembre 2018 intitulé « Déclaration commune : renforcement de la coopération en matière de contrôle des services de renseignement et de sécurité ».

44 - Voir l'arrêt de la CEDH du 13 septembre 2018, n° 58170/13, affaire *Big Brother Watch* et autres contre Royaume-Uni, notamment les paragraphes 422 à 424.

La CEDH, se prononçant en l'espèce sur les « flux entrants », a estimé que, comme pour tout dispositif permettant d'obtenir des renseignements, celui consistant à recevoir des données de partenaires étrangers devait avoir une base légale, accessible et prévisible, ainsi qu'être proportionné et contrôlable de manière adéquate.

Examinant ensuite les critères au regard desquels la conformité à la convention de la nécessaire base légale devait être appréciée[45], la CEDH a considéré que pourrait constituer une garantie adaptée le fait de subordonner l'exploitation des « flux entrants » au respect des exigences légales applicables à la mise en œuvre de techniques de renseignement sur le territoire de l'État receveur. À tout le moins, la législation nationale devrait entourer de garanties la conservation, l'exploitation, la transmission et la destruction des données issues des « flux entrants ».

La cour a averti qu'au cas où les États pourraient disposer à leur discrétion de données fournies par des partenaires, en particulier par des États non parties à la convention de sauvegarde des droits de l'homme et des libertés fondamentales, ils pourraient en user pour contrevenir à leurs obligations au regard de cette convention ou même de leur droit interne. La cour a fait ainsi allusion au risque théorique qu'un service de renseignement auquel une autorisation de recueillir des données aurait été refusée obtienne ces données par l'intermédiaire d'un partenaire étranger.

En l'espèce, après avoir notamment observé que le cadre légal britannique en matière d'échanges internationaux de renseignement était suffisamment précis et accessible, que, sauf exception, les services britanniques ne pouvaient exploiter de données transmises par des partenaires étrangers que sur le fondement d'une autorisation de droit interne, que cette transmission devait être proportionnée aux buts poursuivis, que les données ne pouvaient être conservées qu'aussi longtemps qu'elles étaient nécessaires à ces buts,

45 - La cour a fait usage de l'ensemble des critères énoncés notamment dans son arrêt du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment au paragraphe 232.

enfin qu'un organe de contrôle indépendant, dénommé *Investigatory Powers Commissioner*, se reconnaissait compétent pour contrôler les accords de partage international de renseignements, la CEDH a jugé que la législation britannique ne méconnaissait pas les stipulations de la convention relatives au droit au respect de la vie privée.

e) Enfin, la CNCTR a eu l'occasion de constater que les échanges internationaux de données étaient, en matière de renseignement, un sujet de préoccupation pour certaines organisations de défense des libertés individuelles. Elle a notamment été interrogée en 2017, dans le cadre d'une étude portant sur plusieurs pays, par une organisation non-gouvernementale qui souhaitait obtenir des éclaircissements sur l'encadrement légal et les procédures de contrôle des partages de données entre services de renseignement français et étrangers.

2. Le contrôle de la mise en œuvre des techniques de renseignement : un élargissement de la base légale du contrôle *a priori* et une poursuite de l'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, à la fois *a priori* et *a posteriori*, porte également sur les mesures de surveillance des communications électroniques internationales, en application de l'article L. 854-9 du code de la sécurité intérieure.

Le contrôle préalable de la CNCTR sur les demandes tendant à la mise en œuvre de techniques de renseignement a légèrement crû en 2018, dans des proportions comparables à celles de 2017. Le contrôle *a posteriori*, qui avait fortement progressé en intensité en 2017, a gagné en maturité en 2018 et cherche désormais à s'approfondir.

Les moyens financiers et humains de la CNCTR

Composée d'un collège de neuf membres qui s'appuie sur un secrétariat général de dix-sept agents, la CNCTR dispose d'un budget propre qu'elle gère en toute indépendance.

Les crédits alloués par le Parlement à la CNCTR sont inscrits au budget général de l'État (mission « Direction de l'action du Gouvernement », programme n° 308 « Protection des droits et libertés », action n° 12 « Commission nationale de contrôle des techniques de renseignement »).

La loi de finances initiale pour 2018[46] a attribué à la CNCTR des montants de 2,5 millions d'euros pour ses dépenses de personnel et de 370 000 euros pour ses dépenses de fonctionnement. Ces crédits ont été presque entièrement consommés.

Les dépenses de fonctionnement ont directement participé à l'accomplissement des activités de contrôle de la CNCTR. Ils ont couvert les frais de déplacement des membres et des agents pour contrôler des services de renseignement sur l'ensemble du territoire national. Ils ont financé l'achat et la maintenance des matériels informatiques constituant le réseau interne sécurisé de la commission. Enfin ils ont contribué à l'aménagement des nouveaux locaux de la CNCTR, qui sont caractérisés par un niveau de sécurité très élevé, destiné à respecter toutes les règles prévues par l'instruction générale interministérielle n° 1 300 sur la protection du secret de la défense nationale.

46 - Voir la loi n° 2017-1837 du 30 décembre 2017 de finances pour 2018.

2.1 Une activité de contrôle *a priori* en légère augmentation, entre prédominance de la prévention du terrorisme et léger rééquilibrage des autres finalités légales

Grâce aux développements informatiques conduits par le GIC depuis 2016, la dématérialisation et l'unification de la procédure régissant les demandes de mise en œuvre de techniques de renseignement n'ont cessé de progresser. Les éléments statistiques figurant dans le présent rapport demeurent cependant 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.

Comme dans ses deux premiers rapports d'activité, la CNCTR présente des éléments statistiques sur les techniques de renseignement relevant de la surveillance intérieure, c'est-à-dire destinées à surveiller des personnes situées sur le territoire national[47].

Pour la première fois, la CNCTR présente également le nombre d'avis *a priori* rendus en une année sur des demandes relevant de la surveillance des communications électroniques internationales.

47 - Voir le résumé du cadre juridique en vigueur en introduction au présent rapport.

2.1.1 Le nombre d'avis préalables rendus par la CNCTR en matière de surveillance intérieure : des évolutions toujours contrastées selon les techniques de renseignement

En matière de surveillance intérieure, les avis préalables rendus par la CNCTR, 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, 2017 et 2018. Aucune demande n'a en effet été présentée, au cours de ces trois années, selon la procédure d'urgence absolue prévue 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[48].

48 - 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.

	2016	2017	2018	Évolution 2017 /2018
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	28 741	-4,6 %
Accès aux données de connexion en temps différé (autres demandes, dont celles de « factures détaillées »[49]) (article L. 851-1 du code de la sécurité intérieure)	15 021	18 512	17 443	-5,8 %
Géolocalisations en temps réel (article L. 851-4 du code de la sécurité intérieure)	2 426	3 751	5 191	+38,4 %
Interceptions de sécurité *via* le GIC (I de l'article L. 852-1 du code de la sécurité intérieure)	8 137	8 758	10 562	+20,6 %
Autres techniques de renseignement[50]	9 408	9 295	11 361	+22,2 %
Ensemble des techniques de renseignement	**67 088**	**70 432**	**73 298**	**+4,1 %**

49 - 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.

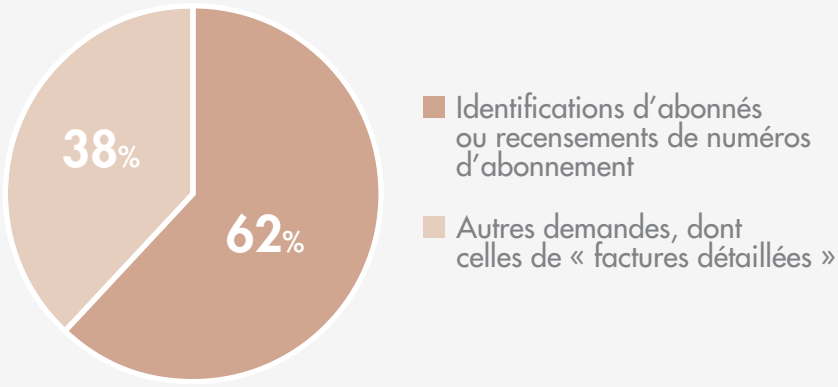
50 - Sont incluses les demandes d'accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure), celles de mise en œuvre de traitements automatisés sur des données de connexion (article L. 851-3 du même code), celles de balisage (article L. 851-5 du même code), celles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

Si le nombre total de demandes tendant à la mise en œuvre de techniques de renseignement a légèrement augmenté d'un peu plus de 4 % au cours de l'année 2018, 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. Ces demandes ont connu une baisse de 5 % en 2018 alors qu'elles augmentaient depuis 2016.

La CNCTR précise que les demandes comptabilisées au titre de l'article L. 851-1 du code de la sécurité intérieure peuvent porter sur plusieurs accès à la fois. Par exemple, une demande de recensement de numéros d'abonnement téléphonique d'une personne peut entraîner le recueil de plusieurs numéros auprès de plusieurs opérateurs de communications électroniques. Le nombre de demandes examinées par la CNCTR représente donc un ensemble de dossiers comportant un ou plusieurs accès à des données de connexion en temps différé.

La répartition des demandes d'accès aux données de connexion en temps différé en 2018



En deuxième lieu, la géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure) a poursuivi en 2018 sa forte progression, qui avait commencé dès l'autorisation de cette technique par la loi au 1er janvier 2015[51]. L'augmentation de plus de 38 % en 2018 est toutefois inférieure à celle de 55 % observée en 2017, qui était elle-même en deçà de celle de 87 % 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 2018, de façon importante dans un contexte marqué par une menace terroriste persistante et par la nécessité de prévenir des violences collectives de nature à porter gravement atteinte à la paix publique. Le taux d'augmentation s'élève à 20 %. Par comparaison, les taux des deux années précédentes étaient plus réduits (+5,6 % en 2016 et +7,6 % 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 ont également nettement augmenté en 2018. Cette hausse de plus de 20 %, comparée à la stabilité observée en 2017, peut s'interpréter comme une appropriation par les services de ces techniques complexes à mettre en œuvre.

Comme dans ses précédents rapports 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 rapport d'activité de la commission 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.

Ainsi qu'elle l'avait fait en 2017, la CNCTR indique cependant que deux nouvelles autorisations ont été accordées en 2018, en application de l'article L. 851-3 du code de la sécurité intérieure, pour mettre en œuvre des algorithmes sur des données de connexion afin de détecter des menaces terroristes. À la fin de l'année 2018, trois algorithmes avaient donc été autorisés depuis l'entrée en vigueur du cadre légal le 3 octobre 2015 et étaient en fonctionnement.

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

Les avis défavorables rendus par la CNCTR

En 2018, 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, 569 avis défavorables, soit 2,1 % du nombre d'avis rendus.

Ce taux, moins élevé que ceux de 6,9 % et 3,6 % observés en 2016 et en 2017, confirme la volonté manifestée par les services demandeurs de se conformer à la doctrine établie et connue 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, dans la continuité, 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 53 avis défavorables sur les demandes d'accès aux données de connexion en temps différé, soit environ 0,1 % du nombre d'avis rendus sur des demandes concernant cette technique.

En 2018, 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 cadre légal le 3 octobre 2015.

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

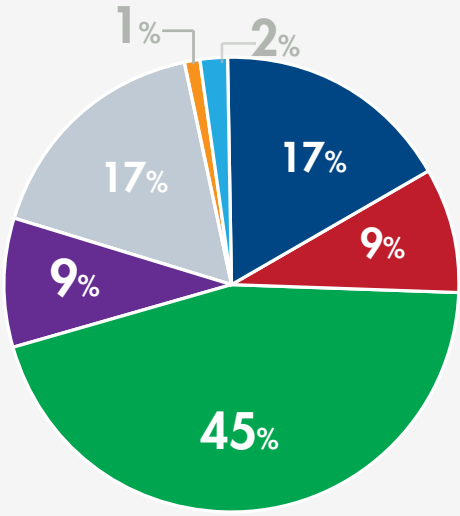
Les techniques de renseignement ne peuvent être mises en œuvre que pour la défense ou la promotion d'une liste limitative d'intérêts fondamentaux de la Nation énoncés à l'article L. 811-3 du code de la sécurité intérieure.

Dans son deuxième rapport d'activité 2017, la commission avait décidé 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. La commission maintiendra cette présentation dans tous ses rapports d'activité.

Par ailleurs, le service de renseignement du « second cercle » relevant du ministère de la justice et chargé du renseignement pénitentiaire peut, en vertu de l'article L. 855-1 du code de la sécurité intérieure, recourir également à une liste limitative de techniques pour des finalités qui lui sont propres, à savoir la prévention des évasions et le maintien de la sécurité et du bon ordre au sein des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues[52]. En 2018, ces finalités ont été invoquées dans 0,04 % des demandes de techniques de renseignement. Dès lors qu'elles ne concernent qu'un seul service et qu'elles sont à ce jour d'un poids marginal, les deux finalités propres au renseignement pénitentiaire ne figurent pas dans le diagramme ci-dessous.

52 - Voir, pour une analyse de ces dispositions légales et de leurs mesures réglementaires d'application, le point 1.3 du deuxième rapport d'activité 2017 de la CNCTR. En même temps que la rédaction du présent rapport, une modification de l'article L. 855-1 du code de la sécurité intérieure a été adoptée par le Parlement à l'article 89 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. Cette modification sera présentée dans le prochain rapport d'activité de la CNCTR.

Les finalités fondant toutes les techniques de renseignement en 2018



- 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 avait montré qu'elle était devenue en janvier 2015 le fondement légal le plus invoqué à l'appui des demandes d'interceptions de sécurité, est demeurée les années suivantes très nettement prédominante lorsque l'on considère les demandes portant sur l'ensemble des techniques de renseignement. Comme en 2017, nonobstant un léger déclin, cette finalité a motivé en 2018 près de 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. Cette dernière finalité a été davantage invoquée en 2018 qu'en 2017, son poids relatif passant de 6 % à 9 %. La CNCTR rappelle, à cet égard, qu'elle se montre particulièrement vigilante sur les demandes fondées sur cette finalité, considérant que la prévention de violences collectives ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, même extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.

2.1.3. Le nombre de personnes surveillées au moyen de techniques de renseignement relevant de la surveillance intérieure : une légère augmentation cohérente avec celle des demandes de techniques

La CNCTR a repris, comme chaque année, l'indicateur qu'elle avait créé à l'occasion de son premier rapport d'activité[53] et a calculé le nombre de personnes ayant fait l'objet, en 2018, 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. Comme les années précédentes, ce chiffre ne comprend pas les accès aux données de connexion en temps différé mentionnés 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[54].

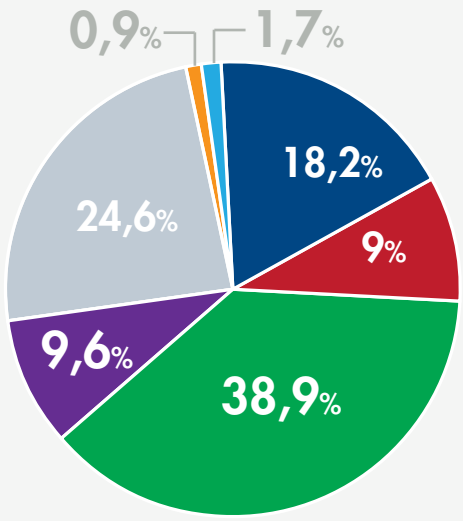
Les éléments de calcul utilisés comportent une marge d'erreur, évaluée à moins de 10 %, dès lors que les demandes tendant à la mise en œuvre de techniques de renseignement sont présentées par technique et non par personne, que le traitement informatisé des demandes n'a pas encore été entièrement harmonisé 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 lors de sa première année de fonctionnement, la fiabilité du calcul a été renforcée.

	2016	2017	2018	Évolution 2017/2018
Nombre de personnes surveillées	20 360	21 386	22 038	+3 %
Dont, au titre de la **prévention du terrorisme**	9 475 (46,5% du total)	9 157 (42,8% du total)	8 574 (38,9% du total)	-6,4 %
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)	5 416 (24,6% du total)	-2 %

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

54 - La CNCTR considère en effet que les identifications d'abonnés et les recensements de numéros d'abonnement constituent moins une mesure de surveillance à proprement parler 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.

La répartition des personnes surveillées selon les finalités motivant leur surveillance en 2018



- 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

Le nombre de personnes surveillées, en augmentation de 3 % en 2018, a connu une évolution du même ordre que celle des demandes de techniques de renseignement. Cette évolution est par ailleurs comparable à celle observée en 2017.

De manière cohérente avec le diagramme 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 39 % en 2018, est nettement majoritaire, devant les quelque 25 % de personnes surveillées au titre de la prévention de la criminalité et de la délinquance organisées.

Les éventuelles différences de valeurs entre les deux diagrammes reflètent le nombre de techniques employées pour surveiller une personne. Si 39 % des personnes surveillées en 2018 l'ont été au titre de la prévention du terrorisme, tandis que 45 % des demandes de techniques de renseignement étaient fondées sur cette finalité, cela signifie que les personnes suspectées d'être impliquées dans un projet terroriste font, en moyenne, l'objet de davantage de techniques que les personnes surveillées sur le fondement d'autres finalités.

2.1.4 Le nombre d'avis préalables rendus par la CNCTR au titre de la surveillance internationale : une nouvelle donnée rendue publique

Mise en place en avril 2016 en application d'un accord informel entre le Premier ministre et la CNCTR[55], la consultation préalable de la commission sur les demandes d'exploitation de communications internationales interceptées, prévues au III de l'article L. 854-2 du code de la sécurité intérieure, a été rendue obligatoire par la loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025[56]. Cette loi, qui a en outre créé au V du même article L. 854-2 une nouvelle autorisation d'exploitation de communications internationales, a également prévu un avis *a priori* de la CNCTR sur les futures demandes présentées en application de ces dispositions.

Les autorisations d'exploitation de communications internationales interceptées prévues au III de l'article L. 854-2 du code de la sécurité intérieure peuvent concerner les communications émises ou reçues au sein d'une zone géographique, par une organisation, par un groupe de personnes ou par une seule personne. La nouvelle autorisation prévue au V du même article ne peut concerner qu'une seule personne et permet l'exploitation de ses communications renvoyant à un identifiant technique rattachable au territoire national, y compris lorsque la personne communique depuis la France. Quelle que soit leur nature, les autorisations d'exploitation ne peuvent être fondées que sur des finalités limitativement prévues par la loi. Ces finalités sont identiques à celles susceptibles de motiver les techniques de renseignement relevant de la surveillance intérieure, c'est-à-dire la défense et la promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure.

55 - Voir le point 2.1.5.1 du premier rapport d'activité 2015/2016 de la CNCTR.

56 - Voir, pour une analyse de cette modification législative, le point 1.1.2 du présent rapport.

Dès lors que la loi prévoit un avis *a priori* de la CNCTR en matière de surveillance des communications électroniques internationales, la commission rend public le nombre de demandes d'autorisation sur lesquelles elle s'est prononcée. Bien que la loi n'ait été modifiée qu'au cours de l'année 2018, la CNCTR a décidé de publier un chiffre couvrant toute l'année, par cohérence avec les éléments statistiques concernant la surveillance intérieure ainsi que pour faciliter les comparaisons avec les années à venir.

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

Les demandes ont porté sur les objets prévus au III de l'article L. 854-2 du code de la sécurité intérieure, zone géographique, organisation, groupe de personnes ou personnes seules. De nombreuses demandes étaient fondées sur plusieurs des finalités mentionnées à l'article L. 811-3 du code de la sécurité intérieure.

2.2 Le maintien d'un rythme élevé de contrôles *a posteriori*, accompagnant des avancées dans le domaine de la centralisation des données recueillies et de la traçabilité de leur exploitation

Dans ses deux premiers rapports d'activité[57], 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, qui lui offrent un accès direct aux données recueillies, voire aux transcriptions et aux extractions réalisées à partir de ces données. La seconde méthode consiste à effectuer des contrôles sur pièces et sur place au sein des services de renseignement.

D'application quotidienne, les contrôles exercés depuis les locaux de la CNCTR peuvent 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 même code), le balisage (article L. 851-5 du même code) et les interceptions de sécurité *via* le GIC (I de l'article L. 852-1 du même code).

Les contrôles sur pièces et sur place au sein des services de renseignement peuvent porter sur l'ensemble des techniques entrant dans le champ de compétence de la commission. Après avoir fortement développé ces contrôles en 2017 grâce aux recrutements venus renforcer le secrétariat

57 - Voir les points 4.1 et 4.2 du premier rapport d'activité 2015/2016 de la CNCTR ainsi que le point 2.2 de son deuxième rapport d'activité 2017.

général de la commission, la CNCTR a maintenu le niveau atteint l'an passé en réalisant plus de 120 contrôles sur pièces et sur place en 2018. Composée de chargés de mission aux compétences tant juridiques que techniques, l'équipe accomplissant les contrôles observe un rythme de deux, parfois trois déplacements par semaine. Un membre du collège de la CNCTR participe, dans la plupart des cas, aux contrôles.

En outre, le président de la CNCTR, généralement accompagné d'un autre membre du collège et d'un chargé de mission, s'est rendu en 2018 dans neuf centres territoriaux relevant du GIC. Ces déplacements sont principalement destinés à rencontrer les chefs de service de renseignement déconcentrés[58], afin de diffuser la doctrine de la commission et de répondre aux interrogations propres à ces services.

