SOMMAIRE

Avant-propos 8

Première partie

L'instauration progressive d'un contrôle de l'activité des services de renseignement 13

1.1. La mise en place de mécanismes de contrôle externe 14

1.1.1. Les fondements du contrôle externe 14

1.1.2. Le contrôle externe exercé par la Commission nationale de contrôle des interceptions de sécurité (CNCIS) 17

1.1.3. Le contrôle externe exercé par le Parlement 20

1.1.3.1. La commission de vérification des fonds spéciaux (CVFS) 20

1.1.3.2. La délégation parlementaire au renseignement (DPR) 21

1.2. Le renforcement des contrôles internes 24

1.2.1. Le respect de la chaîne hiérarchique dans le cadre de la procédure de validation des demandes 24

1.2.2. L'inspection des services de renseignement 24

Deuxième partie

La Commission nationale de contrôle des techniques de renseignement (CNCTR) : une nouvelle autorité administrative indépendante aux missions élargies 27

2.1. La compétence de la CNCTR 28

2.1.1. Le respect de la vie privée dans toutes ses composantes 28

2.1.2. Les finalités pouvant justifier la mise en œuvre de techniques de renseignement 30

2.1.3. Les services autorisés à mettre en œuvre les techniques de renseignement 32

2.1.4. Les techniques de renseignement destinées à surveiller le territoire national 37

2.1.4.1. Les accès administratifs aux données de connexion 38

2.1.4.2. Les interceptions de sécurité 41

2.1.4.3. La captation de paroles, la captation d'images, le recueil et la captation de données informatiques 42

2.1.4.4. L'introduction dans un lieu privé 42

2.1.5. La surveillance des communications électroniques internationales 45

2.1.5.1. Les principes 45

2.1.5.2. La mise en œuvre 45

2.1.6. La limite de la compétence de la commission : « l'exception hertzienne » 48

2.2. Les procédures et délais de traitement de la CNCTR 52

2.2.1. La procédure d'autorisation de droit commun 52

2.2.2. La procédure en cas urgence absolue 56

2.3. L'organisation et le fonctionnement de la CNCTR 57

2.3.1. Une instance collégiale 57

2.3.2. Une instance soumise à des règles d'indépendance et de déontologie . 58

2.3.3. Les moyens humains et matériels de la CNCTR 59

SOMMAIRE

Troisième partie

L'intense activité de contrôle préalable lors d'une première année d'activité marquée par une forte menace terroriste 61

3.1. Les fondements et principes de l'avis préalable de la CNCTR 63

3.2. La présentation statistique des demandes de mise en œuvre de techniques de renseignement 65

3.2.1. Les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure) 66

3.2.2. Les géolocalisations en temps réel (article L. 851-4 du code de la sécurité intérieure) 68

3.2.3. Les interceptions de sécurité (I de l'article L. 852-1 du code de la sécurité intérieure) 68

3.2.4. Les autres techniques de renseignement. 71

3.3. La création d'un nouvel outil d'évaluation : le nombre de personnes surveillées 72

Quatrième partie

Les défis du contrôle *a posteriori* 75

4.1. Des capacités de contrôle performantes sur les accès aux données de connexion, les géolocalisations en temps réel et les interceptions de sécurité 76

4.2. L'approfondissement du contrôle sur les nouvelles techniques de renseignement 78

4.2.1. Une question essentielle : la centralisation des renseignements recueillis 78

4.2.2. Les contrôles sur pièce et sur place 80

4.3. La construction du contrôle *a posteriori* sur la surveillance des communications électroniques internationales 82

4.4. Les recommandations et observations de la CNCTR. 83

4.5. Un dispositif particulier pour protéger les « lanceurs d'alerte ». 85

Cinquième partie

Les voies de recours à l'égard de la mise en œuvre des techniques de renseignement 87

5.1. Les recours exercés par les particuliers 89

5.1.1. La procédure préalable de réclamation devant la CNCTR 89

5.1.2. Le recours contentieux devant le Conseil d'État. 91

5.2. Les recours ouverts à la CNCTR 94

Sixième partie

Le dialogue institutionnel, l'information du public et les relations internationales 95

6.1. Les relations entre la CNCTR et le Parlement 96

6.1.1. L'avis préalable des commissions parlementaires sur la nomination du président de la CNCTR 96

6.1.2. Un dialogue institutionnel régulier et constructif 97

6.2. Les relations de la CNCTR avec les services de renseignement 98

6.2.1. L'audition des directeurs et chefs de services de renseignement 98

6.2.2. Les rencontres régulières avec les services de renseignement 98

6.2.3. La participation aux formations des cadres des services de renseignement 99

6.3. Le partage d'expérience avec les autorités de contrôle étrangères et le dialogue avec les institutions internationales chargées de la promotion des droits fondamentaux 99