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

2.2.1 L'approfondissement des contrôles *a posteriori* : du contrôle du recueil des données à celui de leur exploitation

La CNCTR a décrit, dans son deuxième rapport d'activité[59], la manière dont étaient préparés et accomplis ses contrôles *a posteriori*, en particulier ceux menés sur pièces et sur place au sein des services de renseignement. La commission a fait le choix de se concentrer, dans le présent rapport, sur les résultats et les enseignements des contrôles effectués en 2018.

La CNCTR est, de manière générale, satisfaite des conditions dans lesquelles elle a été accueillie au sein des services de renseignement en 2018. Elle dresse un bilan positif de ses contrôles sur pièces et sur place, qui renforcent la sécurité juridique des activités de renseignement en rendant, pour les services, la doctrine de la CNCTR plus prévisible et en complétant, pour la commission, la compréhension des besoins opérationnels des services.

S'agissant des anomalies constatées, la CNCTR n'a, à une exception près, relevé aucune irrégularité sérieuse lors de ses contrôles *a posteriori* en 2018.

Comme l'année précédente, des anomalies de faible portée ont soit été corrigées au moment de leur détection, soit fait l'objet d'une régularisation dans des délais considérés comme satisfaisants par la commission.

Dans un cas cependant, la CNCTR a estimé nécessaire de procéder de manière plus formelle et de faire usage de son pouvoir de recommander, en application de l'article L. 833-6 du code de la sécurité intérieure, que des renseignements collectés soient détruits, au motif que leur recueil avait méconnu la portée d'une autorisation accordée par le Premier ministre. La CNCTR a en effet constaté qu'une autorisation, destinée à surveiller une personne au sein d'un groupe d'individus, avait été mise en œuvre à l'encontre d'une autre personne. La technique de renseignement avait pris fin mais des données recueillies à l'occasion de sa mise en œuvre étaient conservées par le service concerné.

59 - Voir le point 2.2.1 du deuxième rapport d'activité 2017 de la CNCTR.

L'article L. 833-6 du code de la sécurité intérieure prévoit que la CNCTR peut recommander au service concerné, au ministre dont il relève ou au Premier ministre que la mise en œuvre d'une technique soit interrompue ou des renseignements collectés détruits. En l'espèce, la commission a adressé sa recommandation au service concerné, qui l'a intégralement mise en œuvre en détruisant les données recueillies ainsi que les transcriptions et les extractions réalisées. Compte tenu des circonstances propres à cette affaire, aucune autre mesure n'a paru nécessaire à la CNCTR.

S'agissant, plus généralement, de la portée des contrôles *a posteriori*, la CNCTR, après avoir augmenté le nombre de ces contrôles en 2017, s'est attachée à en approfondir le champ en 2018.

Alors que les contrôles *a posteriori* de l'année 2017 avaient porté en priorité sur le respect des dispositions régissant le recueil et la conservation des données collectées, la commission a souhaité en 2018 renforcer son effort de contrôle sur la phase d'exploitation de ces données, en particulier sur la réalisation, la diffusion et la conservation des transcriptions et des extractions de données. Les renseignements bruts obtenus lors de la mise en œuvre d'une technique de renseignement sont en effet exploités afin d'en tirer les informations pertinentes, susceptibles d'être intégrées dans les documents d'analyse produits par les services de renseignement. Cette exploitation, qui consiste à examiner et à trier les données brutes recueillies, peut prendre la forme d'extractions, lorsqu'une partie de ces données, par exemple une image ou une parole, est prélevée, ou de transcriptions, lorsque des données brutes font l'objet d'une transformation destinée à en faciliter l'analyse, par exemple la mise par écrit de conversations orales.

Les transcriptions et les extractions ne sont pas soumises aux mêmes règles que les données brutes recueillies. Si ces données doivent être détruites au terme de durées de conservation maximales fixées par la loi, les transcriptions et les extractions peuvent, en application de l'article L. 822-3 du code de la sécurité intérieure, être conservées tant qu'elles demeurent indispensables à la poursuite des finalités qui ont motivé leur réalisation. Ces finalités ne peuvent être que la défense ou la promotion des intérêts fondamentaux de la Nation pouvant justifier le recours à des techniques de renseignement et limitativement énumérés à l'article L. 811-3 du même code.

Comme la collecte de données brutes, la réalisation de transcriptions et d'extractions est soumise au contrôle de la CNCTR, en vertu de l'article L. 822-3 du code de la sécurité intérieure. La commission doit s'assurer notamment que ces opérations n'ont d'autres finalités que celles prévues par l'autorisation concernée.

Pour accomplir ses missions, la CNCTR dispose, en vertu du 2° de l'article L. 833-2 du code de la sécurité intérieure, d'un accès permanent, complet, direct et, pour certaines techniques[60], immédiat aux relevés, registres, renseignements collectés, transcriptions et extractions. Cet accès est garanti par la loi, où que ces éléments se trouvent.

Le président de la commission a adressé un courrier à tous les chefs de service, rappelant les dispositions légales et annonçant l'approfondissement du contrôle *a posteriori*. La CNCTR a en outre dialogué informellement avec les services de renseignement, notamment au cours de contrôles *a posteriori*, afin de préciser les modalités de son contrôle sur les transcriptions et les extractions.

En pratique, la CNCTR a demandé aux services contrôlés de répertorier, pour des dossiers qu'elle avait prévu d'aborder lors de contrôles *a posteriori*, toutes les transcriptions et les extractions réalisées à partir de données recueillies au moyen de techniques de renseignement. Ce recensement devait faire apparaître tous les lieux de conservation de ces transcriptions et extractions et indiquer les entités ou les agents disposant d'accès aux informations ainsi que les modalités de traçabilité de ces accès. La CNCTR a compétence, en vertu de l'article L. 833-2 du code de la sécurité intérieure évoqué ci-dessus, pour consulter les transcriptions et les extractions, où qu'elles soient conservées par les services de renseignement, et apprécier la nécessité de leur conservation.

Dans l'hypothèse où un service refuserait que la CNCTR accède à certains lieux, physiques ou logiciels, de conservation des transcriptions et des extractions, l'article L. 833-2 du code de la sécurité intérieure permettrait à la commission de solliciter formellement ces éléments du Premier ministre, à l'exclusion de ceux qui pourraient donner connaissance à la commission, directement ou indirectement, de l'identité des sources des services de

60 - Voir l'introduction du point 2.2 du présent rapport d'activité.

renseignement. L'article L. 833-3 du code punit d'un an d'emprisonnement et de 15 000 d'amende le fait d'entraver l'action de la commission en refusant de lui communiquer les documents qu'elle a sollicités en application de l'article L. 833-2, en dissimulant ces documents ou en les faisant disparaître.

Le contrôle *a posteriori* de « l'exception hertzienne »

Lorsque le législateur a redéfini, à la fin de l'année 2017, le régime juridique des mesures permettant de surveiller les communications empruntant exclusivement la voie hertzienne[61], il a réduit à une portée résiduelle « l'exception hertzienne », c'est-à-dire la surveillance pouvant s'exercer en vertu de la loi sans autorisation préalable du Premier ministre ni avis *a priori* de la CNCTR. Prévue aux articles L. 855-1 A à L. 855-1 C du code de la sécurité intérieure, « l'exception hertzienne » ne concerne plus que les communications échangées sur des réseaux hertziens ouverts, écoutables par toute personne qui règle un appareil de réception sur la fréquence utilisée.

La loi a confié à la CNCTR une mission de contrôle *a posteriori* sur les mesures prises dans le cadre de « l'exception hertzienne ». Si ces mesures ne portent pas en elles-mêmes atteinte à la vie privée, dès lors que les communications sont échangées au sein de réseaux ouverts, certains dispositifs d'interception utilisés peuvent également servir à mettre en œuvre des techniques de renseignement soumises à autorisation du Premier ministre après avis de la CNCTR. Le contrôle *a posteriori* a donc pour but de vérifier que les mesures prises dans le cadre de « l'exception hertzienne » relèvent effectivement de ce seul cadre et que les champs d'application respectifs des dispositions régissant l'emploi de techniques de renseignement et de celles prévoyant « l'exception hertzienne » ont été respectés.

En 2018, la CNCTR a effectué ses premiers contrôles *a posteriori* sur pièces et sur place dans les locaux des services de renseignement utilisant « l'exception hertzienne ». Elle s'est fait présenter les capacités d'interception et a pu consulter les transcriptions et les extractions réalisées à partir des données recueillies. La CNCTR n'a pas détecté d'irrégularité lors de ces contrôles.

61 - Voir, pour une présentation détaillée de la réforme, le point 1.2 du deuxième rapport d'activité 2017 de la CNCTR.

2.2.2 La centralisation des données recueillies et la traçabilité de leur exploitation : un chantier inscrit dans la durée qui a connu de notables avancées en 2018

Deux exigences légales[62], distinctes mais liées, 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. Sont concernés aussi bien les données recueillies au moyen de techniques relevant de la surveillance intérieure que celles interceptées au titre de la surveillance des communications électroniques internationales.

Dans la continuité de ses observations en 2017, la CNCTR a constaté en 2018 que la centralisation des renseignements collectés s'était améliorée, même si l'organisation définitive n'a pas encore été atteinte. De même, la traçabilité de l'exploitation de ces renseignements, en progrès, demeure subordonnée à des développements informatiques en cours.

En ce qui concerne la centralisation des données recueillies, la CNCTR rappelle que, pour que la commission puisse réellement disposer, comme la loi le prévoit[63], 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 est indispensable.

En 2017, la CNCTR avait indiqué que les progrès à accomplir en matière de centralisation des données recueillies concernaient 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 même code), enfin le recueil et la captation de données informatiques (article L. 853-2 du même code). Pour ces techniques caractérisées par une collecte décentralisée du renseignement, les modalités de stockage des données recueillies demeuraient disparates.

---

62 - Voir, pour un rappel du cadre légal à ce sujet, le point 2.2.2 du deuxième rapport d'activité 2017 de la CNCTR.
63 - Voir notamment les articles L. 833-2 et L. 854-9 du code de la sécurité intérieure.

En 2018, certains services de renseignement ont avancé de manière significative dans la construction de dispositifs permettant la centralisation des renseignements au niveau de leur administration centrale, en particulier dans le développement d'applications informatiques unifiées et cohérentes pour conserver et traiter les données.

Un stockage décentralisé subsiste cependant au sein d'échelons territoriaux de certains services, faute de pouvoir concevoir et financer un réseau informatique susceptible d'acheminer de manière sûre des données volumineuses. La CNCTR a donc mené en 2018, comme l'année précédente, plusieurs contrôles sur pièces et sur place dans des unités territoriales des services de renseignement.

Pour proposer une solution à ces difficultés, le GIC a poursuivi, en 2018, la construction d'un dispositif technique permettant à tous les services de renseignement[64] 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 ainsi que, à terme, les données informatiques captées ou recueillies sur le fondement de l'article L. 853-2 du même code. Le dispositif mis en place par le GIC permettra également d'exploiter dans ses centres territoriaux les renseignements collectés.

En 2017, le GIC avait défini les modalités de la centralisation des paroles et des images captées sur le fondement de l'article L. 853-1 du code de la sécurité intérieure. En 2018, le GIC a commencé à déployer, à titre expérimental, son dispositif pour la captation de paroles. Trois services de renseignement ont participé à cette expérimentation, étendue en fin d'année à la captation d'images. Le système pourrait être généralisé à tous les services de renseignement concernés en 2019. La CNCTR disposera alors d'un accès permanent, complet, direct et immédiat non seulement aux renseignements recueillis mais aussi aux transcriptions et aux extractions réalisées.

64 - 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.

En ce qui concerne la traçabilité de l'exploitation des données, la CNCTR relève que l'évolution positive observée en 2017 s'est poursuivie en 2018.

D'une part, la CNCTR a constaté à nouveau des améliorations dans la rédaction des « fiches de traçabilité », c'est-à-dire des relevés de mise en œuvre que les services de renseignement doivent établir, en application de l'article L. 822-1 du code de la sécurité intérieure, pour chaque technique autorisée, en mentionnant les dates de début et de fin de mise en œuvre ainsi que la nature des renseignements collectés.

Pour remplir sa mission de contrôle *a posteriori*, la CNCTR estime nécessaire que les « fiches de traçabilité » soient rédigées dès la fin de la mise en œuvre d'une technique ou, en l'absence de mise en œuvre, dès l'arrivée à échéance de l'autorisation. Grâce aux applications mises à sa disposition par le GIC, la commission peut vérifier de façon immédiate l'existence et le contenu des relevés de mise en œuvre, qui contribuent à la préparation des contrôles sur pièces et sur place au sein des services de renseignement mais peuvent être aussi l'occasion d'échanges quotidiens entre la commission et les services destinés à préciser l'état d'une technique.

D'autre part, le chantier consistant à construire des dispositifs informatiques assurant la traçabilité des consultations, transcriptions et extractions des données recueillies a connu des évolutions inégales selon les services de renseignement. Plusieurs services ont développé des outils de traçabilité ambitieux, qui accroissent les possibilités de contrôle de la commission. À cet égard, la traçabilité des mesures de surveillance des communications électroniques internationales a progressé de manière particulièrement significative en 2018. Dans d'autres services, le contrôle informatisé des consultations, transcriptions et extractions de données recueillies demeure à bâtir.

2.2.3 Les recours contre la mise en œuvre des techniques de renseignement : des évolutions contrastées entre les réclamations administratives devant la CNCTR et les recours contentieux devant le Conseil d'État

2.2.3.1 Une baisse du nombre de réclamations adressées à la CNCTR

Toute personne peut saisir la CNCTR, conformément à l'article L. 833-4 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.

Pour des motifs de sécurité nationale, la CNCTR ne peut, par exception au droit de saisir l'administration par voie électronique, être valablement saisie que par un courrier postal[65]. La réclamation doit être présentée par la personne concernée, justifiant de son identité, et mentionner, le cas échéant, les éléments techniques à partir desquels la personne souhaite que les vérifications soient conduites. Ces éléments techniques, notamment des numéros de téléphone ou des adresses de messagerie électronique, doivent être assortis de justificatifs, par exemple un contrat d'abonnement ou une facture. Les vérifications ne peuvent avoir lieu que lorsque l'ensemble de ces informations et justificatifs ont été communiqués à la commission.

La CNCTR instruit les réclamations qui lui sont adressées de la même manière et en utilisant les mêmes outils que lorsqu'elle effectue un contrôle *a posteriori* de sa propre initiative.

65 - Voir l'annexe 1 au décret n° 2015-1405 du 5 novembre 2015 relatif aux exceptions à l'application du droit des usagers de saisir l'administration par voie électronique, prises sur le fondement de l'article 4 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Le nombre de réclamations reçues par la CNCTR en 2018 est en baisse par rapport à 2017.

	2016	2017	2018
Nombre de réclamations reçues par la CNCTR	**49**	**54**	**30**

Quatre des réclamations reçues en 2018 ont été présentées par des personnes ayant déjà saisi la CNCTR les années précédentes et souhaitant que des vérifications soient à nouveau conduites à leur sujet.

Le délai de réponse aux réclamations contenant toutes les informations nécessaires à leur traitement a été inférieur à deux mois.

Aucune réclamation n'a conduit la CNCTR à envoyer de 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 même 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 2018, 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 d'application depuis l'entrée en vigueur du cadre légal en 2015.

2.2.3.2 Une légère augmentation 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'une technique de renseignement n'est ou n'a pas 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.

S'agissant des techniques de renseignement relevant de la surveillance intérieure, 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.

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, sauf s'il s'agit de vérifier la légalité de l'exploitation des communications de personnes utilisant des identifiants rattachables au territoire national et communiquant depuis la France. Dans ce dernier cas, toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR peut saisir le Conseil d'État, sur le fondement de l'article L. 854-9 du code de la sécurité intérieure[66].

En 2016 et 2017, le Conseil d'État avait respectivement été saisi de 9 et 6 requêtes concernant la mise en œuvre de techniques de renseignement. 6 décisions avaient été rendues en 2016 et 3 en 2017. En 2018, 9 requêtes ont été enregistrées. Le Conseil d'État a par ailleurs rendu 9 décisions ainsi qu'une ordonnance d'irrecevabilité dans une procédure en référé. Au 31 décembre 2018, 5 affaires demeuraient en instance.

66 - Voir, pour une analyse plus détaillée de cette voie de recours et de ses évolutions recommandées par la CNCTR, les points 1.1.2 et 1.2.1 du présent rapport.

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

La CNCTR ne s'est pas trouvée dans la situation d'exercer elle-même un recours contentieux devant le Conseil d'État sur le fondement des articles L. 833-8 ou L. 854-9 du code de la sécurité intérieure. Cette voie de recours est ouverte au président de la commission ou à trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission. En 2018, le Premier ministre a suivi tous les avis *a priori* défavorables émis par la CNCTR et les contrôles *a posteriori* effectués par la commission n'ont pas révélé d'irrégularité justifiant l'envoi d'une recommandation au Premier ministre.

Pour la première fois depuis l'entrée en vigueur du cadre légal, le Conseil d'État s'est prononcé, en 2018, sur une question préjudicielle prévue à l'article L. 841-1 du code de la sécurité intérieure. Aux termes de cet article, « *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* ».

Saisi d'une plainte pour atteinte à la vie privée, fondée sur l'éventuelle mise en œuvre d'une technique de renseignement à l'encontre du plaignant, le procureur de la République près un tribunal de grande instance a demandé au Conseil d'État de vérifier la régularité de la technique de renseignement mentionnée dans la plainte. La CNCTR, à laquelle le Conseil d'État avait transmis la question préjudicielle, a effectué des vérifications. Au vu de ces vérifications ainsi que des éléments fournis par le Premier ministre, le juge administratif a répondu au procureur de la République, « *que la vérification qu'il [avait] sollicitée [avait] été effectuée et que l'examen de la technique de renseignement sur laquelle il [avait] saisi le Conseil d'État n'[avait] révélé aucune illégalité* »[67].

67 - Voir la décision du Conseil d'État du 18 juin 2018 n° 420739, reproduite en annexe n° 6 au présent rapport, notamment ses paragraphes n° 4 et n° 5.

Par ailleurs, dans une décision du 20 juin 2018, le Conseil d'État, saisi de conclusions tendant à l'annulation des décisions nommant les membres de la CNCTR, a jugé que cette demande d'annulation était en tout état de cause tardive et, partant, irrecevable, dès lors qu'elle était présentée en 2018 contre des décisions publiées au Journal officiel de la République française le 2 octobre 2015. Le Conseil d'État a, en outre, jugé qu'une personne ne saurait utilement invoquer l'illégalité dont serait entachée la nomination des membres de la CNCTR à l'occasion d'un recours tendant à vérifier qu'aucune technique de renseignement n'a été irrégulièrement mise en œuvre à son égard[68].

Les questions préjudicielles posées par le Conseil d'État à la Cour de justice de l'Union européenne

Par deux décisions du 26 juillet 2018, le Conseil d'État a adressé plusieurs questions préjudicielles à la Cour de justice de l'Union européenne (CJUE) dans le cadre de recours dirigés contre plusieurs actes réglementaires applicables aux activités de renseignement. Dans un premier cas, les dispositions contestées sont celles définissant les données de connexion que doivent conserver pendant un an, de manière généralisée, les opérateurs de communications électroniques ou les fournisseurs de services au public en ligne[69]. Dans un second cas, les dispositions contestées sont celles de quatre décrets pris pour l'application de la loi du 24 juillet 2015 relative au renseignement[70].

68 - Voir la décision du Conseil d'État du 20 juin 2018 n° 412685, reproduite en annexe n° 7 au présent rapport, notamment ses paragraphes n° 5 et n° 7.

69 - Il s'agit de l'article R. 10-13 du code des postes et des communications électroniques ainsi que du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

70 - Il s'agit du décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, du décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État, du décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4, enfin du décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

Les questions préjudicielles portent sur les conséquences à tirer de l'arrêt du 21 décembre 2016, dit *Tele2 Sverige AB*, dans lequel la CJUE a jugé que le droit de l'Union européenne s'opposait notamment « *à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* ». La cour a également jugé que le droit de l'Union européenne s'opposait à « *l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union* »[71].

Par ses questions préjudicielles, le Conseil d'État a demandé à la CJUE de préciser sa jurisprudence sur plusieurs points.

En premier lieu, en ce qui concerne la conservation généralisée des données de connexion par les opérateurs de communications électroniques et les fournisseurs de services au public en ligne, le Conseil d'État a tout d'abord jugé que « *le fait que l'obligation de conservation (...) revête un caractère général sans être limitée à des personnes ou circonstances particulières n'est pas, par lui-même, contraire aux exigences découlant des stipulations de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* ». Le Conseil d'État a ensuite indiqué qu'une « *telle conservation présente (...) une utilité sans équivalent pour la recherche, la constatation et la poursuite des infractions pénales* » et qu'elle « *n'est pas de nature* », selon les propres termes de la CJUE dans son arrêt *Tele2 Sverige AB*, « *à porter atteinte au "contenu essentiel"* » du droit au respect de la vie privée, « *dès lors qu'elle ne révèle pas le contenu d'une communication* ». Dès lors, le Conseil d'État a demandé à la CJUE si cette conservation ne devait pas être regardée, « *notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté*

71 - 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 et autres), notamment les articles 1er et 2 du dispositif.

garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres »[72].