6.4. L'information du public. 100

SOMMAIRE

Annexes 101

1. Délibération de la CNCTR n° 1/2015 du 29 octobre 2015 (définition des professions protégées à l'article L. 821-7 du code de la sécurité intérieure) 102
2. Délibération de la CNCTR n° 2/2015 du 12 novembre 2015 (avis sur le projet de décret relatif aux services de renseignement dits du « second cercle ») 105
3. Délibération de la CNCTR n° 1/2016 du 14 janvier 2016 (avis sur le projet de décret relatif aux techniques de renseignement) 120
4. Délibération de la CNCTR n° 2/2016 du 10 novembre 2016 (recommandation sur la surveillance et le contrôle des transmissions empruntant la voie hertzienne) 133
5. Règlement intérieur de la CNCTR 137
6. Décret du 1er octobre 2015 relatif à la composition de la Commission nationale de contrôle des techniques de renseignement 145
7. Liste des autorités de contrôle étrangères rencontrées 146
8. Décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015 (loi relative au renseignement) 147
9. Décision du Conseil constitutionnel n° 2015-722 DC du 26 novembre 2015 (loi relative aux mesures de surveillance des communications électroniques internationales) 179
10. Décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016 (surveillance et contrôle des transmissions empruntant la voie hertzienne) 187
11. Décision du Conseil d'État du 19 octobre 2016 n° 396958 193
12. Décision du Conseil d'État du 19 octobre 2016 n° 397623 198

Créée par la loi du 24 juillet 2015 relative au renseignement, la Commission nationale de contrôle des techniques de renseignement (CNCTR) est une autorité administrative indépendante chargée d'exercer le contrôle externe de la légalité de l'activité des services de renseignement et d'apprécier notamment à ce titre la proportionnalité de l'atteinte portée à la vie privée des personnes concernées au regard des menaces invoquées pour solliciter la mise en œuvre de techniques de renseignement. Elle a été mise en place le 3 octobre 2015.

La CNCTR retrace dans son rapport sa première année d'activité.

Durant cette première année, la CNCTR a d'abord relevé le défi de la transition. Elle a en effet assuré, sans interruption, le contrôle des techniques de renseignement jusqu'alors suivies par la Commission nationale de contrôle des interceptions de sécurité (CNCIS), à savoir les interceptions de sécurité et les géolocalisations en temps réel, mais aussi celui des nouvelles techniques de renseignement mentionnées dans la loi du 24 juillet 2015. Elle s'est appuyée, au moment de sa création et pendant plusieurs semaines, sur les seuls moyens humains et techniques hérités de la CNCIS. La transition a pu s'effectuer sans heurts grâce à l'engagement des membres et des agents de la commission et au travail de préparation mené sous l'égide de Jean-Marie DELARUE, qui présidait la CNCIS et auquel je veux ici rendre hommage. Dans cette première phase, la CNCTR a dû concentrer ses efforts sur le contrôle *a priori*. Le renforcement de ses effectifs réalisé tout au long de l'année écoulée lui a ensuite permis de développer le contrôle *a posteriori.*

La CNCTR a aussi dû relever le défi de l'effectivité du contrôle sur l'ensemble des techniques de renseignement couvertes par la loi du 24 juillet 2015 relative au renseignement et par celle du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales. Cette effectivité repose sur l'exhaustivité et la qualité du contrôle *a priori* et sur une bonne complémentarité entre contrôle *a priori* et contrôle *a posteriori.*

La CNCTR exerce depuis l'origine un contrôle *a priori* sur toutes les demandes de techniques de renseignement relevant de la loi du 24 juillet 2015. Le renforcement de ses effectifs lui a permis d'approfondir son contrôle et d'en assurer la permanence vingt-quatre heures sur vingt-quatre et sept jours sur sept. Dans un seul cas, le Premier ministre a eu recours à la procédure d'urgence absolue qui lui permet de donner une autorisation sans l'avis préalable de la commission. La CNCTR a également accepté, à titre expérimental à ce stade, d'exercer sur les demandes d'autorisation d'exploitation des données recueillies au titre de la surveillance internationale un contrôle *a priori* que la loi n'avait pas prévu mais que le Premier ministre lui a proposé d'assumer.