En second lieu, en ce qui concerne la mise en œuvre des techniques de renseignement, le Conseil d'État a tout d'abord jugé que le droit de l'Union européenne interprété par l'arrêt *Tele2 Sverige AB* de la CJUE ne concernait que les recueils de données de connexion imposant des obligations spécifiques aux opérateurs de communications électroniques ou aux fournisseurs de services au public en ligne, à savoir 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 même code), la mise en œuvre d'algorithmes sur des données de connexion à la seule fin de détecter des menaces terroristes (article L. 851-3 du même code) et la géolocalisation en temps réel (article L. 851-4 du même code).

À propos de ces techniques, le Conseil d'État :

- a relevé que la conservation généralisée de données de connexion par les opérateurs de communications électroniques ou les fournisseurs de services au public en ligne présentait, « *dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, (...) une utilité sans équivalent par rapport au recueil de ces mêmes données à partir seulement du moment où l'individu en cause aurait été identifié comme susceptible de présenter une menace pour la sécurité publique, la défense ou la sûreté de l'État* ». Dès lors, le Conseil d'État a posé à la CJUE la même question que celle mentionnée plus haut concernant la conservation généralisée de données de connexion ;

- a constaté que le recueil de données de connexion en temps réel et la mise en œuvre d'algorithmes sur des données de connexion à la seule fin de détecter des menaces terroristes présentaient, « *dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, (...) une utilité*

72 - Voir la décision du Conseil d'État du 26 juillet 2018 n° 393099, reproduite en annexe n° 8 au présent rapport.

opérationnelle sans équivalent ». Dès lors, le Conseil d'État a demandé à la CJUE si le droit de l'Union européenne ne devait pas être interprété comme autorisant des mesures législatives prévoyant ces techniques de renseignement ;

- a noté que la CJUE, dans la motivation de son arrêt *Tele2 Sverige AB*, avait estimé « *que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé* » devaient en informer « *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* ». Dès lors, le Conseil d'État a demandé à la CJUE si le droit de l'Union européenne subordonnait « *dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou si de telles procédures peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours* »[73].

La CJUE ne s'était pas prononcée sur ces questions préjudicielles à la date de rédaction du présent rapport.

73 - Voir la décision du Conseil d'État du 26 juillet 2018 n° 394922, reproduite en annexe n° 9 au présent rapport.

2.2.4 Le dialogue institutionnel avec le Parlement, l'information du public et les relations internationales : une année riche d'initiatives et de rencontres

Au sein de la chaîne opérationnelle conduisant au recueil et à l'exploitation du renseignement, la CNCTR se voit confier par la loi une mission de contrôle qui ne peut, en application du principe de la séparation des pouvoirs et eu égard aux exigences du secret de la défense nationale, être accomplie que par un organisme distinct non seulement du Gouvernement mais également du Parlement et du public. La CNCTR se conçoit dès lors comme un « tiers de confiance », auquel le législateur a attribué une compétence spécialisée qu'il ne peut assurer directement. En retour, la CNCTR rend compte tout au long de l'année de ses activités au Parlement et au public, dans le respect du secret de la défense nationale qui couvre ses travaux en vertu de l'article L. 832-5 du code de la sécurité intérieure.

Par ailleurs, la CNCTR conduit une action internationale destinée à faire connaître le cadre légal français applicable aux activités de renseignement ainsi qu'à recueillir les bonnes pratiques auprès de partenaires étrangers.

Dans le cadre du dialogue institutionnel avec le Parlement, le président de la CNCTR a été auditionné en janvier et en décembre 2018 par la délégation parlementaire au renseignement.

Invité par la rapporteuse de la commission des lois de l'Assemblée nationale à l'occasion des débats sur le projet de loi relative à la protection des données personnelles, il a rappelé l'étendue du contrôle confié à la commission par la loi en la matière.

En mai et en juin 2018, le président de la CNCTR a été reçu par le président du Sénat et par le président de l'Assemblée nationale afin de leur présenter le deuxième rapport d'activité de la commission pour l'année 2017.

Auditionné en septembre 2018 par le président et par le rapporteur de la mission d'information de l'Assemblée nationale relative aux fichiers mis à la disposition des forces de sécurité, il a présenté les différentes modalités d'exercice par la commission de son contrôle *a posteriori* sur la mise en œuvre des techniques de renseignement.

Lors de l'examen du projet de loi de règlement du budget et d'approbation des comptes de l'année 2017, le président de la CNCTR a été entendu par la rapporteuse spéciale de la commission des finances de l'Assemblée nationale. Lors de l'examen au Sénat du projet de loi de finances pour l'année 2019, il a répondu aux demandes d'information du rapporteur de la commission des lois saisie pour avis concernant les moyens alloués à la commission pour remplir ses missions.

Pour promouvoir l'information du public, la CNCTR et la section du rapport et des études du Conseil d'État ont organisé conjointement le 6 avril 2018 un colloque intitulé « *Le renseignement et son contrôle* », en présence notamment de parlementaires, de représentants d'autorités administratives indépendantes françaises et d'autorités étrangères de contrôle du renseignement, de magistrats, d'avocats, d'universitaires, de journalistes et de représentants d'associations spécialisées dans la protection des libertés. Ce colloque a permis de dresser un bilan des activités de contrôle du renseignement par des autorités administratives, juridictionnelles et parlementaires à partir de l'exemple français et d'autres expériences européennes.

Le président de la CNCTR a, par ailleurs, été entendu en juillet 2018 par l'assemblée plénière de la Commission nationale consultative des droits de l'homme (CNCDH). Il y a présenté le cadre dans lequel sont contrôlées les activités des services de renseignement depuis l'entrée en vigueur du régime juridique de 2015 et le bilan que la CNCTR tire de ses premières années de fonctionnement à la lumière des normes nationales, européennes et internationales qui protègent le respect du droit à la vie privée.

S'agissant des relations internationales, la CNCTR s'est déplacée à Londres en février 2018 pour y rencontrer des institutions chargées de contrôler les services de renseignement britanniques, l'*Investigatory Powers Commissioner* et le président de l'*Intelligence and Security Committee of Parliament*.

Elle a rencontré à Paris en mai 2018 la rapporteuse spéciale des Nations unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste.

En septembre 2018, la CNCTR s'est rendue à Stockholm pour s'entretenir avec la présidente de la commission de contrôle suédoise, dénommée *Säkerhets- och integritetsskyddsnämnden*.

Elle a accueilli à Paris en octobre 2018 une délégation roumaine de la commission parlementaire de contrôle, la *Comisia comună permanentă a Camerei Deputaților și Senatului pentru exercitarea controlului parlamentar asupra activității SRI*.

Un représentant de la CNCTR a participé à une conférence sur le contrôle du renseignement, organisée à Malte en novembre 2018 par le rapporteur spécial des Nations unies sur le droit à la vie privée.

La conférence européenne des autorités nationales de contrôle

Le 7 décembre 2018, la CNCTR et l'institution belge chargée de contrôler les services de renseignement, le *Comité permanent de contrôle des services de renseignement et de sécurité*, ont organisé conjointement une conférence européenne des autorités nationales de contrôle du renseignement.

La conférence a réuni à Paris des représentants d'organes de contrôle administratifs ou judiciaires exerçant des missions et disposant de compétences comparables. Étaient présents des représentants d'autorités issues de quatorze pays européens : Allemagne, Autriche, Belgique, Danemark, France, Grèce, Italie, Luxembourg, Norvège, Pays-Bas, Portugal, Royaume-Uni, Suède et Suisse.

Cette conférence multilatérale, la première de cette nature depuis l'entrée en fonctions de la CNCTR, a permis à chaque délégation, à travers quatre ateliers thématiques, de présenter le cadre de son action et d'échanger sur les bonnes pratiques mises en œuvre. Les débats ont fait apparaître la diversité des régimes juridiques applicables en Europe, nonobstant des principes communs tels que ceux issus de la jurisprudence de la Cour européenne des droits de l'homme.

Une nouvelle conférence, destinée à prolonger les travaux de cette première rencontre, se tiendra aux Pays-Bas en décembre 2019.

Étude

Éléments de jurisprudence européenne sur le droit au respect de la vie privée en matière de renseignement[74]

Le recueil de renseignements destinés à défendre ou à promouvoir les intérêts fondamentaux des États participe de l'exercice de leur souveraineté nationale. Aussi l'édiction de règles juridiques contraignantes en la matière relève-t-elle essentiellement de la compétence des États. Les pays du continent européen sont cependant, pour la plupart, parties à des ordres juridiques supranationaux particulièrement intégrés dont les principes trouvent à s'appliquer y compris en matière de renseignement.

Dans le cadre du Conseil de l'Europe, d'une part, a été adoptée en 1950 la convention de sauvegarde des droits de l'homme et des libertés fondamentales, qui énonce un ensemble de droits et de libertés et institue une juridiction, la Cour européenne des droits de l'homme (CEDH), pour préciser leur portée et veiller à leur respect par les États parties à la convention. Parmi ces droits figurent celui de toute personne au respect de sa vie privée et familiale, de son domicile et de sa correspondance, stipulé à l'article 8 de la convention. Or les activités des services de renseignement sont, par définition, susceptibles de porter atteinte à la vie privée. Depuis plusieurs décennies, la CEDH a eu ainsi l'occasion de se prononcer sur la conformité à la convention de législations nationales prévoyant et encadrant le recueil de renseignements.

Dans le cadre de l'Union européenne, d'autre part, a été adoptée en 2000 la Charte des droits fondamentaux de l'Union européenne, qui énonce des droits et des libertés proches de ceux protégés par les instruments juridiques du Conseil de

74 - Cette étude a été rédigée avec le concours de madame Katia BOUSLIMANI, doctorante en section droit public à l'université Grenoble-Alpes.

l'Europe. Ce sont notamment, à ses articles 7 et 8, le droit de toute personne au respect de sa vie privée et familiale, de son domicile et de ses communications ainsi que le droit de toute personne à la protection des données à caractère personnel la concernant. Ces droits et libertés, qui n'ont vocation qu'à régir les situations dans lesquelles est mis en œuvre le droit de l'Union européenne, ont été récemment invoqués par la Cour de justice de l'Union européenne (CJUE) dans des affaires ayant des incidences en matière de recueil de renseignements.

À partir de l'exemple du droit au respect de la vie privée, dont la conciliation avec les besoins de la sécurité nationale et de la prévention des infractions constitue l'enjeu essentiel de l'encadrement juridique des activités de renseignement, l'objet de la présente étude est de rappeler quelques éléments de jurisprudence de la CEDH et de la CJUE sur le recours à des mesures de surveillance, en analysant la portée des principes applicables et la marge de manœuvre que les deux cours reconnaissent aux États pour les garantir.

1. La CEDH examine, en s'appuyant sur de multiples critères d'analyse, les garanties d'ensemble présentées par un cadre juridique régissant des activités de renseignement

L'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, qui énonce le droit de toute personne au respect de sa vie privée et familiale, de son domicile et de sa correspondance, prévoit qu'une autorité publique ne peut porter atteinte à ce droit « *que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

Ces stipulations, selon lesquelles il ne peut être porté atteinte à un droit que si cette atteinte est légalement encadrée, sont applicables aux activités de renseignement, nonobstant leur caractère secret. Les mesures de surveillance utilisées par les services de renseignement doivent donc respecter la règle de droit, qui peut seulement être aménagée pour tenir compte des conditions particulières dans lesquelles une telle surveillance est mise en œuvre.

En application de ces principes, le recueil de renseignements doit s'effectuer sur le fondement d'une base légale et ne s'appuyer que sur des mesures nécessaires, notamment du fait de leur caractère proportionné. La jurisprudence de la CEDH a précisé ces notions en les appliquant à différentes mesures de surveillance mises en œuvre à l'encontre de personnes, telles que des interceptions de contenus de communications, des accès à des données de connexion ou des géolocalisations.

1.1 L'atteinte à la vie privée doit être prévue par une loi suffisamment accessible, prévisible et limitative

Selon la CEDH, les mots « prévue par la loi », à l'article 8 de la convention, «*signifient que la mesure litigieuse doit avoir une base en droit interne*»[75].

La CEDH a appliqué aux mesures de surveillance des personnes sa conception élargie de la notion de loi, qui ne doit pas nécessairement être un acte adopté par un Parlement. La cour « *a toujours entendu le terme "loi" dans son acception "matérielle" et non "formelle" ; elle y a inclus à la fois des textes de rang infra-législatif (...) et le "droit non écrit"*, comme la « *common law* » de certains systèmes juridiques anglo-saxons[76]. De plus, la CEDH tient compte de la jurisprudence des juridictions nationales, dont elle souligne le rôle parfois « *considérable (...), à telle enseigne que des branches entières du droit positif y résultent, dans une large mesure, des décisions des cours et tribunaux* »[77]. Pour la CEDH, la loi « *est donc le texte en vigueur tel que les juridictions compétentes l'ont interprété en ayant égard, au besoin, à des données techniques nouvelles, et la Cour ne saurait mettre en question l'interprétation des cours et tribunaux nationaux sauf en cas d'inobservation flagrante, ou d'application arbitraire, de la législation interne pertinente* »[78].

La loi, au sens de la CEDH, doit assurer « *la prééminence du droit* », concept voisin de celui d'État de droit, ce qui implique tout d'abord que la règle de droit soit « *accessible à la personne concernée et prévisible quant à ses effets* »[79].

75 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 228.

76 - Voir l'arrêt de la CEDH du 24 avril 1990, n° 11105/84, affaire Huvig contre France, notamment le paragraphe n° 28. Pour mémoire, cet arrêt concernait des écoutes judiciaires et non une surveillance administrative par des services de renseignement.

77 - Voir l'arrêt de la CEDH du 24 avril 1990, n° 11105/84, affaire Huvig contre France, notamment le paragraphe n° 28.

78 - Voir la décision d'irrecevabilité de la CEDH du 29 juin 2006, n° 54934/00, affaire Weber et Saravia contre Allemagne, notamment le paragraphe n° 90.

79 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 228.

L'accessibilité tient essentiellement à la publicité de la règle[80], la possibilité de surveiller secrètement une personne ne signifiant pas que la base légale de la surveillance puisse elle-même être secrète. La CEDH relève désormais fréquemment le fait que les textes applicables en matière de renseignement sont disponibles en ligne[81]. Elle a admis, tout en la regrettant, une publication dans un bulletin ministériel diffusé uniquement par abonnement, dès lors qu'une base juridique en ligne, bien que privée, permettait au grand public d'accéder aux dispositions concernées[82].

La prévisibilité, en matière de renseignement, prend un sens particulier. La CEDH a ainsi jugé que « *dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence* ». En revanche, « *la loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes* »[83]. Est, à cet égard, suffisamment claire une loi qui se réfère, sans le détailler, au concept de sécurité nationale pour fonder des mesures de surveillance, dès lors que le texte même de la convention mentionne ce concept et que « *par la force des choses, des menaces dirigées contre la sécurité nationale peuvent être de différentes natures et peuvent être imprévues et difficiles à définir à l'avance* »[84]. De même, lorsque la loi prévoit le recours à des

80 - Voir l'arrêt de la CEDH du 26 mars 1987, n° 9248/81, affaire Leander contre Suède, notamment le paragraphe n° 54.

81 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 157.

82 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 242.

83 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 229.

84 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 159. La CEDH examine toutefois la manière dont la notion est généralement interprétée en droit national. Elle a ainsi critiqué *« la possibilité d'intercepter les communications, téléphoniques ou autres, après réception d'informations sur des faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Russie »* alors que *« la nature des faits ou activités pouvant passer pour mettre en péril ces types d'intérêts en matière de sécurité n'est définie nulle part dans le droit russe »* (voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 246).

mesures de surveillance pour prévenir des infractions, il ne s'agit pas, en l'espèce, pour les États d'énumérer exhaustivement toutes les infractions qui peuvent justifier des mesures de surveillance, mais de « *fournir des précisions suffisantes sur la nature des infractions en question* »[85].

La prééminence du droit signifie, en outre, que la loi ne peut se borner à prévoir des mesures de surveillance mais doit également fixer les limites de leur usage. Selon les termes de la CEDH, les stipulations de l'article 8 de la convention seraient méconnues « *si le pouvoir d'appréciation accordé à l'exécutif ou à un juge ne connaissait pas de limites* ». En conséquence, la règle de droit « *doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire* »[86].

En application de ce principe, la cour a progressivement dégagé les six « *garanties minimales (...) contre les abus de pouvoir que la loi doit renfermer* » lorsque sont notamment en cause des interceptions de communications par des services de renseignement :

- « *la nature des infractions susceptibles de donner lieu à un mandat d'interception* »,
- « *la définition des catégories de personnes susceptibles d'être mises sur écoute* »,
- « *la fixation d'une limite à la durée d'exécution de la mesure* »,
- « *la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies* »,
- « *les précautions à prendre pour la communication des données à d'autres parties* »,
- « *les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements* »[87].

85 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 159.

86 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 230.

87 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 231.

1.2 L'atteinte à la vie privée doit constituer une ingérence nécessaire dans une société démocratique car proportionnée et entourée de garanties

Selon la CEDH, une mesure de surveillance doit, comme toute atteinte au droit au respect de la vie privée, être nécessaire au sein d'une société démocratique, au sens de l'article 8 de la convention.

La cour a précisé à cet égard que :

- « *l'adjectif "nécessaire" n'est pas synonyme d'"indispensable", mais n'a pas non plus la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun"* » ;
- « *les États contractants jouissent d'une certaine marge d'appréciation - non illimitée - en matière de recours à des restrictions, mais la décision finale sur la compatibilité de celles-ci avec la Convention appartient à la Cour* » ;
- « *"nécessaire dans une société démocratique" signifie que pour se concilier avec la Convention, l'ingérence doit notamment correspondre à un "besoin social impérieux" et être "proportionnée au but légitime poursuivi"* »[88].

En matière de renseignement, la CEDH apprécie tout d'abord la nécessité des mesures de surveillance au regard du contexte sécuritaire. Dès les années 1970, la cour a estimé, par exemple, que « *les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire* »[89].

88 - Voir l'arrêt de la CEDH du 25 mars 1983, n° 5947/72, affaire Silver et autres contre Royaume-Uni, notamment le paragraphe n° 97.

89 - Voir l'arrêt de la CEDH du 6 septembre 1978, n° 5029/71, affaire Klass et autres contre Allemagne, notamment le paragraphe n° 48.

La CEDH examine ensuite si les motifs prévus par la loi pour recourir à des mesures de surveillance ont notamment pour but la « *sécurité nationale* », la « *sûreté publique* », le « *bien-être économique du pays* », la « *défense de l'ordre* » et la « *prévention des infractions pénales* », comme l'énonce l'article 8 de la convention[90].

Enfin, la CEDH contrôle la proportionnalité du cadre légal applicable aux activités de renseignement, en examinant la manière dont les autorités nationales « *mettent en balance l'intérêt de l'État défendeur à protéger la sécurité nationale au moyen de mesures de surveillance secrète, d'une part, et la gravité de l'ingérence dans l'exercice par un requérant du droit au respect de la vie privée, d'autre part* »[91].

La CEDH reconnaît aux États « *un certain pouvoir discrétionnaire* » et se refuse à « *substituer à l'appréciation des autorités nationales une autre appréciation de ce que pourrait être la meilleure politique* » dans le domaine du renseignement[92]. Elle considère cependant que la marge d'appréciation des États « *est d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre "intime" qui lui sont reconnus* », ce qui est le cas notamment de la protection des données à caractère personnel[93].

La marge d'appréciation reconnue aux États conduit la cour à admettre la compatibilité avec la convention de mesures de surveillance ciblées comme de régimes d'interception massive de communications. Le caractère massif d'une interception ne viole pas en lui-même le droit au respect de la vie privée[94].

90 - Voir la décision d'irrecevabilité de la CEDH du 29 juin 2006, n° 54934/00, affaire Weber et Saravia contre Allemagne, notamment le paragraphe n° 104.

91 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 232.

92 - Voir l'arrêt de la CEDH du 6 septembre 1978, n° 5029/71, affaire Klass et autres contre Allemagne, notamment le paragraphe n° 49.

93 - Voir l'arrêt de la CEDH du 4 décembre 2008, n° 30562/04, affaire S. et Marper contre Royaume-Uni, notamment le paragraphe n° 102.

94 - Voir l'arrêt de la CEDH du 13 septembre 2018, n° 58170/13, affaire Big Brother Watch et autres contre Royaume-Uni, notamment le paragraphe n° 314.

Dans tous les cas, la CEDH juge que les législations nationales doivent entourer le recueil et l'exploitation de renseignements de « *garanties adéquates et effectives contre les abus* », dont la validité est appréciée par la cour au regard de « *toutes les circonstances de la cause, par exemple la nature, la portée et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit interne* »[95].

La CEDH reprend tout d'abord les six « *garanties minimales* » mentionnées plus haut, en examinant la manière dont la loi prévoit leur mise en œuvre :

- s'agissant de la nature des infractions dont la prévention peut justifier une mesure de surveillance, la seule référence à des infractions graves peut suffire, la cour estimant en l'espèce que « *l'emploi de l'expression "infractions graves", lue à la lumière des dispositions interprétatives de la loi, donne aux citoyens une indication suffisante des situations et des conditions dans lesquelles les pouvoirs publics sont habilités à recourir à des mesures de surveillance secrète* »[96]. La CEDH se déclare en revanche « *préoccupée* » lorsqu'elle constate qu'une loi « *autorise l'interception secrète des communications pour un très large éventail d'infractions pénales, y compris (...) le vol à la tire* »[97] ;
- s'agissant des catégories de personnes susceptibles d'être surveillées, la cour tient compte de l'implication directe ou non des personnes dans des projets d'infraction, tout en admettant que « *les mesures d'interception visant une personne non soupçonnée d'une infraction mais susceptible de détenir des informations sur une telle infraction pouvaient être justifiées au regard de l'article 8 de la Convention* »[98]. Elle porte en outre au crédit d'une législation une disposition selon laquelle « *le mandat d'interception lui-même*

95 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 232.