Le contrôle *a posteriori* de la CNCTR sur les techniques de renseignement mises en œuvre au titre des deux lois de 2015 s'est étoffé au fur et à mesure de la montée en puissance de ses moyens. Il a nécessité le recrutement de nouveaux agents dotés d'une solide formation juridique mais aussi d'ingénieurs capables de maîtriser la haute technicité de certains modes de recueil de renseignements. La centralisation des données recueillies, prévue par la loi et gage d'une pleine effectivité du contrôle *a posteriori*, s'applique d'ores et déjà pour la très grande majorité des données. Elle reste encore à bâtir pour une partie des données recueillies par les nouvelles techniques de renseignement dont la mise en œuvre est nécessairement locale. La CNCTR veille et continuera à veiller à ce que le chantier de cette centralisation, qui requiert la création d'infrastructures relativement lourdes, soit conduit avec détermination.

Dans cette première année, la CNCTR a eu une intense activité doctrinale, qu'elle a veillé à porter à la connaissance du Premier ministre ainsi que des ministres et des services concernés. Le rapport en retrace les principaux éléments qui ne sont pas couverts par le secret de la défense nationale.

La CNCTR a pu constater dans sa pratique quotidienne que les lois du 24 juillet 2015 et du 30 novembre 2015 ont apporté un net renforcement de l'encadrement de l'activité des services de renseignement par rapport à la situation antérieure.

La CNCTR a cependant été confrontée à deux difficultés d'application de la loi du 24 juillet 2015. La première avait trait à l'article L. 851-2 du code de la sécurité intérieure qui imposait, pour le recueil de données de connexion en temps réel dans un but de prévention du terrorisme, des conditions plus restrictives que pour les interceptions de sécurité, alors que celles-ci, plus intrusives, permettent le recueil en temps réel non seulement de ces données mais aussi du contenu des correspondances. Cette incohérence a été corrigée par la loi du 21 juillet 2016 qui a prorogé l'état d'urgence. La seconde a été traitée par la décision du 21 octobre 2016 du Conseil constitutionnel qui a censuré ce qui est généralement désigné comme l'« exception hertzienne ». Héritée de la loi du 10 juillet 1991 et maintenue par la loi du 24 juillet 2015, cette exception mal définie faisait échapper à l'autorisation du Premier ministre et au contrôle de la CNCTR certaines mesures de surveillance. Son maintien, dans la loi du 24 juillet 2015, n'était pas cohérent avec la volonté de mieux encadrer l'activité des services de renseignement. La censure de cette disposition contraint les pouvoirs publics à légiférer à nouveau sur ce point d'ici le 31 décembre 2017 s'ils souhaitent maintenir une « exception hertzienne ». Dans cette attente, la CNCTR qui, comme l'exige la décision du Conseil constitutionnel, doit désormais être informée des mesures de surveillance menées dans le cadre de l'« exception hertzienne » veillera à ce que ces mesures soient strictement limitées à ce qu'autorise le Conseil constitutionnel. Elle souhaite par ailleurs être consultée sur l'éventuelle nouvelle législation.

Le lecteur trouvera dans le rapport une série d'éléments chiffrés sur l'activité de la CNCTR durant l'année écoulée. Ils permettent d'apprécier, notamment sur le champ spécifique auparavant couvert par la CNCIS (interceptions de sécurité et géolocalisations en temps réel), les évolutions intervenues et ils permettront, dans les années futures, d'observer les évolutions sur l'ensemble du champ désormais couvert par la CNCTR.

Le lecteur trouvera aussi dans le rapport un indicateur nouveau destiné à permettre de mesurer l'impact sur les libertés individuelles des techniques de renseignement contrôlées : celui du nombre des personnes ayant fait l'objet d'au moins une mesure de surveillance dans le cours d'une année. Ce chiffre, qui sera rendu public chaque année par la CNCTR, permettra de mesurer l'évolution de l'ampleur des atteintes portées à la vie privée par les mesures de surveillance mises en œuvre sur notre territoire.

J'espère que ce premier rapport de la CNCTR facilitera la compréhension de la nouvelle architecture encadrant la mise en œuvre des techniques de renseignement et qu'il permettra de montrer comment est contrôlée la proportionnalité des atteintes portées à la vie privée.