96 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 159.

97 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 244.

98 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 245.

doit définir précisément, par la mention de son nom ou par sa description, la personne faisant l'objet de l'interception ou le bâtiment visé par l'interception autorisée par le mandat »[99] ;

- s'agissant de la durée d'exécution de la mesure, la CEDH considère que « *la durée totale d'une opération d'interception dépend de la complexité et de la durée de l'enquête et que, pourvu qu'il existe des garanties suffisantes, il n'est pas déraisonnable de laisser cette question à l'appréciation des autorités internes* »[100]. Constituent pour la cour des garanties suffisantes « *des indications claires dans le droit interne sur le délai d'expiration de l'autorisation d'interception, les conditions dans lesquelles elle peut être renouvelée et les circonstances dans lesquelles elle doit être annulée* »[101] ;

- s'agissant de la procédure à suivre pour l'exploitation et la conservation des renseignements recueillis, la CEDH s'attache principalement à mesurer le degré de protection dont bénéficient ces données, eu égard notamment à la sécurisation dont elles font l'objet ou aux restrictions régissant leur consultation. La cour a plusieurs fois relevé le caractère satisfaisant d'une législation soumettant les données collectées au régime du secret de l'État, seules les personnes spécialement habilitées pouvant y avoir accès [102] ;

- s'agissant des précautions à prendre pour la diffusion des données collectées, la CEDH a validé des dispositions instituant une « *divulgation sélective* », selon laquelle « *l'étendue de la divulgation doit être limitée aux besoins du destinataire des informations interceptées* »[103] ;

99 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 160.

100 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 161.

101 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 250.

102 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 253.

103 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 163.

- s'agissant de la destruction des données collectées, la CEDH examine si la loi fixe un délai maximal au terme duquel ces données doivent être effacées. Elle n'émet pas d'objection à des dispositions se bornant à prévoir, dans le cas d'interceptions de communications, que « *toutes les données (...) ainsi que toutes les copies des informations ou des données en question soient détruites dès lors que les motifs qui rendaient leur conservation nécessaire au sens de [la loi nationale] ont disparu* »[104]. Elle déplore en revanche le cas où une législation, bien que fixant une durée maximale de conservation, ne contient pas « *d'obligation de détruire sur-le-champ les données qui n'ont pas de rapport avec le but pour lequel elles ont été recueillies* » ; une « *conservation automatique (...) de données manifestement dénuées d'intérêt* » pendant la durée maximale de conservation légale « *ne saurait passer pour justifiée au regard de l'article 8* » de la convention[105].

La CEDH apprécie ensuite la manière dont les mesures de surveillance peuvent être autorisées, contrôlées et, le cas échéant, contestées. Elle recherche ainsi « *si les procédures de contrôle du déclenchement et de la mise en œuvre de mesures restrictives sont de nature à circonscrire "l'ingérence" à ce qui est "nécessaire dans une société démocratique"* »[106].

La cour distingue trois étapes lors desquelles peut s'exercer le contrôle des mesures de surveillance, « *lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé* »[107].

La CEDH concède que, lors des deux premières étapes, « *la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le*

104 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment le paragraphe n° 164.

105 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 255.

106 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 232.

107 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 233.

contrôle qui l'accompagne » ; elle estime dès lors indispensable que « *les procédures existantes procurent en elles-mêmes des garanties appropriées (...) sauvegardant les droits de l'individu* »[108]. Lors de la troisième étape, la seule offrant l'occasion à la personne concernée de faire valoir son droit au respect de sa vie privée, se posent deux questions supplémentaires, celle de « *l'effectivité des recours judiciaires* » et, de façon liée, celle de « *la notification a posteriori de mesures de surveillance* » à la personne qui en a fait l'objet[109].

Pour apprécier la conformité à la convention d'une législation à chacune de ces trois étapes, la CEDH examine successivement les garanties entourant :

- l'autorisation des mesures de surveillance ;
- l'accès des autorités nationales aux renseignements recueillis ;
- le contrôle de l'application des mesures ;
- la notification des mesures aux personnes qui en ont fait l'objet.

S'agissant de la procédure d'autorisation, la CEDH prend en compte « *le service compétent pour autoriser la surveillance, la portée de l'examen qu'il effectue et le contenu de l'autorisation d'interception* »[110] :

- l'autorité décisionnaire en matière de renseignement peut être « *un service non judiciaire* », pourvu qu'il soit « *suffisamment indépendant à l'égard de l'exécutif* »[111]. La cour a également admis qu'il puisse s'agir de l'exécutif lui-même, à condition qu'il existe un organe indépendant de lui exerçant un contrôle effectif[112] ;
- la portée de l'examen effectué par l'autorité décisionnaire doit inclure la vérification de « *l'existence d'un soupçon raisonnable à l'égard de la personne concernée* », ce qui consiste en particulier à

108 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 233.

109 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 234.

110 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 257.

111 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 258.

112 - Voir l'arrêt de la CEDH du 18 mai 2010, n° 26839/05, affaire Kennedy contre Royaume-Uni, notamment les paragraphes n° 166 à n° 168.

relever, le cas échéant en réclamant des « *pièces justificatives* », « *s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme des actes mettant en péril la sécurité nationale* » ; en outre l'autorité décisionnaire doit s'assurer que la mesure de surveillance satisfait le critère de « *nécessité dans une société démocratique* » prévu à l'article 8 de la convention, en examinant notamment si cette mesure est « *proportionnée aux buts légitimes poursuivis* » ; cet examen de proportionnalité doit pouvoir inclure un contrôle de subsidiarité, par lequel l'autorité décisionnaire recherche « *s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs* »[113], c'est-à-dire moins attentatoires à la vie privée ;

- l'autorisation doit « *désigner clairement la personne précise à placer sous surveillance ou l'unique ensemble de locaux (...) visé par l'interception autorisée* ». Cette désignation peut prendre la forme de « *noms, adresses, numéros de téléphone ou d'autres informations pertinentes* »[114].

S'agissant de l'accès des autorités nationales aux renseignements, la CEDH considère, en matière d'interception de communications, qu'une « *obligation de présenter une autorisation d'interception au fournisseur de services de communication pour pouvoir accéder aux communications d'une personne constitue l'une des garanties importantes contre les abus de la part des services* » de renseignement[115].

113 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 260.

114 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 264.

115 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 269.

S'agissant du contrôle de l'exécution des mesures, la CEDH vérifie que le droit interne garantit que « *les prescriptions légales concernant la mise en œuvre de mesures de surveillance ainsi que la conservation, la consultation, l'utilisation, le traitement, la communication et la destruction des éléments interceptés sont systématiquement respectées* »[116] :

- la cour examine tout d'abord s'il existe un organe de contrôle indépendant. Elle considère « *en principe souhaitable que la fonction de contrôle soit confiée à un juge* » mais « *le contrôle par un organe non judiciaire peut passer pour compatible avec la Convention dès lors que cet organe est indépendant des autorités qui procèdent à la surveillance et est investi de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent* ». L'indépendance tient au « *mode de désignation et [au] statut juridique des membres de l'organe de contrôle* » ; selon ces critères, la cour a jugé « *suffisamment indépendants les organes composés de députés – de la majorité comme de l'opposition – ou de personnes possédant les qualifications requises pour accéder à la magistrature et nommées soit par le parlement soit par le Premier ministre* », mais pas « *un ministre de l'Intérieur qui non seulement était nommé par le pouvoir politique et membre de l'exécutif, mais de plus était directement impliqué dans la commande de moyens spéciaux de surveillance* », non plus qu'un « *procureur général et des procureurs de rang inférieur compétents* »[117] ;
- la cour apprécie ensuite le caractère effectif du contrôle, en recherchant[118] :
  - si l'organe compétent a pour seule mission de contrôler la mise en œuvre de mesures de surveillance ou s'il s'agit d'une compétence parmi d'autres plus ou moins étendues ;

116 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 273.

117 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment les paragraphes n° 275 et n° 278.

118 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment les paragraphes n° 280 à n° 282.

- si l'organe compétent dispose d'un accès à tous les documents pertinents, y compris classifiés ;
- si le champ du contrôle comprend toutes les activités de renseignement ou en exclut certaines ;
- si l'organe de contrôle dispose, en cas d'infraction constatée, du pouvoir d'ordonner l'interruption d'une mesure et la destruction des informations recueillies ;

- la cour est enfin attentive au « *droit de regard du public* » sur les activités de contrôle[119]. Prenant note des législations imposant à l'organe de contrôle de rédiger un rapport public, elle critique les cadres juridiques ne prévoyant aucun mécanisme de reddition de comptes aux citoyens sur le fonctionnement général du recueil de renseignement. Lorsque des rapports sont établis, la cour analyse le degré de précision des informations qu'ils contiennent.

S'agissant de la notification des mesures de surveillance aux personnes qui en ont fait l'objet[120], la CEDH considère la question « *indissolublement liée à celle de l'effectivité des recours judiciaires* »[121]. Relevant 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* », la cour admet qu'« *une notification ultérieure à chaque individu touche 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* »[122]. Le principe selon lequel il est « *souhaitable d'aviser la personne concernée après la levée des mesures de surveillance*

119 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 283.

120 - Voir, pour une analyse plus détaillée du sujet, l'étude figurant dans le deuxième rapport d'activité 2017 de la CNCTR intitulée « La notification aux personnes concernées des mesures de surveillance mises en œuvre à leur encontre par le passé ».

121 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 286.

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

dès que la notification peut être donnée sans compromettre le but de la restriction »[123] peut donc souffrir des exceptions. La cour a également déclaré compatible avec la convention un cadre juridique excluant toute notification, dès lors que « *toute personne soupçonnant que ses communications faisaient ou avaient fait l'objet d'interceptions pouvait saisir la commission des pouvoirs d'enquête* »[124].

C'est à l'issue de l'ensemble de cet examen que la CEDH s'estime en mesure de juger si une mesure de surveillance prévue par une loi constitue une « *ingérence nécessaire dans une société démocratique* » au sens de l'article 8 de la convention. La cour porte ainsi une appréciation globale. Les multiples critères d'analyse dont elle se sert sont conçus comme lui permettant de mettre en lumière un faisceau de garanties, satisfaisant ou non. La faiblesse d'une garantie particulière peut être compensée par l'existence ou le caractère renforcé d'une autre garantie. La conformité d'une législation à la convention, comme la violation de celle-ci, est déclarée sur le fondement d'un ensemble de constatations.

123 - Voir la décision d'irrecevabilité de la CEDH du 29 juin 2006, n° 54934/00, affaire Weber et Saravia contre Allemagne, notamment le paragraphe n° 135.

124 - Voir l'arrêt de la CEDH du 4 décembre 2015, n° 47143/06, affaire Roman Zakharov contre Russie, notamment le paragraphe n° 288.

2. La CJUE a énoncé des critères que doivent satisfaire les législations nationales régissant l'accès des autorités publiques à certaines données de connexion

L'article 52 de la Charte des droits fondamentaux de l'Union européenne prévoit que « *toute limitation de l'exercice des droits et libertés reconnus par la [charte] doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés* » et que « *dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui* ». Le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, énoncés aux articles 7 et 8 de la charte, sont concernés par ces stipulations.

2.1 L'atteinte à la vie privée doit être prévue par une règle contraignante, claire et précise

Selon la CJUE, une mesure limitant les droits reconnus par la Charte des droits fondamentaux de l'Union européenne doit être prévue par « *des règles claires et précises régissant la portée et l'application d'une telle mesure* ». Se prononçant sur l'accès d'autorités nationales à des données de connexion conservées par des opérateurs de communications électroniques, ce qui peut inclure des techniques de renseignement, la cour a précisé que la réglementation nationale devait « *prévoir des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services de communications*

électroniques doivent accorder aux autorités nationales compétentes l'accès aux données ». Par ailleurs, pour la CJUE, une réglementation de cette nature « *doit être légalement contraignante en droit interne* »[125].

Si le vocabulaire utilisé par la CEDH et la CJUE diffère sur la forme, la proximité des jurisprudences sur le fond est renforcée par le fait que la CJUE a déjà motivé des jugements sur ce point par analogie avec des arrêts de la CEDH[126].

2.2 L'atteinte doit respecter le contenu essentiel du droit au respect de la vie privée ainsi que le principe de proportionnalité

La CJUE exerce un contrôle voisin de celui conduit par la CEDH, mais dispose de critères et de méthodes d'analyse propres.

L'article 52 de la Charte des droits fondamentaux de l'Union européenne prévoit que toute « *limitation de l'exercice des droits et libertés* » reconnus par la Charte doit non seulement être « *nécessaire* », respecter « *le principe de proportionnalité* » et répondre à « *des objectifs d'intérêt général reconnus par l'Union* » ou au « *besoin de protection des droits et libertés d'autrui* », mais également respecter le « *contenu essentiel* » des droits et libertés ainsi limités.

La CJUE définit au cas par cas ce qu'elle estime relever du « *contenu essentiel* » d'un droit reconnu par la charte. En matière de renseignement, la cour a jugé, en examinant la validité d'une décision de la Commission européenne qualifiant d'adéquat le niveau de protection des données à caractère personnel transférées depuis les États membres de l'Union vers des organisations établies aux États-Unis, qu'une réglementation telle que celle

125 - 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 et autres), notamment les paragraphes n° 109 et n° 117.

126 - Voir l'arrêt de la CJUE du 8 avril 2014, affaires C 293/12 (*Digital Rights Ireland Ltd.* contre *Minister for Communications* et autres) et C-594/12 (*Kärntner Landesregierung* et autres), notamment le paragraphe n° 54.

en vigueur dans ce pays « *permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée* »[127]. En revanche, une réglementation prévoyant la conservation, par des opérateurs de communications électroniques, de données de connexion relatives au trafic ou à la localisation de leurs abonnés « *n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel* » du droit au respect de la vie privée[128].

Dans l'affaire concernant le niveau de protection des données à caractère personnel aux États-Unis, l'appréciation de l'éventuelle atteinte au contenu essentiel d'un droit reconnu par la charte a primé le contrôle de la nécessité, en particulier de la proportionnalité, des mesures concernées. Après avoir affirmé l'existence d'une telle atteinte, la cour a constaté la méconnaissance du droit européen, lu à la lumière de la charte, « *sans qu'il soit besoin d'examiner les principes [de la décision invalidée] quant à leur contenu* »[129].

En l'absence d'atteinte au « *contenu essentiel* » d'un droit, la CJUE poursuit son examen de la limitation apportée à ce droit, en qualifiant son degré de gravité. Une mesure de surveillance consistant à accéder aux numéros de téléphone d'une personne ainsi qu'à son identité et, le cas échéant, à son adresse « *ne saurait être qualifiée d'ingérence "grave" dans les droits fondamentaux des personnes dont les données sont concernées* »[130]. En revanche, la conservation par des opérateurs de communications électroniques et, *a fortiori*, le recueil par des autorités nationales compétentes de données de connexion relatives au trafic et à la localisation d'abonnés constituent une ingérence « *particulièrement grave* » dans le droit au respect à la vie privée, dès lors que ces données permettent de savoir

127 - Voir l'arrêt de la CJUE du 6 octobre 2015, affaire C 362/14 (Maximillian Schrems contre *Data Protection Commissioner*), notamment le paragraphe n° 94.

128 - 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 et autres), notamment le paragraphe n° 101.

129 - Voir l'arrêt de la CJUE du 6 octobre 2015, affaire C 362/14 (Maximillian Schrems contre *Data Protection Commissioner*), notamment le paragraphe n° 98.

130 - Voir l'arrêt de la CJUE du 2 octobre 2018, affaire C 207/16 (*Ministerio fiscal*), notamment le paragraphe n° 61.

quelle personne communique avec quelle autre, par quel moyen, combien de temps, à quelle fréquence et en quel lieu, ce qui rend possible de « *tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées* »[131].

À la gravité de l'ingérence doit correspondre, selon la CJUE, un objectif « *en relation* » avec ce niveau de gravité. Ainsi, lorsque l'ingérence consiste à accéder à des données de connexion relatives au trafic et à la localisation de personnes et que l'objectif poursuivi est, notamment, la prévention d'infractions pénales, « *seule la lutte contre la criminalité grave est susceptible de justifier un tel accès aux données* »[132].

La CJUE s'assure ensuite que l'ingérence d'une particulière gravité dans le droit reconnu par la charte « *n'ait lieu que dans les limites du strict nécessaire* » et respecte le « *principe de proportionnalité* »[133]. En application de ce principe, la réglementation applicable doit prévoir, en garantie, « *les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données* » de connexion relatives au trafic et à la localisation des personnes[134], ce qui inclut :

- la fixation de « *critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données* ». En matière de lutte contre la criminalité, les personnes concernées doivent être « *soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* ». La cour admet cependant que « *dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la*

131 - 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 et autres), notamment les paragraphes n° 98 à n° 100.

132 - 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 et autres), notamment le paragraphe n° 115.

133 - 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 et autres), notamment le paragraphe n° 116.

134 - 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 et autres), notamment le paragraphe n° 118.

sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités »[135] ;

- l'existence, « *sauf cas d'urgence dûment justifiés* », d'un « *contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante* ». La cour précise que « *la décision de cette juridiction ou de cette entité* » doit intervenir « *à la suite d'une demande motivée* » des autorités souhaitant accéder aux données[136] ;

- l'information des personnes surveillées « *dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées* ». La cour qualifie l'information des personnes intéressées de « *nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours* »[137] ;

- la conservation sur le territoire de l'Union européenne des données conservées ainsi que « *la destruction irrémédiable des données au terme de la durée de conservation* »[138] ;

- le contrôle « *par une autorité indépendante* » des accès aux données afin de s'assurer du respect du « *niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel* »[139].

---

135 - 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 et autres), notamment le paragraphe n° 119.

136 - 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 et autres), notamment le paragraphe n° 120.

137 - 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 et autres), notamment le paragraphe n° 121.

138 - 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 et autres), notamment le paragraphe n° 122.

139 - 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 et autres), notamment le paragraphe n° 123.

La CJUE a énoncé ces principes en réponse à des questions générales d'interprétation du droit de l'Union posées par des juridictions nationales. Contrairement au contrôle exercé par la CEDH au regard de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, elle ne s'est pas prononcée sur la conformité à la Charte des droits fondamentaux de l'Union européenne d'une législation en particulier. La manière dont elle a exposé les critères permettant d'apprécier le caractère légal, nécessaire et proportionné d'une législation permettant d'accéder à des données de connexion laisse toutefois entendre que ces critères devraient être intégralement respectés.

À la différence de la jurisprudence de la CEDH, celle de la CJUE est encore nouvelle et repose sur un nombre limité d'arrêts. Plusieurs questions préjudicielles concernant la conservation générale et indifférenciée des données de connexion par les opérateurs de communications électroniques ainsi que la mise en œuvre de techniques de renseignement sur ces données ont été posées à la CJUE en 2017 et en 2018 par des juridictions britannique, belge et française, en l'espèce le Conseil d'État dans le dernier cas[140]. La jurisprudence de la CJUE sera donc prochainement précisée.

140 - Voir, pour une analyse des questions préjudicielles posées par le Conseil d'État, l'encadré figurant au point 2.2.3.2 du présent rapport.

Annexes

Annexe n° 1

Délibération de la CNCTR n° 5/2017 du 7 décembre 2017

Saisie pour avis le 8 novembre 2017 par le ministre de l'intérieur[1] d'un projet de décret modifiant la partie réglementaire du code de la sécurité intérieure et relatif à la désignation d'un nouveau service autorisé à recourir aux techniques mentionnées au titre V du livre VIII du code, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

I. Remarques de portée générale

Le projet de décret est pris pour l'application de l'article L. 811-4 du code de la sécurité intérieure, qui prévoit que 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 sont désignés par décret en Conseil d'État pris après avis de la CNCTR. Ce décret doit préciser les techniques ainsi que les finalités mentionnées à l'article L. 811-3 du code qui peuvent faire l'objet d'autorisations.

La CNCTR rappelle qu'elle a déjà rendu deux avis sur des projets de décret[2] désignant des services, dits du « second cercle », autorisés à recourir aux techniques de renseignement en application de l'article L. 811-4 du code de

1 - Voir le courrier n° 1914 du 6 novembre 2017, adressé par l'adjointe au directeur des libertés publiques et des affaires juridiques du ministère de l'intérieur et reçu le 8 novembre 2017.

2 - 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.

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, et apporte les précisions ci-dessous.

a) La CNCTR considère notamment que la nature et le nombre de techniques auxquelles peuvent avoir accès les services du « second cercle » dépend 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.

La commission indique que cette conception stricte et limitative des besoins des services du « second cercle » en matière de techniques de renseignement, outre qu'elle est justifiée par la protection de la vie privée, est corroborée par la pratique observée depuis l'entrée en vigueur en décembre 2015 du premier décret en Conseil d'État désignant ces services.

b) La CNCTR estime en outre 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, qui ne pourra en revanche participer à l'exploitation des renseignements collectés. Elle admet également que le service du « second cercle » demandeur fasse appel, pour la seule réalisation de l'opération, à un autre service de renseignement disposant de l'expérience et des compétences requises.

c) La CNCTR indique que l'ouverture, au profit d'un service de renseignement, de la faculté de mettre en œuvre des techniques pour une finalité particulière n'exclut pas que tous les services de renseignement concernés par cette finalité continuent à agir de façon coordonnée et complémentaire, en fonction de leurs missions, de leurs compétences et de leur expertise technique.

d) La CNCTR rappelle enfin 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 de ces données, 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).

II. Observations détaillées

1. Sur la désignation du service

Le projet de décret soumis à la CNCTR désigne comme service de renseignement du « second cercle » le département de la criminalité organisée au sein de la sous-direction spécialisée dans la lutte contre l'immigration irrégulière (SDLII) de la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP) de la préfecture de police de Paris.

Pour lutter contre des flux d'immigration irrégulière de grande ampleur et renforcer la coordination entre les services de police chargés de cette lutte à Paris et dans les départements des Hauts-de-Seine, de la Seine-Saint-Denis et du Val-de-Marne, la SDLII, sous-direction spécialisée dans ce domaine, a été créée à la préfecture de police de Paris par arrêté n° 2017/559 du 15 mai 2017. Née du rapprochement de différentes unités précédemment rattachées à plusieurs directions, cette sous-direction comprend un département de lutte contre la criminalité organisée, qui a pour mission le démantèlement de filières d'acheminement illégal, de traite d'êtres humains et d'aide au maintien irrégulier sur le territoire national. Si le département diligente essentiellement des enquêtes judiciaires, il peut exercer sa mission à titre préventif dans un cadre de police administrative. La SDLII a indiqué à la CNCTR qu'à ce titre, une unité précédemment rattachée à la direction du renseignement avait pu, sous l'empire du cadre juridique antérieur au livre VIII du code de la sécurité intérieure, être autorisée à mener des interceptions de sécurité.

Eu égard à ces éléments, la CNCTR considère que le département de lutte contre la criminalité organisée de la SDLII peut être autorisé à recourir à des techniques de renseignement pour la finalité prévue au 6° de l'article L. 811-3 du code de la sécurité intérieure, à savoir la prévention de la criminalité et de la délinquance organisée.

2. Sur les techniques autorisées

a) La CNCTR émet un avis favorable à ce que le département de lutte contre la criminalité organisée de la SDLII puisse être autorisé 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 ;
- la géolocalisation en temps réel, prévue à l'article L. 851-4 du code de la sécurité intérieure ;
- le balisage, prévu à l'article L. 851-5 du code de la sécurité intérieure ;
- l'interception de sécurité réalisée *via* le GIC, prévue au I de l'article L. 852-1 du code de la sécurité intérieure ;
- la captation de paroles prononcées à titre privé et la captation d'images dans un lieu privé, prévues à l'article L. 853-1 du code de la sécurité intérieure ;
- l'introduction dans un lieu privé ne constituant pas un lieu d'habitation, prévue à l'article L. 853-3 du code de la sécurité intérieure, pour y mettre en place, utiliser ou retirer une balise ou un dispositif de captation de paroles ou d'images.

La CNCTR précise que le recours du service concerné à des dispositifs de captation de paroles ou d'images peut être admis à la condition que ces techniques soient mises en œuvre par un opérateur disposant de la compétence requise, en l'espèce la cellule d'assistance technique de l'état-major de la direction régionale de la police judiciaire de Paris, comme le prévoit le projet de décret. Il en va de même pour l'introduction dans un lieu privé ne constituant pas un lieu d'habitation, dont le projet de décret attribue la réalisation au centre opérationnel des ressources techniques de la direction opérationnelle des services techniques et logistiques à la préfecture de police de Paris.

b) Au cours de son instruction, la CNCTR a constaté que la SDLII n'avait à ce jour ni les compétences techniques ni même le besoin opérationnel de recueillir des données de connexion par *IMSI catcher* sur le fondement de

l'article L. 851-6 du code de la sécurité intérieure. La commission n'est dès lors pas favorable à ce que le département de lutte contre la criminalité organisée de la SDLII puisse avoir recours à cette technique de renseignement.

S'agissant du recueil et de la captation de données informatiques, prévus aux 1° et 2° du I de l'article L. 853-2 du code de la sécurité intérieure, la CNCTR rappelle que, dans sa délibération n° 2/2015 du 12 novembre 2015, elle a estimé que le recours, à des fins de renseignement, à ces techniques particulièrement complexes et intrusives, qui peuvent être mises en œuvre dans un cadre judiciaire sur le fondement du code de procédure pénale, n'était pas justifié pour l'Office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre (OCRIEST), qui remplit, au sein de la direction centrale de la police aux frontières à la direction générale de la police nationale, une mission similaire à celle du service concerné par le projet de décret. Conformément à cette doctrine, corroborée par la pratique, la commission n'est pas favorable à ce que le département de lutte contre la criminalité organisée de la SDLII, service de police essentiellement judiciaire, puisse être autorisé à recueillir ou capter des données informatiques dans un cadre administratif, la CNCTR ayant de surcroît constaté que la SDLII ne disposait pas de compétences en la matière.

Annexe n° 2

Délibération de la CNCTR n° 1/2018 du 9 mai 2018

Saisie pour avis le 4 mai 2018 par le Gouvernement d'un projet de modification législative du chapitre IV du titre V du livre VIII du code de la sécurité intérieure, relatif aux mesures de surveillance des communications électroniques internationales, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

I. Remarques de portée générale

Le projet de texte soumis à la CNCTR a pour objet de prévoir dans la loi les conditions et les limites dans lesquelles les services spécialisés de renseignement, dans le cadre de la surveillance des communications électroniques internationales, peuvent être autorisés à vérifier ponctuellement et, le cas échéant, à exploiter des données de connexion, voire des correspondances de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national[1].

Le cadre légal actuellement en vigueur en matière de surveillance des communications électroniques internationales prohibe, au troisième alinéa de l'article L. 854-1 du code de la sécurité intérieure, « *la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national* ». Deux exceptions sont toutefois prévues à ce même alinéa lorsque

1 - Les numéros d'abonnement ou les identifiants techniques rattachables au territoire national peuvent être, par exemple, des numéros de téléphone portable précédés de l'indicatif français +33.

« *ces personnes communiquent depuis l'étranger* » et « *soit faisaient l'objet d'une autorisation d'interception de sécurité, délivrée en application de l'article L. 852-1, à la date à laquelle elles ont quitté le territoire national, soit sont identifiées comme présentant une menace au regard des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3* » du code de la sécurité intérieure.

Le projet de texte soumis à la CNCTR maintient cette interdiction et ses deux exceptions, tout en complétant le champ des mesures pouvant être prises à l'égard des personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national :

- des vérifications ponctuelles, qui ne constituent pas des mesures de surveillance individuelle, pourraient être effectuées dans les conditions et les limites prévues par la loi ;
- une nouvelle exception à l'interdiction de prendre des mesures de surveillance individuelle serait créée et légalement encadrée.

La CNCTR n'émet pas d'objection au principe d'une telle évolution législative. Elle estime en effet que, près de deux ans et demi après l'entrée en vigueur de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, l'expérience a montré que le cadre légal issu de cette loi comportait des restrictions pouvant paraître excessives au regard de la conciliation à effectuer entre la protection de la vie privée et la préservation des intérêts fondamentaux de la Nation.

La CNCTR considère que certaines des restrictions portant sur les communications de personnes utilisant des numéros d'abonnement ou des identifiants rattachables au territoire national pourraient être allégées, comme le prévoit le projet de texte soumis à son examen, sous réserve du respect de garanties détaillées ci-dessous.

II. Observations détaillées

1. Sur les mesures de vérification ponctuelle

a) Le projet de texte soumis à la CNCTR prévoit de compléter l'article L. 854-2 du code de la sécurité intérieure par un IV selon lequel les autorisations d'exploitation de communications ou de seules données de connexion prévues au III du même article vaudraient également autorisation d'effectuer des vérifications ponctuelles sur des données de connexion, voire sur des correspondances de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national.

Les vérifications ponctuelles seraient effectuées à la seule fin de détecter des menaces affectant les intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code de la sécurité intérieure. Il ne pourrait s'agir que de menaces liées aux relations qu'entretiennent les numéros d'abonnement ou les identifiants techniques concernés avec les zones géographiques, les organisations, les groupes de personnes ou les personnes faisant l'objet d'une autorisation d'exploitation de communications ou de seules données de connexion accordée par le Premier ministre après avis de la CNCTR sur le fondement du III de l'article L. 854-2 du code de la sécurité intérieure.

La CNCTR considère que, tel qu'est rédigé le projet de texte soumis à son examen, les vérifications ponctuelles doivent être regardées comme ne constituant pas des mesures de surveillance individuelle des personnes concernées, mais des mesures préparatoires destinées à lever des soupçons et, tout au plus, à vérifier si une telle surveillance devrait être mise en œuvre ou non. Le caractère ponctuel des vérifications, qui exclut que celles-ci soient effectuées de manière répétée, ainsi que leur objet, limité à la seule détection d'une éventuelle menace, garantissent que ces mesures seraient moins intrusives qu'une surveillance individuelle.

Il en résulte que des vérifications ponctuelles sur des données de connexion, voire sur des correspondances de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire

national pourraient être légalement effectuées, même lorsque ces personnes communiquent depuis le territoire national. La restriction imposée sur ce point par le troisième alinéa de l'article L. 854-1 du code de la sécurité intérieure ne concerne en effet que les mesures de surveillance individuelle.

b) Le projet de texte soumis à la CNCTR prévoit que, lorsqu'elles porteraient sur des données de connexion, les vérifications ponctuelles pourraient être effectuées pour détecter une menace affectant tout intérêt fondamental de la Nation mentionné à l'article L. 811-3 du code de la sécurité intérieure.

Dès lors que les vérifications sont seulement ponctuelles, qu'elles ne concernent que des données de connexion, qu'elles ont pour seul but la détection d'une menace et qu'elles sont effectuées dans le cadre d'une autorisation accordée par le Premier ministre après avis de la CNCTR sur le fondement du III de l'article L. 854-2 du code de la sécurité intérieure, la commission n'estime pas disproportionné le recours à ces vérifications au titre de l'ensemble des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du code.

Le projet de texte soumis à la CNCTR prévoit également que des vérifications ponctuelles pourraient porter sur des correspondances pour deux finalités exclusivement :

- la détection d'une attaque informatique susceptible d'affecter l'indépendance nationale, l'intégrité du territoire ou la défense nationale ;
- la détection, en cas d'urgence, d'une menace terroriste.

Aux limites déjà applicables, à savoir le caractère ponctuel des vérifications, le but unique de détection d'une menace et le cadre défini par une autorisation accordée par le Premier ministre après avis de la CNCTR sur le fondement du III de l'article L. 854-2 du code de la sécurité intérieure, s'ajouteraient donc des restrictions spécifiques, liées à la protection de certains intérêts fondamentaux de la Nation : seules l'indépendance nationale, l'intégrité du territoire et la défense nationale, mentionnées au 1° de l'article L. 811-3 du code, ou la prévention du terrorisme, mentionnée au 4° du même article, pourraient justifier des vérifications sur des

correspondances. De plus, la première finalité serait elle-même restreinte à la prévention d'attaques informatiques et la seconde à des mesures d'urgence face à une menace terroriste.

Dans ces conditions, la CNCTR n'estime pas disproportionné la réalisation de vérifications ponctuelles sur des correspondances de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national.

c) Le projet de texte soumis à la CNCTR précise que, lorsque les vérifications ponctuelles révèleraient une menace nécessitant la mise en place d'une surveillance, les communications de la personne concernée ne pourraient être exploitées sans l'obtention préalable d'une autorisation ciblée, accordée par le Premier ministre après avis de la CNCTR. Seule cette autorisation spécifique permettrait au service bénéficiaire de passer de mesures de vérification ponctuelle à des mesures de surveillance individuelle.

La CNCTR n'émet pas d'objection à ces dispositions, qui renforcent la cohérence du cadre légal et garantissent qu'aucune surveillance individuelle ne pourra être menée sans autorisation ciblée spécifique. Elle considère cependant que la rédaction du projet de texte soumis à son examen devrait être complétée sur un point.

En l'état de sa rédaction, le projet de texte n'impose une autorisation spécifique que pour « l'exploitation des communications » des personnes concernées, ce qui inclut à la fois les données de connexion et les correspondances constitutives de ces communications. Or l'exploitation de seules données de connexion peut également constituer une mesure de surveillance individuelle. La CNCTR préconise donc de remplacer les mots : « *l'exploitation des communications* » par les mots : « *l'exploitation des communications ou des seules données de connexion interceptées* », au dernier alinéa du projet de IV de l'article L. 854-2 du code de la sécurité intérieure.

2. Sur les mesures de surveillance individuelle

Dans le cadre légal actuel, la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national est interdite au titre de la surveillance des communications électroniques internationales, sauf exceptions rappelées dans les remarques générales de la présente délibération.

Le projet de texte soumis à la CNCTR prévoit, par l'ajout d'un V à l'article L. 854-2 du code de la sécurité intérieure, une nouvelle exception. Par dérogation à l'interdiction de principe, le Premier ministre pourrait, après avis de la CNCTR, autoriser les services spécialisés de renseignement à exploiter les communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, alors même que ces personnes communiquent depuis la France.

La nouvelle exception ne pourrait être mise en œuvre que pour la défense ou la promotion des intérêts fondamentaux de la Nation mentionnés aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3 du code de la sécurité intérieure, à savoir :

- l'indépendance nationale, l'intégrité du territoire ou 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 ;
- la prévention du terrorisme ;
- la prévention de la criminalité et de la délinquance organisées ;
- la prévention de la prolifération des armes de destruction massive.

La CNCTR n'émet pas d'objection à la faculté d'utiliser une nouvelle exception, dès lors que cette faculté ne pourra être mise en œuvre sans autorisation préalable accordée par le Premier ministre après avis de la CNCTR.

La CNCTR relève toutefois que l'exploitation de communications projetée est similaire, dans son principe, aux interceptions de sécurité prévues à l'article L. 852-1 du code de la sécurité intérieure. Or ces interceptions de

sécurité sont soumises à un contingentement, décidé par le Premier ministre, qui limite le nombre d'autorisations simultanément en vigueur.

Par cohérence avec les garanties entourant les interceptions de sécurité et pour limiter au strict nécessaire la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, la CNCTR recommande d'instituer un contingentement des autorisations d'exploitation prévues au projet de V de l'article L. 854-2 du code de la sécurité intérieure.

Le projet de V pourrait, à cet effet, être complété par un alinéa ainsi rédigé : « *Le nombre maximal des autorisations d'exploitation en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 est porté à la connaissance de la commission* ».

En outre, pour les mêmes raisons que celles exposées plus haut à propos du projet de IV de l'article L. 854-2 du code de la sécurité intérieure, la CNCTR préconise de remplacer les mots : « *exploitation de communications* » par les mots : « *exploitation de communications ou de seules données de connexion interceptées* », au premier alinéa du projet de V de l'article L. 854-2 du code de la sécurité intérieure.

Enfin, la CNCTR estime que la création d'une nouvelle exception à l'interdiction énoncée au troisième alinéa de l'article L. 854-1 du code de la sécurité intérieure nécessite, comme pour les autres exceptions, de déroger également au dernier alinéa du même article, qui prohibe l'interception de communications échangées entre des personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national. La commission propose dès lors de rédiger ainsi le début du dernier alinéa de l'article L. 854-1 du code de la sécurité intérieure : « *Sous réserve des dispositions particulières des troisième et quatrième alinéas du présent article ainsi que du V de l'article L. 854-2, (le reste sans changement)* ».

3. Sur les pouvoirs de contrôle de la CNCTR

a) Le projet de texte soumis à la CNCTR inscrit dans la loi l'obligation de recueillir un avis *a priori* de la commission avant d'accorder toute autorisation d'exploitation de communications ou de seules données de connexion interceptées, sur le fondement du III ou du projet de V de l'article L. 854-2 du code de la sécurité intérieure.

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

La CNCTR est donc favorable à ce que la loi lui confère, comme pour les techniques de renseignement destinées à surveiller le territoire national, un pouvoir de contrôle *a priori* sur les demandes tendant à exploiter des communications ou des seules données de connexion internationales.

Le projet de texte soumis à la CNCTR prévoit que l'avis *a priori* de la commission serait rendu dans les mêmes délais que ceux applicables en matière de surveillance nationale. La CNCTR n'y voit pas d'objection.

b) En matière de contrôle *a posteriori*, le projet de texte soumis à la CNCTR attribue de nouvelles prérogatives à la commission.

Selon le deuxième alinéa du projet de IV de l'article L. 854-2 du code de la sécurité intérieure, lorsque des vérifications ponctuelles pourraient porter, au titre de la prévention du terrorisme, sur des correspondances de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, la CNCTR devrait recevoir immédiatement communication des numéros et des identifiants concernés.

La CNCTR est favorable à cette transmission, qui participerait à la bonne organisation de son contrôle *a posteriori* sur une partie des vérifications ponctuelles les plus sensibles puisque portant sur des correspondances.

Les mesures comparables devant être entourées des mêmes garanties, la CNCTR considère qu'une transmission immédiate devrait être également prévue en cas de vérifications ponctuelles sur des correspondances de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, lorsque ces vérifications auraient pour but, en application du troisième alinéa du projet de IV de l'article L. 854-2 du code de la sécurité intérieure, la prévention d'attaques informatiques susceptibles d'affecter l'indépendance nationale, l'intégrité du territoire ou la défense nationale. Toutes les vérifications ponctuelles effectuées sur des correspondances de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national seraient ainsi encadrées de manière identique.

Le projet de texte soumis à la CNCTR prévoit en outre que les vérifications ponctuelles feraient l'objet d'une traçabilité organisée par le Premier ministre après avis de la CNCTR, en application de l'article L. 854-4 du code de la sécurité intérieure.

La CNCTR, qui estime indispensable une telle traçabilité pour l'accomplissement de son contrôle *a posteriori*, est favorable à sa mise en place.

4. Sur la combinaison entre surveillance nationale et surveillance internationale

Le projet de texte soumis à la CNCTR prévoit d'insérer un nouvel alinéa dans l'article L. 854-1 du code de la sécurité intérieure pour que certaines autorisations accordées dans le cadre de la surveillance nationale puissent, si elles le prévoient, valoir également autorisation de mettre en œuvre, à l'égard des personnes en cause, des mesures de surveillance des communications électroniques internationales.

Cette faculté concernerait 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 pour la seule prévention du terrorisme (article L. 851-2 du code de la sécurité intérieure) et les interceptions de sécurité (I de l'article L. 852-1 du code de la sécurité intérieure).

Les mesures de surveillance des communications électroniques internationales prises dans ce cadre ne pourraient excéder la portée des autorisations accordées au titre de la surveillance nationale et devraient respecter les garanties propres à ces autorisations.

Cela signifie, pour la CNCTR, que les autorisations nationales ne pourraient permettre, en matière internationale, que l'exploitation de données équivalentes, soumises aux mêmes durées de conservation. Plus généralement, les conditions d'exploitation seraient identiques à celles prévues pour la surveillance nationale. L'exécution des interceptions de sécurité étant centralisée par un service du Premier ministre, le groupement interministériel de contrôle, l'exploitation des communications internationales devrait également avoir lieu au sein de ce service.

Dans ces conditions, la CNCTR n'émet pas d'objection à ce que les autorisations nationales rappelées ci-dessus soient complétées par le recueil et l'exploitation de données équivalentes issues de communications électroniques internationales, sous réserve que cette nouvelle faculté ne soit applicable qu'aux autorisations nationales accordées postérieurement à la modification de la loi.

5. Sur les voies de recours contentieux

Le projet de texte soumis à la CNCTR prévoit d'ouvrir à toute personne la faculté de saisir le Conseil d'État d'un recours contentieux afin que le juge administratif vérifie qu'aucune de ses communications impliquant un numéro d'abonnement ou un identifiant technique rattachable au territoire national n'a été irrégulièrement exploitée en méconnaissance du futur V de l'article L. 854-2 du code de la sécurité intérieure.

Dans le cadre légal actuel, la CNCTR peut être saisie par toute personne souhaitant que la commission vérifie qu'aucune mesure de surveillance de ses communications électroniques internationales n'a été irrégulièrement mise en œuvre à son encontre. En revanche, seul le président de la CNCTR ou trois de ses membres peuvent saisir le Conseil d'État, sur le fondement de l'article L. 854-9 du code de la sécurité intérieure, d'un recours contentieux portant sur la légalité de mesures de surveillance des communications électroniques internationales.

Le projet de texte soumis à la CNCTR ne modifie pas ces dispositions. Il se borne à instituer un droit de recours direct pour les seules personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national et pour les seules mesures de surveillance individuelle portant sur les communications de ces personnes.

Il semble cependant à la CNCTR que toutes les mesures concernant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national devraient pouvoir être contestées, qu'il s'agisse de mesures de surveillance individuelle ou de vérifications ponctuelles, dès lors que toutes peuvent concerner aussi bien des données de connexion que des correspondances et, partant, porter une atteinte à la vie privée des personnes en cause.

Plus largement, la CNCTR s'interroge sur la pertinence de maintenir une inégalité en matière de droit de recours, qui ne se fonderait que sur le rattachement au territoire national des numéros ou des identifiants concernés. La pratique des réclamations adressées à la CNCTR par des particuliers sur le fondement de l'article L. 854-9 du code de la sécurité intérieure depuis l'entrée en vigueur du cadre légal actuel il y a près de deux ans et demi ne fournit pas de justification à l'absence de droit de recours direct en matière de surveillance des communications électroniques internationales.