Francis DELON

Conseiller d'État honoraire,
président de la CNCTR

1re partie

L'instauration progressive d'un contrôle de l'activité des services de renseignement

L'instauration progressive d'un contrôle de l'activité des services de renseignement

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications[1] a institué la première autorité administrative indépendante chargée de contrôler les interceptions administratives de correspondances, dites « interceptions de sécurité ».

Ce contrôle externe, au champ limité à une seule technique de renseignement, a par la suite été complété par celui exercé par le Parlement, sous l'égide notamment de la délégation parlementaire au renseignement (DPR) instituée par la loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

Parallèlement à ces mécanismes de contrôle externe, les outils de contrôle interne à l'administration ont été progressivement renforcés.

1.1. La mise en place de mécanismes de contrôle externe

1.1.1. Les fondements du contrôle externe

L'élaboration d'un cadre juridique renforçant la protection de la vie privée et fixant les conditions dans lesquelles il peut être porté atteinte au secret des correspondances pour des motifs de police administrative trouve son origine dans une décision du Premier ministre du 28 mars 1960 créant le groupement interministériel de contrôle (GIC), service placé sous son autorité et chargé d'exécuter, pour le compte des services de renseignement,

1 - Cette loi sera désormais mentionnée comme « la loi du 10 juillet 1991 ».

les interceptions téléphoniques administratives. Cette décision avait également institué une commission administrative ayant pour mission de tenir un fichier des autorisations d'interception et de veiller à ce que les interceptions effectuées soient conformes aux missions des services bénéficiaires.

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

Après plusieurs questions écrites adressées au Gouvernement, une commission de contrôle parlementaire[2], dénommée « commission de contrôle des services administratifs procédant aux écoutes téléphoniques », fut créée le 29 juin 1973 par une résolution du Sénat. Le rapport[3] qu'elle rendit le 23 octobre suivant préconisa vainement l'adoption d'une loi pour fonder en droit les écoutes légitimes et contrôler leur exécution.

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

Par deux arrêts n° 11105/84 et n° 11801/85 du 24 avril 1990 (affaires Huvig et Kruslin contre France), relatifs au régime français des écoutes judiciaires, la Cour européenne des droits de l'homme condamna la France pour violation de l'article 8 de la convention de sauvegarde des droits de l'homme

2 - Dans sa rédaction en vigueur à cette époque, l'article 6 de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires prévoyait la création de commissions de contrôle, destinées à « *examiner la gestion administrative, financière ou technique de services publics ou d'entreprises nationales en vue d'informer l'assemblée qui les a créées du résultat de leur examen* ».

3 - Voir le rapport n° 30 fait au nom de la commission sénatoriale de contrôle des services administratifs procédant aux écoutes téléphoniques par M. Pierre MARCILHACY, président, et M. René MONORY, rapporteur (le rapport est consultable sur le site du Sénat).

et des libertés fondamentales, qui protège le droit de toute personne au respect de sa vie privée et familiale. La cour affirmait que « *les écoutes et les autres formes d'interceptions des entretiens téléphoniques [représentaient] une atteinte grave au respect de la vie privée et de la correspondance* » et devaient « *donc se fonder sur une loi d'une précision particulière* » (voir le paragraphe n° 32 dans l'affaire Huvig). En l'espèce, le droit français « *[n'indiquait] pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités* » dans le domaine des écoutes judiciaires de sorte que les requérants n'avaient pas bénéficié « *du degré minimal de protection voulu par la prééminence du droit dans une société démocratique* » (voir le paragraphe n° 36 dans l'affaire Huvig). À la suite de ces arrêts, les initiatives, en France, se sont multipliées en faveur de la création d'un cadre législatif pour l'interception des communications.

C'est dans ce contexte qu'a été élaborée la loi du 10 juillet 1991, qui a fourni un cadre juridique précis tant aux interceptions judiciaires qu'aux interceptions administratives, dites « interceptions de sécurité ».

L'article 1er de la loi rappelait que « *le secret des correspondances émises par la voie des télécommunications est garanti par la loi* » et soulignait qu'« *il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci* ». Le titre II de la loi déterminait le cadre juridique dans lequel la puissance publique pouvait, à titre exceptionnel, procéder à des interceptions de sécurité.

La loi du 10 juillet 1991 a également créé la Commission nationale de contrôle des interceptions de sécurité (CNCIS), autorité administrative indépendante composée de trois membres (un président issu du Conseil d'État ou de la Cour de cassation, un député et un sénateur) et chargée de veiller au respect des dispositions légales relatives à l'autorisation et à la réalisation des mesures d'interception.