Aussi la CNCTR recommande-t-elle au Gouvernement de permettre à toute personne de saisir le juge administratif de toute mesure susceptible de concerner ses communications électroniques internationales, sous réserve de justifier avoir préalablement saisi la CNCTR d'une réclamation.

Annexe n° 3

Délibération de la CNCTR n° 2/2018 du 17 mai 2018

Saisie pour avis le 19 avril 2018 par le ministre de l'intérieur[1] d'un projet de décret modifiant la partie réglementaire du code de la sécurité intérieure et relatif à la désignation des services autres que les services spécialisés de renseignement pouvant être autorisés à recourir à la technique mentionnée à l'article L. 852-2 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

Le projet de décret est pris pour l'application de l'article L. 811-4 du code de la sécurité intérieure, qui prévoit que 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 sont désignés par décret en Conseil d'État pris après avis de la CNCTR. Ce décret doit préciser les techniques ainsi que les finalités mentionnées à l'article L. 811-3 du code qui peuvent faire l'objet d'autorisations.

La CNCTR rappelle qu'elle a déjà rendu trois avis sur des projets de décret[2] désignant des services, dits du « second cercle », autorisés à recourir aux

1 - Voir le courrier n° 1956 du 17 avril 2018, adressé au président de la CNCTR par le directeur des libertés publiques et des affaires juridiques du ministère de l'intérieur et reçu le 19 avril suivant.

2 - 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 deuxième 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. Le troisième projet n'avait, à la date d'adoption de la présente délibération, pas encore donné lieu à l'édiction d'un texte définitif.

techniques de renseignement en application de l'article L. 811-4 du code de la sécurité intérieure. La commission reprend l'intégralité des remarques de portée générale formulées dans ces trois précédents avis, que constituent sa délibération n° 2/2015 du 12 novembre 2015, sa délibération n° 3/2016 du 8 décembre 2016 ainsi que sa délibération n° 5/2017 du 7 décembre 2017, et apporte les précisions suivantes.

a) La CNCTR considère notamment que la nature et le nombre de techniques auxquelles peuvent avoir accès les services du « second cercle » dépend 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.

La commission indique que cette conception stricte et limitative des besoins des services du « second cercle » en matière de techniques de renseignement, outre qu'elle est justifiée par la protection de la vie privée, est corroborée par la pratique observée depuis l'entrée en vigueur le 12 décembre 2015 du premier décret en Conseil d'État désignant ces services.

b) La CNCTR estime en outre 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, qui ne pourra en revanche participer à l'exploitation des renseignements collectés.

c) La CNCTR rappelle enfin 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 de ces données, 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). À défaut, cette centralisation ne peut se concevoir qu'au niveau de l'état-major des grandes structures de rattachement des services mentionnées dans le projet de décret, à savoir la direction générale de la police nationale (DGPN), la direction générale de la gendarmerie (DGGN), la préfecture de police (PP) et la direction de l'administration pénitentiaire.

II. Observations détaillées

1. Sur la technique autorisée

L'article L. 852-2 du code de la sécurité intérieure, issu de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, dispose que « *peuvent être autorisées les interceptions de correspondances 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, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs* ». Par ailleurs, « *lorsque l'identité de la personne concernée n'est pas connue, la demande précise les éléments nécessaires à l'identification du réseau concerné* ». Enfin l'autorisation, accordée par le Premier ministre après avis de la CNCTR, vaut autorisation de recueil des données de connexion associées à l'exécution de l'interception et à son exploitation.

Les travaux parlementaires ayant précédé l'adoption de ces dispositions législatives ont précisé que « *sont ici visées les conversations transitant par des moyens de communication à courte portée utilisant des techniques de cryptage entre utilisateurs identifiés, les communications par private mobile radio (PMR), aujourd'hui principalement les talkies walkies numériques, et les transmissions entre objets connectés, qui peuvent n'appartenir qu'à une seule personne* »[3].

La CNCTR constate que ces nouvelles interceptions de sécurité visent des correspondances échangées au sein de réseaux et au moyen de matériels spécifiques. De telles interceptions, réalisées de manière décentralisée, nécessitent l'acquisition par les services de renseignement de dispositifs

3 - Voir le rapport n° 164 fait au nom de la commission des lois de l'Assemblée nationale par M. Raphaël GAUVIN, député, enregistré le 14 septembre 2017, page 239. On pourra également consulter les pages 29 à 33 de l'avis n° 161 fait au nom de la commission de la défense de l'Assemblée nationale par M. Guillaume GOUFFIER-CHA, député, enregistré le 14 septembre 2017.

lourds et onéreux dont l'usage suppose des compétences techniques particulières, notamment pour positionner ces dispositifs de manière adéquate ou pour déterminer la fréquence à intercepter. La commission relève également que le traitement des données recueillies se heurte à des contraintes techniques.

La CNCTR estime, en conséquence, que la mise en œuvre de la technique prévue à l'article L. 852-2 du code de la sécurité intérieure devrait être réservée aux services du « second cercle » attestant un besoin réel et disposant de capacités opérationnelles adaptées.

La commission n'émet en revanche pas d'objection, eu égard aux usages susceptibles d'être faits des réseaux de communication hertziens privatifs, à ce que les services du « second cercle » pertinents puissent intercepter les correspondances échangées sur ces réseaux pour défendre ou promouvoir, en fonction de leurs missions respectives, les intérêts fondamentaux de la Nation mentionnés aux 1°, 4°, 5° et 6° de l'article L. 811-3 du code de la sécurité intérieure, à savoir :

- l'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- 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, 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.

2. Sur la désignation des services

La CNCTR livre ses commentaires par service, dans le même ordre que celui suivi dans le projet de décret qui lui est soumis.

2.1 Services de la direction générale de la police nationale

a) Direction centrale de la police judiciaire (DCPJ)

Le projet de décret soumis à l'avis de la CNCTR prévoit que le service central des courses et jeux, la sous-direction de la lutte contre la criminalité organisée et la délinquance financière, la sous-direction antiterroriste et la sous-direction de la lutte contre la cybercriminalité ainsi que les services territoriaux (les directions interrégionales et régionales de police judiciaire, les services régionaux de police judiciaire et les antennes de police judiciaire) pourraient être autorisés à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure, au titre des finalités prévues au 4° et/ou au 6° de l'article L. 811-3 du même code.

La commission émet un avis favorable à ce que les trois sous-directions évoquées ci-dessus puissent être autorisées à mettre en œuvre la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure, au besoin avec le concours du service interministériel d'assistance technique (SIAT).

La CNCTR estime en revanche que les missions du service central des courses et jeux ne justifient pas que ce service puisse recourir aux interceptions de sécurité hertziennes.

La commission émet également un avis défavorable à ce que les services territoriaux de police judiciaire puissent être autorisés à recourir à la technique mentionnée à l'article L. 852 2 du code de la sécurité intérieure eu égard, d'une part, aux contraintes techniques, opérationnelles et financières qui caractérisent ces interceptions et, d'autre part, au faible nombre de demandes qu'ont à ce jour présentées les services territoriaux de police judiciaire pour mettre en œuvre des techniques de renseignement complexes.

b) Direction centrale de la police aux frontières (DCPAF)

Le projet de décret soumis à l'avis de la CNCTR prévoit que l'office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre (OCRIEST) pourrait être autorisé à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure, au titre de la finalité prévue au 6° de l'article L. 811-3 du même code.

La CNCTR émet un avis défavorable eu égard, d'une part, aux contraintes techniques, opérationnelles et financières qui caractérisent les interceptions de sécurité hertziennes et, d'autre part, au faible nombre de demandes qu'a présentées à ce jour l'OCRIEST pour mettre en œuvre des techniques de renseignement complexes.

c) Direction centrale de la sécurité publique

Le projet de décret soumis à l'avis de la CNCTR prévoit que les services du renseignement territorial pourraient être autorisés à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure, au titre des finalités prévues aux 1°, 4°, 5° et 6° de l'article L. 811-3 du même code.

La CNCTR rappelle que le service central du renseignement territorial (SCRT) exerce une mission exclusive de renseignement destinée à compléter celle de la direction générale de la sécurité intérieure.

La commission admet, dans ces conditions, que l'unité nationale de recherche et d'appui du SCRT puisse être autorisée à recourir aux interceptions de sécurité hertziennes.

En revanche, la CNCTR émet un avis défavorable à ce que les échelons territoriaux du SCRT puissent être autorisés à y recourir eu égard, d'une part, aux contraintes techniques, opérationnelles et financières qui caractérisent ces interceptions et, d'autre part, au faible nombre de demandes qu'ont à ce jour présentées les échelons territoriaux du SCRT pour mettre en œuvre des techniques de renseignement complexes.

2.2 Services de la direction générale de la gendarmerie nationale (DGGN)

a) Direction des opérations et de l'emploi (DOE)

Le projet de décret soumis à l'avis de la CNCTR prévoit que la sous-direction de l'anticipation opérationnelle (SDAO) et la sous-direction de la police judiciaire (SDPJ) pourraient être autorisées à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure, au titre, respectivement, des finalités prévues aux 1°, 4° et 5° ou aux 1°, 4° et 6° de l'article L. 811-3 du même code.

La CNCTR rappelle que la SDAO a exclusivement pour compétence la prévention des menaces dans les domaines de la défense, de l'ordre public et de la sécurité nationale et contribue à la mise en œuvre de la mission de renseignement confiée à la gendarmerie nationale par l'article L. 421-1 du code de la sécurité intérieure.

La commission n'émet, dès lors, aucune objection à ce qu'elle puisse être autorisée à mettre en œuvre la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure.

Si la SDPJ a une vocation essentiellement judiciaire et n'exerce qu'à titre accessoire une mission de prévention relevant de la police administrative, la commission admet, compte tenu des besoins opérationnels pour prévenir la criminalité et la délinquance organisées ainsi que le risque terroriste, que la faculté de recourir à la technique en cause lui soit également ouverte.

b) Sections de recherches de la gendarmerie nationale (SR)

Le projet de décret soumis à l'avis de la CNCTR prévoit que les sections de recherches de la gendarmerie nationale pourraient être autorisées à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure au titre des finalités mentionnées aux 4° et 6° de l'article L. 811-3 du même code.

La CNCTR émet un avis défavorable eu égard, d'une part, aux contraintes techniques, opérationnelles et financières qui caractérisent les interceptions de sécurité hertziennes et, d'autre part, au faible nombre de demandes qu'ont à ce jour présentées les SR de la gendarmerie nationale pour mettre en œuvre des techniques de renseignement complexes.

2.3 Services de la préfecture de police de Paris

Le projet de décret soumis à l'avis de la CNCTR prévoit que la sous-direction de la sécurité intérieure et celle du renseignement territorial, relevant toutes deux de la direction du renseignement de la préfecture de police (DRPP), pourraient être autorisées à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure au titre des finalités prévues aux 4°, 5° et 6° de l'article L. 811-3 du même code.

La commission, compte tenu de la mission exclusive de renseignement assurée par ces services, n'émet pas d'objection à ce qu'ils puissent être autorisés à mettre en œuvre des interceptions de sécurité hertziennes, au besoin avec le concours de la direction générale de la sécurité intérieure, comme le prévoit le projet de décret.

2.4 Services placés sous l'autorité d'emploi du ministère de la défense

Le projet de décret soumis à l'avis de la CNCTR prévoit que les sections de recherches de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement pourraient être autorisées à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure au titre des finalités prévues aux 1°, 4° et 6° de l'article L. 811-3 du même code.

Destinées à protéger des bases de défense maritimes ou aériennes ainsi que des implantations de la direction générale de l'armement, ces sections de recherches spécialisées, placées pour emploi sous l'autorité du ministre de la défense, se distinguent des sections de recherche de droit commun de la gendarmerie. La CNCTR estime que les enjeux de sécurité nationale propres aux missions des sections de recherches spécialisées justifient de leur accorder la faculté de recourir à certaines techniques de renseignement.

La commission admet, dans ces conditions, que les sections de recherches de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement puissent être autorisées à recourir aux interceptions de sécurité hertziennes.

2.5 Services de la direction de l'administration pénitentiaire

Le projet de décret soumis à l'avis de la CNCTR prévoit que le bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire pourraient être autorisés à recourir à la technique mentionnée à l'article L. 852-2 du code de la sécurité intérieure, au titre des finalités prévues aux 4° et 6° de l'article L. 811-3 du même code.

La CNCTR relève que le bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire se consacrent exclusivement à des missions de renseignement. La commission constate en outre que ces services développent actuellement leur expertise technique en la matière.

En outre, l'administration pénitentiaire a fait valoir que le déploiement en cours, au sein des établissements pénitentiaires, de dispositifs de brouillage visant à neutraliser les communications illicites sur un large spectre de fréquences empruntées par les opérateurs téléphoniques pourrait conduire les personnes détenues à employer de nouveaux moyens techniques de communication tels que la private mobile radio.

En conséquence, la CNCTR émet un avis favorable à ce que le bureau central du renseignement pénitentiaire et les cellules interrégionales du renseignement pénitentiaire puissent être autorisés à recourir à des interceptions de sécurité hertziennes. La commission estime cependant que l'expertise technique et opérationnelle requise pour mettre en œuvre ces interceptions impose que leur exécution, à l'exclusion de toute mesure d'exploitation des données recueillies, soit systématiquement confiée un opérateur disposant des compétences requises.

Annexe n° 4

Délibération de la CNCTR n° 3/2018 du 7 juin 2018

Saisie le 29 mai 2018 pour avis par le Premier ministre, 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, après avis favorable de la commission[1], par une décision du Premier ministre du 26 avril 2017. Il avait alors été porté de 2700 à 3040. Le Premier ministre se propose désormais de l'élever à 3 600, soit une hausse d'un peu plus de 18 %.

La CNCTR a constaté à nouveau que le contingent en vigueur n'était pas loin d'être entièrement utilisé. Eu égard en particulier à la persistance d'une menace terroriste élevée, 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 la délibération de la CNCTR n° 3/2017 du 26 avril 2017.

Annexe n° 5

Délibération n° 4/2018 du 8 novembre 2018

Saisie pour avis le 28 octobre 2018 par la ministre des armées[1] d'un projet d'arrêté pris pour l'application de l'article L. 2371-2 du code de la défense, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

L'article L. 2371-2 du code de la défense[2] prévoit que, sous réserve d'une déclaration préalable à la CNCTR, la direction générale de l'armement ainsi que certaines unités des forces armées sont autorisées à effectuer des essais d'appareils ou dispositifs permettant de mettre en œuvre des recueils de données de connexion par *IMSI catcher* (il s'agit de la technique de renseignement prévue à l'article L. 851-6 du code de la sécurité intérieure), des interceptions de correspondances par *IMSI catcher* (II de l'article L. 852-1 du code de la sécurité intérieure), des interceptions de correspondances empruntant exclusivement une voie hertzienne privative (article L. 852-2 du code de la sécurité intérieure), des mesures de surveillance des communications électroniques internationales (article L. 854-1 du code de la sécurité intérieure) et des interceptions de communications empruntant exclusivement une voie hertzienne ouverte (article L. 855-1 A du code de la sécurité intérieure).

Les essais autorisés par l'article L. 2371-2 du code de la défense portent sur des matériels et dispositifs destinés à appuyer l'action des forces armées engagées dans des opérations à l'étranger, en leur donnant la maîtrise d'outils qui permettent le recueil hors du territoire national de renseignements d'intérêt militaire.

---

1 - Voir le courrier n° 001D18030078 ARM/SGA/DAJ/D2P/DPSP du 25 octobre 2018, adressé au président de la CNCTR par la directrice des affaires juridiques du ministère des armées et reçu le 28 octobre suivant.

2 - La rédaction en vigueur résulte de l'article 36 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

Les essais étant susceptibles d'être effectués en France, les dispositions rappelées ci-dessus instituent une autorisation, sans laquelle les essais constitueraient des infractions pénales, dès lors qu'ils sont susceptibles d'entraîner l'interception résiduelle de communications privées[3].

L'article L. 2371-2 du code de la défense entoure la conduite des essais de plusieurs garanties. Une déclaration préalable est adressée à la CNCTR. Les essais sont réalisés par des agents individuellement désignés et habilités, à la seule fin d'effectuer ces opérations techniques et à l'exclusion de toute exploitation des données recueillies. Ces données ne peuvent être conservées que pour la durée des essais et sont détruites au plus tard une fois les essais terminés. La CNCTR est informée du champ et de la nature des essais effectués. Un registre recensant les opérations techniques réalisées est communiqué, à sa demande, à la commission.

Le projet d'arrêté soumis à la CNCTR a pour but de fixer les conditions d'application de ces garanties.

L'article 1er du projet d'arrêté précise la nature des essais autorisés par la loi, en les liant aux travaux de recherche et de développement, de vérification, de validation et de qualification des appareils ou dispositifs concernés.

La CNCTR n'émet pas d'objection à cette précision, qui renforce l'encadrement légal des essais.

Les articles 2 et 3 du projet d'arrêté énumèrent les informations que doivent comporter, d'une part, la déclaration adressée à la CNCTR avant tout essai et, d'autre part, le registre recensant les opérations réalisées.

La CNCTR considère que les informations prévues, qui incluent notamment l'auteur des essais, leur objectif, leur date, leur durée, leur lieu, les matériels ou dispositifs sur lesquels ils portent ainsi que les attestations de non exploitation et d'effacement des données recueillies, sont de nature à permettre à la commission d'assurer le contrôle que la loi lui confie sur ces essais.

3 - Voir l'étude d'impact (pages 139 et suivantes) jointe par le Gouvernement au projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense. Voir également le rapport (pages 396 et suivantes du tome I) fait le 14 mars 2018 au nom de la commission de la défense nationale et des forces armées de l'Assemblée nationale sur le même projet de loi.

La CNCTR ajoute que, si le projet d'arrêté ne fixe pas de délai pour adresser à la commission la déclaration préalable, celle-ci devra lui parvenir avec un délai suffisant pour que la CNCTR puisse utilement l'examiner et formuler, le cas échéant, les observations nécessaires pour garantir le respect de la loi.

Dans les conditions énoncées par la présente délibération, la CNCTR émet un avis favorable au projet d'arrêté soumis par la ministre des armées.

Annexe n° 6

Décision du Conseil d'État statuant au contentieux

N° 420739

Publié au recueil Lebon

Formation spécialisée

M^me^ Emmanuelle Prada Bordenave, rapporteur

M. Gilles Pellissier, rapporteur public

Lecture du lundi 18 juin 2018

AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête du 15 mai 2018, enregistrée le 18 mai 2018 au secrétariat du contentieux du Conseil d'État, le procureur de la République près le tribunal de grande instance de X... demande au Conseil d'État de vérifier la régularité de la mise en œuvre d'une technique de renseignement.

Vu les autres pièces du dossier ;

Vu :

- le code de procédure pénale ;
- le code de la sécurité intérieure ;
- la loi n° 2015-912 du 24 juillet 2015 ;
- le code de justice administrative ;

Après avoir convoqué à une séance à huis-clos, 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. Gilles Pellissier, rapporteur public ;

Considérant ce qui suit :

1. Aux termes du premier alinéa de l'article L. 821-1 du code de la sécurité intérieure : « *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* ». Elle exerce sa mission dans les conditions prévues aux articles L. 833-2 à L. 833-11 du même code et peut, notamment, en vertu de l'article L. 833-4, procéder « *de sa propre initiative (...) 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* ».

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. / (...) / 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, y compris celles qui, initiées avant cette date, ont continué à être mises en œuvre après.

3. Selon l'article L. 773-2 du code de justice administrative, les renvois présentés sur le fondement de l'article L. 841-1 du code de la sécurité intérieure sont portés, sous les réserves prévues à cet article, devant une formation spécialisée du Conseil d'État, dont les membres et le rapporteur public sont habilités ès qualités au secret de la défense nationale. Aux termes du dernier alinéa de cet article : « *Dans le cadre de l'instruction de la requête, les membres de la formation de jugement et le rapporteur public sont autorisés à connaître de l'ensemble des pièces en possession de la Commission nationale de contrôle des techniques de renseignement ou des services mentionnés à l'article L. 811-2 du code de la sécurité intérieure et ceux désignés par le décret en Conseil d'État mentionné à l'article L. 811-4 du même code et utiles à l'exercice de leur office, y compris celles protégées au titre de l'article 413-9 du code pénal* ». Aux termes de l'article L. 773-6 du même code : « *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 (...) à la juridiction de renvoi qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une technique* ». Enfin, aux termes de son article L. 773-7 : « *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 juridiction de renvoi qu'une illégalité a été commise (...)* ».

4. Saisi d'une plainte pour atteinte à la vie privée, le procureur de la République près le tribunal de grande instance de X... demande au Conseil d'État de vérifier la régularité de la technique de renseignement mentionnée dans cette plainte.

5. La formation spécialisée a examiné 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, il y a lieu de répondre au procureur de la République près le tribunal de grande instance de X... que la vérification qu'il a sollicitée a été effectuée et que l'examen de la technique de renseignement sur laquelle il a saisi le Conseil d'État n'a révélé aucune illégalité.

D É C I D E :

Article 1er : La vérification à laquelle il a été procédé à la demande du procureur de la République près le tribunal de grande instance de X... n'a révélé aucune illégalité.

Article 2 : La présente décision sera notifiée au procureur de la République près le tribunal de grande instance de X..., au Premier ministre et à la Commission nationale de contrôle des techniques de renseignement.

Annexe n° 7

Décision du Conseil d'État statuant au contentieux

N° 412685

Publié au recueil Lebon

Formation spécialisée

M^me^ Catherine de Salins, rapporteur

M. Gilles Pellissier, rapporteur public

Lecture du mercredi 20 juin 2018

AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête, un mémoire complémentaire et deux mémoires en réplique, enregistrés les 21 juillet et 2 octobre 2017 et le 13 février 2018 au secrétariat du contentieux du Conseil d'État, M. A... B... demande au Conseil d'État :

1°) de vérifier qu'aucune technique de renseignement n'a été irrégulièrement mise en œuvre à son égard ;

2°) d'annuler la décision de recourir à des techniques de renseignement à son égard révélée par la décision de la Commission nationale de contrôle des techniques de renseignement du 26 juin 2017 ;

3°) d'annuler les décisions nommant les membres de la Commission nationale de contrôle des techniques de renseignement ;

4°) d'ordonner la destruction des données interceptées le concernant.

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 ;
- la loi n° 2015-912 du 24 juillet 2015 ;
- le code de justice administrative ;

Après avoir convoqué à une séance à huis-clos, d'une part, M. A... B..., 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 Mme Catherine de Salins, conseillère d'État,
- et, hors la présence des parties, les conclusions de M. Gilles Pellissier, rapporteur public ;

Considérant ce qui suit :

1. Aux termes du premier alinéa de l'article L. 821-1 du code de la sécurité intérieure : « *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 : « *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, y compris celles qui, initiées avant cette date, ont continué à être mises en œuvre après.

3. Aux termes de l'article L. 773-1 du code de justice administrative : « *Le Conseil d'État examine les requêtes présentées sur le fondement des articles L. 841-1 et L. 841-2 du code de la sécurité intérieure conformément aux règles générales du présent code, sous réserve des dispositions particulières du présent chapitre* » ; aux termes de l'article L. 773-2 du même code : « *Sous réserve de l'inscription à un rôle de l'assemblée du contentieux ou de la section du contentieux qui siègent alors dans une formation restreinte, les affaires relevant du présent chapitre sont portées devant une formation spécialisée (...). Dans le cadre de l'instruction de la*

requête, les membres de la formation de jugement et le rapporteur public sont autorisés à connaître de l'ensemble des pièces en possession de la Commission nationale de contrôle des techniques de renseignement ou des services mentionnés à l'article L. 811-2 du code de la sécurité intérieure et ceux désignés par le décret en Conseil d'État mentionné à l'article L. 811-4 du même code et utiles à l'exercice de leur office, y compris celles protégées au titre de l'article 413-9 du code pénal ». Aux termes de l'article L. 773-3 du même code : « *Les exigences de la contradiction mentionnées à l'article L. 5 du présent code sont adaptées à celles du secret de la défense nationale (...) /. La formation chargée de l'instruction entend les parties séparément lorsqu'est en cause le secret de la défense nationale* ». Aux termes de l'article L. 773-4 du même code : « *Le président de la formation de jugement ordonne le huis-clos lorsque est en cause le secret de la défense nationale* ». Aux termes de l'article L. 773-6 du même code : « *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 : « *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. B... a saisi la Commission nationale de contrôle des techniques de renseignement (CNCTR) le 15 mai 2017 afin de vérifier qu'aucune technique de renseignement n'était irrégulièrement mise en œuvre à son égard. Par lettre du 26 juin 2017, le président de la Commission a informé M. B... 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. B... demande au Conseil d'État de vérifier si des techniques de renseignement ont été mises en œuvre pour le surveiller, le cas échéant, de constater qu'elles l'ont été illégalement, enfin, d'annuler la décision de les mettre en œuvre et d'ordonner la destruction des éléments ainsi recueillis. Il demande également l'annulation pour excès de pouvoir des décisions nommant les membres de la CNCTR.

5. Il ressort des pièces du dossier que les décisions nommant les membres de la CNCTR ont été publiées au Journal officiel le 2 octobre 2015. Les conclusions de M. B... tendant à leur annulation pour excès de pouvoir, présentées pour la première fois dans son mémoire enregistré le 13 février 2018, soit après l'expiration du délai de deux mois prévu à l'article R. 421-1 du code de justice

administrative, sont, en tout état de cause, tardives et, par suite, irrecevables.

6. Il appartient à la formation spécialisée, créée par l'article L. 773-2 du code de justice administrative, saisie de conclusions tendant à ce qu'elle s'assure qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à l'égard du requérant, 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.

7. La formation spécialisée a examiné, selon les modalités décrites au point précédent, 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. Si M. B... allègue que le président de la CNCTR n'aurait pas été impartial et que les vérifications opérées par la Commission devraient, par suite, être écartées des débats, il n'assortit cette allégation d'aucun élément permettant d'en apprécier le bien fondé. Il ne saurait également invoquer utilement, à cet effet, l'illégalité dont serait entachée la nomination des membres de cette commission. À l'issue de l'examen auquel s'est livré la formation spécialisée, il y a lieu de répondre à M. B... que la vérification qu'il a sollicitée a été effectuée et que, n'ayant révélé aucune illégalité, notamment aucune méconnaissance de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, elle n'appelle aucune mesure de la

part du Conseil d'État. Par suite, doivent être également rejetées ses conclusions tendant à l'annulation de la décision de recourir illégalement à des techniques de renseignement à son égard et à l'indemnisation du préjudice qui en aurait résulté pour lui.

DÉCIDE :

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

Article 2 : Le surplus des conclusions de sa requête est rejeté.

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

Annexe n° 8

Décision du Conseil d'État statuant au contentieux

N° 393099

Publié au recueil Lebon

10e - 9e chambres réunies

M. Vincent Villette, rapporteur

M. Édouard Crépey, rapporteur public

Lecture du jeudi 26 juillet 2018

AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête sommaire, un mémoire complémentaire et quatre autres mémoires, enregistrés les 1er septembre et 27 novembre 2015, le 24 mai 2016, le 25 juillet 2016, le 7 février 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'État, *French Data Network*, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs demandent au Conseil d'État :

1°) d'annuler pour excès de pouvoir la décision implicite de rejet résultant du silence gardé par le Premier ministre sur leur demande tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du décret n° 2011-219 du 25 février 2011 ;

2°) d'enjoindre au Premier ministre d'abroger ces dispositions ;

3°) de mettre à la charge de l'État la somme de 1 024 euros au titre de l'article L. 761-1 du code de justice administrative.

Vu les autres pièces du dossier ;

Vu :

- la Charte des droits fondamentaux de l'Union européenne ;
- la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;
- la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 ;
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 ;
- le code des postes et des communications électroniques ;
- la loi n° 2004-575 du 21 juin 2004 ;
- la loi n° 2013-1168 du 18 décembre 2013 ;
- le décret n° 2011-219 du 25 février 2011 ;
- l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016, *Tele2 Sverige AB c/ Post-och telestyrelsen* et *Secretary of State for the Home Department c/* Tom Watson et autres (C-203/15 et C-698/15) ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Vincent Villette, maître des requêtes,
- les conclusions de M. Édouard Crépey, rapporteur public ;

Considérant ce qui suit :

1. *Privacy International* et le *Center for Democracy and Technology* ont intérêt à l'annulation de la décision attaquée. Ainsi, leur intervention est recevable.

2. *French Data Network,* la Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs ont demandé au Premier ministre d'abroger l'article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Ces trois associations attaquent la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande.

3. L'autorité compétente, saisie d'une demande tendant à l'abrogation d'un règlement illégal, est tenue d'y déférer, soit que, réserve faite des vices de forme et de procédure dont il serait entaché, ce règlement ait été illégal dès la date de sa signature, soit que l'illégalité résulte de circonstances de droit ou de fait postérieures à cette date.

Sur le refus d'abroger l'article R. 10-13 du code des postes et des communications électroniques :

4. Aux termes de l'article L. 34-1 du code des postes et des communications électroniques dans sa rédaction applicable : « *I.-Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification. / II.-Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI. / Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes. / Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au*

réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. / III.-Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs ». L'article R. 10 13 de ce même code, dont les requérants ont demandé l'abrogation, met en œuvre les dispositions précitées du III de l'article L. 34-1, notamment en énumérant les données qui doivent être conservées par les opérateurs de communications électroniques et en fixant à un an leur durée de conservation.

5. En premier lieu, contrairement à ce que soutiennent les intervenants, le fait que l'obligation de conservation décrite au point précédent revête un caractère général sans être limitée à des personnes ou circonstances particulières n'est pas, par lui-même, contraire aux exigences découlant des stipulations de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

6. En second lieu, d'une part, aux termes de l'article 4 du Traité sur l'Union européenne, l'Union « *respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre* ». L'article 51 de la Charte des droits fondamentaux de l'Union européenne prévoit que « *1. Les dispositions de la présente Charte s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. (...) 2. La présente Charte n'étend pas le champ d'application du droit de l'Union au-delà des compétences de l'Union, ni ne crée aucune compétence ni aucune tâche nouvelles pour l'Union et ne modifie pas les compétences et tâches définies dans les traités* ». Aux termes de son article 54 : « *Aucune des dispositions de la présente Charte ne doit être interprétée comme impliquant un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Charte (...)* ».

7. D'autre part, la directive 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, qui a été prise sur le fondement de l'article 95 du traité instituant la Communauté européenne, désormais repris à l'article 114 du traité sur le fonctionnement de l'Union européenne, procède de la volonté de rapprocher les législations des États membres afin de permettre l'établissement et le fonctionnement du marché intérieur. Elle a pour objet, ainsi que l'énonce le paragraphe 1 de son article 3, le « *traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans la Communauté* ». Mais, ainsi que le rappelle son article 1er, paragraphe 3, elle « *ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne (...) et, en tout état de cause, aux activités concernant la sécurité publique, la défense,*

la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal ». Par ailleurs, son article 15 prévoit que « *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne* ». Les États membres sont ainsi autorisés, pour des motifs tenant à la sûreté de l'État ou à la lutte contre les infractions pénales, à déroger, notamment, à l'obligation de confidentialité des données à caractère personnel, ainsi que de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1 de la directive.

En ce qui concerne l'obligation de conservation généralisée et indifférenciée :

8. Par son arrêt du 21 décembre 2016, *Tele2 Sverige AB c/ Post-och telestyrelsen* et *Secretary of State for the Home Department c/* Tom Watson et autres (C-203/15 et C-698/15), la Cour de justice de l'Union européenne a dit pour droit que l'article 15, paragraphe 1, de cette directive, « *lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il*

s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ».

9. D'une part, il est constant qu'une telle conservation préventive et indifférenciée permet à l'autorité judiciaire d'accéder aux données relatives aux communications qu'un individu a effectuées avant d'être suspecté d'avoir commis une infraction pénale. Une telle conservation présente dès lors une utilité sans équivalent pour la recherche, la constatation et la poursuite des infractions pénales.

10. D'autre part, ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 21 décembre 2016, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au « *contenu essentiel* » des droits consacrés par les articles 7 et 8 de la Charte. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017, que ces droits « *n'apparaissent pas comme étant des prérogatives absolues* » et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que « *la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui* » et que « *l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté* ».

11. Dans ces conditions la question de déterminer si l'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les

exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États-membres en vertu de l'article 4 du traité sur l'Union européenne, soulève une première difficulté d'interprétation du droit de l'Union européenne.

Sur le refus d'abroger les dispositions du chapitre Ier du décret du 25 février 2011 :

12. Le premier alinéa du II de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit que les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services « *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ». Le troisième alinéa du II prévoit que l'autorité judiciaire peut requérir communication auprès de ces personnes des données mentionnées au premier alinéa. Le dernier alinéa du II dispose qu'un décret en Conseil d'État « *définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation* ». Le premier chapitre du décret du 25 février 2011 a été pris à cette fin.

13. Le II de l'article 6 de la loi du 21 juin 2004, qui impose une obligation de détention et de conservation des seules données relatives à la création de contenu, n'entre pas dans le champ d'application de la directive du 12 juillet 2002, clairement réservé, aux termes de son article 3, paragraphe 1, « *au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté* ».

14. En revanche, les dispositions précitées du II de l'article 6 de la loi du 21 juin 2004 relèvent, de façon claire, du champ d'application de la directive 2000/31/CE du Parlement européen et du Conseil du

8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, laquelle a, aux termes de son article 1er, paragraphe 1, « *pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres* ». Les articles 12 et 14 de cette directive sont relatifs aux services respectivement fournis par les fournisseurs de services de communication au public et par les prestataires au titre de l'hébergement. L'article 15, paragraphe 1, de cette directive prévoit que « *Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites* ». Aux termes du paragraphe 2 de ce même article : « *Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement* ». Ainsi, la directive n'instaure pas, par elle-même, une interdiction de principe quant à la conservation des données relatives à la création de contenu, à laquelle il pourrait seulement être dérogé par exception.

15. La question de déterminer si ces dispositions précitées de la directive du 8 juin 2000 lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doivent être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes rappelées au point 12 de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité

judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale, soulève une seconde difficulté sérieuse d'interprétation du droit de l'Union européenne.

16. Les deux questions énoncées aux points 11 et 15 sont déterminantes pour la solution complète du litige que doit trancher le Conseil d'État. Elles présentent, ainsi qu'il a été dit, des difficultés sérieuses d'interprétation du droit de l'Union européenne. Il y a lieu, par suite, d'en saisir la Cour de justice de l'Union européenne en application de l'article 267 du traité sur le fondement de l'Union européenne et, jusqu'à ce que celle-ci se soit prononcée, de surseoir à statuer sur la requête des associations requérantes.

DÉCIDE :

Article 1er : L'intervention de *Privacy International* et du *Center for Democracy and Technology* est admise.

Article 2 : Il est sursis à statuer sur la requête de *French Data Network*, la Quadrature du net et la Fédération des fournisseurs d'accès à Internet associatifs, jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur la question suivante :

1° L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États-membres en vertu de l'article 4 du traité sur l'Union européenne ?

2° Les dispositions de la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doivent-elles être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes

dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ?

Article 3 : La présente décision sera notifiée à *French Data Network*, à la Quadrature du net, à la Fédération des fournisseurs d'accès à Internet associatifs, au Premier ministre, à la garde des sceaux, ministre de la justice, et au greffier de la Cour de justice de l'Union européenne.

Annexe n° 9

Décision du Conseil d'État statuant au contentieux

N° 394922

Publié au recueil Lebon

10e - 9e chambres réunies

M. Vincent Villette, rapporteur

M. Édouard Crépey, rapporteur public

Lecture du jeudi 26 juillet 2018

AU NOM DU PEUPLE FRANCAIS

1° Sous le numéro 394922, par une requête sommaire, un mémoire complémentaire et trois autres mémoires, enregistrés le 30 novembre 2015, le 29 février 2016 et le 6 mai 2016, le 13 novembre 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'État, la Quadrature du Net, *French Data Network* et la Fédération des fournisseurs d'accès à Internet associatifs demandent au Conseil d'État :

1°) d'annuler pour excès de pouvoir le décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'État la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

2° Sous le numéro 394925, par une requête sommaire, un mémoire complémentaire et trois autres mémoires, enregistrés le 30 novembre 2015, le 29 février 2016 et le 6 mai 2016, le 13 novembre 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'État, la Quadrature du Net, *French Data Network* et la Fédération des fournisseurs d'accès à Internet associatifs demandent au Conseil d'État :

1°) d'annuler pour excès de pouvoir le décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'État la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

3° Sous le numéro 397844, par une requête sommaire, un mémoire complémentaire et deux autres mémoires, enregistrés le 11 mars 2016, le 6 mai 2016, le 13 novembre 2017 et le 10 juillet 2018 au secrétariat du contentieux du Conseil d'État, l'association Igwan.net demande au Conseil d'État :

1°) d'annuler pour excès de pouvoir 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 ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'État la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

4° Sous le numéro 397851, par une requête sommaire, un mémoire complémentaire et deux autres mémoires, enregistrés le 11 mars 2016, le 19 mai 2016, le 24 novembre 2017 et le 10 juillet 2018 au

secrétariat du contentieux du Conseil d'État, la Quadrature du Net, *French Data Network* et la Fédération des fournisseurs d'accès à Internet associatifs demandent au Conseil d'État :

1°) d'annuler pour excès de pouvoir le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement ;

2°) à titre subsidiaire, de renvoyer à la Cour de justice de l'Union européenne plusieurs questions préjudicielles ;

3°) de mettre à la charge de l'État la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Vu :

- la Constitution, notamment son Préambule et ses articles 61-1 et 62 ;
- le traité sur l'Union européenne ;
- le traité sur le fonctionnement de l'Union européenne ;
- la Charte des droits fondamentaux de l'Union européenne ;
- la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;
- la convention du 23 novembre 2001 sur la cybercriminalité ;
- la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 ;
- la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 ;
- le code de la sécurité intérieure, notamment son livre VIII ;
- la décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016 ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Vincent Villette, maître des requêtes ;
- les conclusions de M. Édouard Crépey, rapporteur public ;

La parole ayant été donnée, avant et après les conclusions, à la SCP Spinosi et Sureau, avocat de la Quadrature du Net, de *French Data Network* et de la Fédération des fournisseurs d'accès à Internet associatifs ;

Considérant ce qui suit :

1. Par trois requêtes, la Quadrature du Net, *French Data Network* et la Fédération des fournisseurs d'accès à Internet associatifs demandent l'annulation pour excès de pouvoir, sous le numéro 394922 du décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement, sous le numéro 394925 du décret du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État, et sous le numéro 397851 du décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement. L'association Igwan.net, sous le numéro 397844, demande l'annulation du décret 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. Ces requêtes présentent à juger les mêmes questions. Il y a lieu de les joindre pour statuer par une seule décision.

Sur les moyens de légalité externe :

2. Lorsque, comme en l'espèce, un décret doit être pris en Conseil d'État, le texte retenu par le Gouvernement ne peut être différent à la fois du projet qu'il a soumis au Conseil d'État et du texte adopté par ce dernier. Il ressort des copies des minutes de la section de l'intérieur du Conseil d'État, telles qu'elles ont été produites au dossier par le Premier ministre, que le texte des quatre décrets attaqués ne contient pas de disposition qui diffèrerait à la fois du projet initial du Gouvernement et du texte adopté par la section. Il s'ensuit que les moyens tirés de la méconnaissance des règles qui gouvernent l'examen par le Conseil d'État des projets de décret doivent être écartés.

Sur les moyens de légalité interne :

En ce qui concerne le moyen tiré de la méconnaissance de l'article L. 851-1 du code de la sécurité intérieure par le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement :

3. Les dispositions de l'article R. 851-5 du code de la sécurité intérieure créées par le décret du 29 janvier 2016 relatif aux techniques de recueil de renseignement qui définissent les données de connexion susceptibles d'être recueillies auprès des opérateurs de communications électroniques excluent des données ainsi recueillies le contenu des correspondances échangées ou des informations consultées. En outre, ces dispositions réservent le recueil de certaines de ces données aux seules techniques de renseignement prévues aux articles L. 851-2 et L. 851-3 du code de la sécurité intérieure, lesquelles ne sont mises en œuvre que pour les seuls besoins de la prévention du terrorisme. Ce faisant, contrairement à ce que soutiennent les associations requérantes, ces dispositions réglementaires ne méconnaissent pas les dispositions de l'article L. 851-1 du même code pour l'application desquelles elles ont été prises.

En ce qui concerne les moyens invoqués par la voie de l'exception :

4. À l'appui de leurs conclusions, les requérants soulèvent des moyens, par la voie de l'exception, à l'encontre de l'ensemble des dispositions du livre VIII du code de la sécurité intérieure, de celles du chapitre III bis du titre VII du livre VII du code de justice administrative et de celles de l'article 323-8 du code pénal.

S'agissant du moyen tiré de la contrariété à la Constitution de l'article L. 811-5 du code de la sécurité intérieure :

5. Par sa décision n° 2016-590 QPC du 21 octobre 2016, le Conseil constitutionnel a déclaré l'article L. 811-5 du code de la sécurité intérieure contraire au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration de 1789. Le dispositif de cette décision énonce que la déclaration d'inconstitutionnalité prend effet dans les conditions prévues aux

paragraphes 11 et 12. Aux termes de ces paragraphes : « *L'abrogation immédiate de l'article L. 811-5 du code de la sécurité intérieure aurait pour effet de priver les pouvoirs publics de toute possibilité de surveillance des transmissions empruntant la voie hertzienne. Elle entraînerait des conséquences manifestement excessives. Afin de permettre au législateur de remédier à l'inconstitutionnalité constatée, il y a donc lieu de reporter au 31 décembre 2017 la date de cette abrogation. / Afin de faire cesser l'inconstitutionnalité constatée à compter de la publication de la présente décision, il y a lieu de juger que, jusqu'à l'entrée en vigueur d'une nouvelle loi ou, au plus tard, jusqu'au 30 décembre 2017, 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 au titre II ou au chapitre IV du titre V du livre VIII du code de la sécurité intérieure. Pendant le même délai, les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne sauraient être mises en œuvre sans que la Commission nationale de contrôle des techniques de renseignement soit régulièrement informée sur le champ et la nature des mesures prises en application de cet article* ». Alors même que, selon les motifs de la décision du Conseil constitutionnel, la déclaration d'inconstitutionnalité doit, en principe, bénéficier à l'auteur de la question prioritaire de constitutionnalité, l'absence de prescriptions relatives à la remise en cause des effets produits par l'article L. 811-5 du code de la sécurité intérieure avant son abrogation doit, en l'espèce, eu égard, d'une part, à la circonstance que la question prioritaire de constitutionnalité a été soulevée à l'occasion de recours pour excès de pouvoir dirigés contre des actes réglementaires, d'autre part, à la circonstance que le Conseil constitutionnel a décidé de reporter dans le temps les effets abrogatifs de sa décision, être regardée comme indiquant que le Conseil constitutionnel n'a pas entendu remettre en cause les effets que la disposition déclarée contraire à la Constitution avait produits avant la date de son abrogation. Il s'ensuit que, alors même

que les associations requérantes sont les auteurs de la question prioritaire de constitutionnalité, la déclaration d'inconstitutionnalité de l'article L. 811-5 du code de la sécurité intérieure est, en tout état de cause, sans incidence sur l'issue des présents litiges dirigés contre les quatre décrets mentionnés au point 1.

S'agissant de l'exception d'inconventionnalité dirigée contre l'article 323-8 du code pénal :

6. La contrariété d'une disposition législative aux stipulations d'un traité international ne peut être utilement invoquée à l'appui de conclusions dirigées contre un acte réglementaire que si ce dernier a été pris pour son application ou si en elle constitue la base légale. Or le décret du 28 septembre 2015 portant désignation des services spécialisés de renseignement n'a été pris ni sur le fondement ni pour l'application des dispositions de l'article 323-8 du code pénal. Il s'ensuit que les associations requérantes ne peuvent utilement soutenir que ce décret serait dépourvu de base légale en raison de la contrariété des dispositions de l'article 323-8 du code pénal aux stipulations des articles 6 et 32 de la convention du 23 novembre 2001 sur la cybercriminalité et à celles des articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi que de l'article 1er du premier protocole additionnel à cette convention.

S'agissant des moyens tirés de la méconnaissance de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales :

7. En premier lieu, les associations requérantes soutiennent que les décrets attaqués ont été pris sur le fondement ou pour l'application de dispositions législatives qui méconnaissent le droit à un recours effectif garanti notamment par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, en raison des atteintes portées au droit au recours, aux droits de la défense et au principe du contradictoire dans le cadre du contentieux de la mise en œuvre des techniques de renseignement.

8. Les dispositions des articles L. 841-1 et L. 841-2 du code de la sécurité intérieure prévoient les conditions dans lesquelles le Conseil d'État est compétent pour connaître des requêtes concernant la mise en œuvre des techniques de renseignement soumises à autorisation. Il peut être saisi soit par toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre et justifiant d'avoir au préalable saisi la Commission nationale de contrôle des techniques de renseignement sur le fondement de l'article L. 833-4 du même code, soit par le président de cette commission, ou trois de ses membres, lorsque le Premier ministre ne donne pas suite aux avis ou aux recommandations de la commission ou que les suites qui y sont données sont estimées insuffisantes. S'agissant des mesures de surveillance des communications électroniques internationales encadrées par le chapitre IV du titre V du livre VIII du code de la sécurité intérieure, si la personne qui pense faire l'objet d'une telle mesure de surveillance ne peut directement saisir un juge pour en contester la régularité, elle peut en revanche, sur le fondement des dispositions de l'article L. 854-9 de ce code, former une réclamation à cette fin auprès de la Commission nationale de contrôle des techniques de renseignement. Or ce même article prévoit que lorsque la commission identifie un manquement, de sa propre initiative ou à la suite d'une telle réclamation, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin et que les renseignements collectés soient, le cas échéant, détruits. Elle peut également saisir le Conseil d'État.

9. Saisie de conclusions tendant à ce qu'elle s'assure qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à l'égard du requérant ou de la personne concernée, il appartient à la formation spécialisée, créée par l'article L. 773-2 du code de justice administrative, de vérifier, au vu des éléments qui lui ont été communiqués hors la procédure contradictoire, si le requérant fait ou non l'objet d'une telle technique. Dans l'affirmative, il lui appartient d'apprécier si cette technique est mise en œuvre dans le respect du livre VIII du code de la sécurité intérieure. 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 et qu'aucune illégalité n'a été commise, sans autre précision. Dans le cas où une technique de renseignement est mise en œuvre dans des conditions qui apparaissent entachées d'illégalité, elle en informe le requérant, sans faire état d'aucun élément protégé par le secret de la défense nationale. En pareil cas, par une décision distincte dont seule l'administration compétente et la Commission nationale de contrôle des techniques de renseignement sont destinataires, la formation spécialisée annule le cas échéant l'autorisation et ordonne la destruction des renseignements irrégulièrement collectés.

10. La dérogation apportée, par les dispositions contestées du code de justice administrative, au caractère contradictoire de la procédure juridictionnelle, qui a pour seul objet de porter à la connaissance des juges des éléments couverts par le secret de la défense nationale et qui ne peuvent, dès lors, être communiqués au requérant, permet à la formation spécialisée, qui entend les parties, de statuer en toute connaissance de cause. Les pouvoirs dont elle est investie, pour instruire les requêtes, relever d'office toutes les illégalités qu'elle constate et enjoindre à l'administration de prendre toutes mesures utiles afin de remédier aux illégalités constatées garantissent l'effectivité du contrôle juridictionnel qu'elle exerce.

11. Il s'ensuit que ni les conditions dans lesquelles la formation spécialisée peut être saisie ni celles dans lesquelles elle remplit son office juridictionnel ne méconnaissent, contrairement à ce qui est soutenu, le droit au recours effectif des personnes qui la saisissent, garanti notamment par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

12. En second lieu, les associations requérantes soutiennent que les décrets attaqués ont été pris sur le fondement ou pour l'application de dispositions législatives qui méconnaissent le droit au respect de la vie privée garanti notamment par l'article 8 de la convention

européenne de sauvegarde des droits de l'homme et des libertés fondamentales, en raison de l'absence de notification des mesures de surveillance aux personnes concernées après qu'elles ont été levées.

13. Eu égard, d'une part, aux attributions de la Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante à laquelle il appartient de vérifier, sous le contrôle du juge, que les techniques de recueil de renseignement sont mises en œuvre, sur le territoire national, conformément aux exigences découlant du code de la sécurité intérieure, et, d'autre part, au recours effectif ouvert, dans les conditions décrites aux points précédents, devant la formation spécialisée du Conseil d'État, la circonstance que les dispositions législatives contestées ne prévoient pas la notification aux personnes concernées des mesures de surveillance dont elles ont fait l'objet, une fois ces dernières levées, ne caractérise pas, par elle-même, une atteinte excessive portée au droit au respect de la vie privée.

14. Il résulte de ce qui précède que les moyens tirés de la contrariété des dispositions législatives contestées aux articles 8 et 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales doivent, en tout état de cause, être écartés.

S'agissant du moyen tiré de la méconnaissance de la directive du 8 juin 2000 :

15. Les dispositions de l'article L. 851-3 du code de la sécurité intérieure permettent d'imposer aux opérateurs de communications électroniques et aux prestataires techniques « *la mise en œuvre sur leurs réseaux de traitements automatisées destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste* ». Cette technique vise uniquement à recueillir pendant une durée limitée, parmi l'ensemble des données de connexion traitées par ces personnes, celles de ces données qui pourraient présenter un lien avec une telle infraction grave. Dans ces conditions, ces dispositions, qui n'imposent pas une obligation générale de

surveillance active, ne méconnaissent pas les dispositions claires de l'article 15 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, qui prévoient que « Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services de simple transport, de stockage et d'hébergement une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ». Il s'ensuit qu'en tout état de cause, le moyen tiré de la méconnaissance de la directive du 8 juin 2000 doit être écarté.

S'agissant des moyens tirés de la méconnaissance de la directive du 12 juillet 2002 et de la Charte des droits fondamentaux de l'Union européenne :

16. D'une part, aux termes de l'article 4 du Traité sur l'Union européenne, l'Union « *respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre* ». L'article 51 de la Charte des droits fondamentaux de l'Union européenne prévoit que « *1. Les dispositions de la présente Charte s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. (...) 2. La présente Charte n'étend pas le champ d'application du droit de l'Union au-delà des compétences de l'Union, ni ne crée aucune compétence ni aucune tâche nouvelles pour l'Union et ne modifie pas les compétences et tâches définies dans les traités* ». Aux termes de son article 54 : « *Aucune des dispositions de la présente Charte ne doit être interprétée comme impliquant un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Charte (...)* ».

17. D'autre part, 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, qui a été prise sur le fondement de l'article 95 du traité instituant la Communauté européenne, désormais repris à l'article 114 du traité sur le fonctionnement de l'Union européenne, procède de la volonté de rapprocher les législations des États membres afin de permettre l'établissement et le fonctionnement du marché intérieur. Elle a pour objet, ainsi que l'énonce le paragraphe 1 de son article 3, le « *traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans la Communauté* ». Mais, ainsi que le rappelle son article 1er, paragraphe 3, elle « *ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne (...) et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal* ». Par ailleurs, son article 15 prévoit que « *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes*

généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ». Les États membres sont ainsi autorisés, pour des motifs tenant à la sûreté de l'État ou à la lutte contre les infractions pénales, à déroger, notamment, à l'obligation de confidentialité des données à caractère personnel, ainsi que de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1, de la directive.

Quant au champ d'application de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 :

18. Il résulte des dispositions précitées de la directive du 12 juillet 2002, ainsi que l'a dit pour droit la Cour de justice de l'Union européenne par son arrêt *Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/* Tom Watson et autres (C-203/15 et C-698/15), du 21 décembre 2016, qu'elle « *doit être regardée comme régissant les activités des fournisseurs* [de services de communications électroniques] ». Les dispositions imposant des obligations à ces fournisseurs, telles que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation de leurs utilisateurs et abonnés, aux fins mentionnées à l'article 15, paragraphe 1, de la directive du 12 juillet 2002, parmi lesquelles figure la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique relèvent dès lors du champ d'application de cette directive dans la mesure où, ainsi que l'a dit pour droit la Cour de justice, elles régissent leur activité. Par ailleurs, ainsi que l'a également dit pour droit la Cour, la circonstance que de telles obligations n'interviennent qu'aux seules fins de rendre accessibles aux autorités nationales compétentes les données personnelles qu'elles concernent, implique que la réglementation nationale encadrant l'accès et l'utilisation de ces données relève également du champ d'application de la directive du 12 juillet 2002. En revanche, les dispositions nationales qui portent sur des techniques de recueil de renseignement directement mises en œuvre par l'État sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques ne relèvent pas du champ d'application de cette directive.

19. L'article L. 851-1 du code de la sécurité intérieure dispose que : « *Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs 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 (...)* ». Les articles L. 851-2 et L. 851-4 du code de la sécurité intérieure organisent, pour des finalités et selon des modalités différentes, des accès administratifs en temps réel aux données de connexion ainsi conservées.

20. Il résulte clairement de ce qui précède, eu égard au champ d'application de l'article 15, paragraphe 1, de la directive du 12 juillet 2002 tel qu'interprété par la Cour de justice de l'Union européenne, qu'en relèvent tant l'obligation de conservation induite par les dispositions précitées de l'article L. 851-1 du code de la sécurité intérieure que les accès administratifs aux données de connexion, y compris en temps réel, qui la justifient, prévus aux articles L. 851-1, L. 851-2 et L. 851-4 de ce code. Il en va de même des dispositions de l'article L. 851-3 du code de la sécurité intérieure qui, si elles ne font pas peser sur les opérateurs et personnes concernés une obligation préalable de conservation, leur imposent cependant de mettre en œuvre sur leurs réseaux des traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste.

21. En revanche, il résulte clairement de la directive du 12 juillet 2002 que ne relèvent pas de son champ les dispositions des articles L. 851-5 et L. 851-6, ainsi que celles des chapitres II, III et IV du titre V du livre VIII du code de la sécurité intérieure, dès lors qu'elles portent sur des techniques de recueil de renseignement qui sont directement mises en œuvre par l'État sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Dès lors, ces dispositions ne sauraient être regardées comme mettant en œuvre le droit de l'Union européenne et, par suite, les moyens tirés de la méconnaissance de la directive du 12 juillet 2002 interprétée à la lumière de la Charte des droits fondamentaux de l'Union européenne ne peuvent être utilement invoqués à leur encontre.

Quant à l'obligation de conservation généralisée et indifférenciée :

22. Par son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a dit pour droit que l'article 15, paragraphe 1, de cette directive, « *lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* ».

23. D'une part, il est constant qu'une telle conservation préventive et indifférenciée permet aux services de renseignement d'accéder aux données relatives aux communications qu'un individu a effectuées avant que soient identifiées les raisons de penser qu'il présente une menace pour la sécurité publique, la défense ou la sûreté de l'État. Dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, une telle conservation présente une utilité sans équivalent par rapport au recueil de ces mêmes données à partir seulement du moment où l'individu en cause aurait été identifié comme susceptible de présenter une menace pour la sécurité publique, la défense ou la sûreté de l'État.

24. D'autre part, ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 21 décembre 2016, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au « *contenu essentiel* » des droits consacrés par les articles 7 et 8 de la Charte. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017, que ces droits « *n'apparaissent pas comme étant des prérogatives absolues* » et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que « *la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui* » et que « *l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté* ».

25. Dans ces conditions, la question de déterminer si l'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit pas être regardée, notamment eu égard aux garanties et contrôles, évoqués aux points 7 à 13, dont sont assortis les accès administratifs aux données de connexion et l'utilisation de celles-ci, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États-membres en vertu de l'article 4 du traité sur l'Union européenne, soulève une première difficulté d'interprétation du droit de l'Union européenne.

Quant aux autres obligations susceptibles d'être imposées aux fournisseurs d'un service de communications électroniques :

26. Les dispositions de l'article L. 851-2 du code de la sécurité intérieure autorisent, pour les seuls besoins de la prévention du terrorisme, le recueil des informations ou documents prévus à l'article L. 851-1, auprès des mêmes personnes. Ce recueil, qui ne concerne qu'un ou plusieurs individus préalablement identifiés

comme étant susceptibles d'être en lien avec une menace terroriste, s'effectue en temps réel. Il en va de même des dispositions de l'article L. 851-4 du même code, qui autorisent la transmission en temps réel par les opérateurs des seules données techniques relatives à la localisation des équipements terminaux. Il suit de là que ces techniques ne font pas peser sur les fournisseurs concernés une exigence de conservation supplémentaire par rapport à ce qui est nécessaire à la facturation de leurs services, à la commercialisation de ceux-ci et à la fourniture de services à valeur ajoutée. Par ailleurs, ainsi qu'il a été rappelé au point 15, les dispositions de l'article L. 851-3 du code de la sécurité intérieure n'impliquent pas davantage une conservation généralisée et indifférenciée.

27. Or, d'une part, il est constant que les accès en temps réel aux données de connexion permettent de suivre, avec une forte réactivité, les comportements d'individus susceptibles de représenter une menace immédiate pour l'ordre public. D'autre part, la technique prévue à l'article L. 851-3 du code de la sécurité intérieure permet de détecter, sur le fondement de critères précisément définis à cette fin, les individus dont les comportements, notamment compte tenu de leurs modes de communication, sont susceptibles de révéler une menace terroriste. Dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, ces techniques présentent ainsi une utilité opérationnelle sans équivalent.

28. D'autre part, ainsi que l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 21 décembre 2016, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au « *contenu essentiel* » des droits consacrés par les articles 7 et 8 de la Charte. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017, que ces droits « *n'apparaissent pas comme étant des prérogatives absolues* » et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que « *la protection*

de la sécurité publique contribue également à la protection des droits et des libertés d'autrui » et que « *l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté* ».

29. Dans ces conditions, soulève une deuxième difficulté sérieuse d'interprétation du droit de l'Union européenne la question de déterminer si la directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne doit être interprétée en ce sens qu'elle autorise des mesures législatives relevant d'activités concernant la sécurité publique, la défense et la sûreté de l'État telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données.

Quant à l'accès des autorités nationales compétentes aux données conservées :

30. Dans son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a également dit pour droit que l'article 15, paragraphe 1, de la directive du 12 juillet 2002 « *doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union* ». La Cour a, à cette occasion, estimé « *qu'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. En effet, cette information est, de fait, nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits ».

31. Soulève une troisième difficulté sérieuse d'interprétation du droit de l'Union la question de déterminer si la directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou si de telles procédures peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours.

32. Les trois questions énoncées aux points 25 à 31 sont déterminantes pour la solution des litiges que doit trancher le Conseil d'État sur les quatre décrets attaqués en tant qu'ils ont été pris pour la mise en œuvre des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure. Elles présentent, ainsi qu'il a été dit, plusieurs difficultés sérieuses d'interprétation du droit de l'Union européenne. Il y a lieu, par suite, d'en saisir la Cour de justice de l'Union européenne en application de l'article 267 du traité sur le fonctionnement de l'Union européenne et, jusqu'à ce que celle-ci se soit prononcée, de surseoir à statuer, dans cette mesure et sans qu'il soit besoin de statuer sur les fins de non-recevoir opposées en défense, sur les requêtes des associations requérantes et de rejeter le surplus de leurs conclusions.

D É C I D E :

Article 1er : Les requêtes sont rejetées en tant qu'elles sont dirigées contre les décrets n° 2015-1185 du 28 septembre 2015, n° 2015-1211 du 1er octobre 2015, n° 2015-1639 du 11 décembre 2015 et n° 2016-67 du 29 janvier 2016 en tant qu'ils mettent en œuvre les dispositions des articles L. 851-5 et L. 851-6, ainsi que celles des chapitres II, III et IV du titre V du livre VIII du code de la sécurité intérieure.

Article 2 : Il est sursis à statuer, dans cette mesure, sur les requêtes des associations requérantes, jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée sur les questions suivantes :

1° L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États-membres en vertu de l'article 4 du traité sur l'Union européenne ?

2° La directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne doit-elle être interprétée en ce sens qu'elle autorise des mesures législatives, telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données ?

3° La directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit-elle être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les

enquêtes menées par les autorités compétentes ou de telles procédures peuvent-elles être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours ?

Article 3 : La présente décision sera notifiée à la Quadrature du Net, à l'association Igwan.net, au Premier ministre, au ministre d'État, ministre de l'intérieur, à la garde des sceaux, ministre de la justice, à la ministre des armées et au greffier de la Cour de justice de l'Union européenne. Les autres requérantes seront informées de la présente décision par la SCP Spinosi et Sureau, avocat au Conseil d'État et à la Cour de cassation, qui les représente devant le Conseil d'État.

Annexe 10

Les modifications législatives du livre VIII du code de la sécurité intérieure en 2018

Le tableau ci-dessous résume les modifications de nature législative apportées au livre VIII du code de la sécurité intérieure par l'article 37 de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

	Dispositions créées ou modifiées	Objet	Texte d'application	Délibération de la CNCTR
Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense Voir l'article 37 de la loi (entrée en vigueur le 15 juillet 2018)	Article L. 854-1 (4e alinéa)	Autorisation permettant d'exploiter les communications internationales interceptées entrant dans le champ d'application d'autorisations individuelles délivrées sous le régime de la surveillance intérieure		Délibération de la CNCTR n° 1/2018 du 9 mai 2018 Voir l'annexe n° 2 au présent rapport

	Dispositions créées ou modifiées	Objet	Texte d'application	Délibération de la CNCTR
Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense Voir l'article 37 de la loi (entrée en vigueur le 15 juillet 2018)	Article L. 854-2 (III, IV et V)	1. Avis préalable obligatoire de la CNCTR sur les demandes d'exploitation des communications internationales 2. Autorisation de réaliser des vérifications ponctuelles sur des données de connexion, voire sur des contenus de communications interceptées renvoyant à des identifiants techniques rattachables au territoire national 3. Autorisation d'exploitation de communications ou de seules données de connexion d'une personne utilisant un identifiant technique rattachable au territoire français, alors même que cette personne communique depuis la France		

	Dispositions créées ou modifiées	Objet	Texte d'application	Délibération de la CNCTR
Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense Voir l'article 37 de la loi (entrée en vigueur le 15 juillet 2018)	Article L. 854-4 Article L. 854-9	Contingentement des autorisations portant sur le contenu des communications Traçabilité des vérifications ponctuelles Examen par la CNCTR des demandes d'autorisation d'exploitation des communications internationales dans les conditions de droit commun applicables à la surveillance intérieure Droit au recours devant le juge administratif ouverte à toute personne souhaitant vérifier qu'aucune exploitation de communications internationales renvoyant à des identifiants techniques rattachables au territoire national n'a été irrégulièrement réalisée à son encontre		

	Dispositions créées ou modifiées	Objet	Texte d'application	Délibération de la CNCTR
Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense Voir l'article 36 de la loi (entrée en vigueur le 15 juillet 2018)	Article L. 2371-2 du code de la défense	Essais de matériels de renseignement par la direction générale de l'armement et certaines unités des armées, à l'exclusion de toute exploitation des données recueillies Déclaration préalable à la CNCTR	Arrêté du 3 janvier 2019 relatif aux essais de matériels de renseignement réalisés en application de l'article L. 2371-2 du code de la défense	Délibération de la CNCTR n° 4/2018 du 8 novembre 2018 Voir l'annexe n° 5 au présent rapport

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

Hôtel de Cassini - 32 rue de Babylone - 75007 Paris

Maquette et impression : DSAF/DRSG – Pôle graphique, Fabrication, image – Avril 2019.