1.1.2. Le contrôle externe exercé par la Commission nationale de contrôle des interceptions de sécurité (CNCIS)

La CNCIS a exercé un contrôle de légalité, incluant un contrôle de proportionnalité, sur les autorisations accordées par le Premier ministre aux fins de pratiquer des interceptions de sécurité. La loi prévoyait qu'elle vérifiait *a posteriori* les conditions d'autorisation et de mise en œuvre des interceptions. Cependant, en vertu d'une pratique observée dès les premiers mois suivant l'entrée en vigueur de la loi du 10 juillet 1991 et établie d'un commun accord entre la CNCIS et le Gouvernement, la commission rendait également un avis au Premier ministre sur la légalité des demandes d'interception avant que celui-ci ne statue sur ces demandes.

Lorsqu'elle rendait un tel avis préalable, la CNCIS effectuait tout d'abord un contrôle formel en vérifiant que les signataires des demandes d'autorisation avaient bien été habilités par les ministres compétents. Elle examinait ensuite le bien-fondé de la demande, qui ne pouvait porter sur des faits dont était déjà saisie l'autorité judiciaire et qui devait respecter différents critères :

- la concordance entre les motifs invoqués dans la demande et les finalités définies par la loi : (sécurité nationale, sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, prévention du terrorisme, prévention de la criminalité et de la délinquance organisées, prévention de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées) ; la commission pouvait formuler toutes observations utiles sur la pertinence du motif invoqué ;
- l'implication directe et personnelle de la personne visée : l'identification de la personne devait être la plus précise possible et son implication dans des agissements attentatoires à la liberté devait être personnelle et directe ; la CNCIS en déduisait que l'entourage de la personne ne pouvait être concerné ;

- la nécessité et la subsidiarité de la mesure sollicitée : la commission s'assurait de l'impossibilité pour le service de recueillir par un autre moyen, moins intrusif, les informations recherchées ;
- la proportionnalité entre la mesure sollicitée et l'importance de la menace invoquée : la recherche de cet équilibre pouvait se traduire, au cas par cas, par une restriction de la durée de la mesure par rapport au maximum légal.

La commission avait la possibilité de demander au service concerné de lui fournir les éléments d'information complémentaires qui lui paraissaient nécessaires pour formuler son avis.

Une fois son instruction achevée, la commission pouvait rendre soit un avis défavorable, soit un avis favorable, assorti le cas échéant d'observations tendant, le plus souvent, à la réduction de la durée de la mesure par rapport au maximum légal.

Le contrôle *a posteriori* de la CNCIS portait sur les modalités d'exécution des interceptions de sécurité autorisées par le Premier ministre. De sa propre initiative ou sur réclamation de toute personne ayant un intérêt direct et personnel, la commission pouvait procéder au contrôle des « productions », c'est-à-dire du contenu des correspondances interceptées afin de vérifier le respect des dispositions légales. Ce contrôle avait pour objet de s'assurer que le contenu des enregistrements transcrits et exploités se rattachait aux motifs fondant la demande, que la ligne téléphonique écoutée était active et effectivement utilisée, que la personne dont les communications étaient interceptées était bien celle mentionnée dans la demande et que les transcriptions ne concernaient que les motifs pour lesquels l'interception avait été autorisée.

La commission vérifiait enfin les conditions de destruction des enregistrements et des transcriptions, attestées par des procès-verbaux. La destruction devait intervenir dans un délai de dix jours à compter de la réalisation des enregistrements. Les transcriptions devaient, quant à elles, être détruites dès que leur conservation n'apparaissait plus indispensable aux fins pour lesquelles l'interception avait été autorisée.

Créée pour contrôler les interceptions de sécurité, la CNCIS a vu sa compétence élargie par l'article 6 de la loi n° 2006-64 du 20 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers, qui l'a chargée du contrôle *a posteriori* des accès administratifs aux données techniques de connexion[4]. Il s'agissait de demandes formées, indépendamment d'une interception de sécurité, par des services habilités du ministère de l'intérieur, pour la prévention des actes de terrorisme. Ces demandes devaient être approuvées par une « personnalité qualifiée » désignée par la CNCIS sur proposition du ministre de l'intérieur et placée auprès de ce dernier. La personnalité qualifiée adressait à la commission les autorisations de recueil accompagnées de leurs motifs ainsi qu'un rapport d'activité annuel. La commission pouvait, de sa propre initiative, procéder à tout moment à des contrôles.

À compter du 1er janvier 2015, en application de l'article 20 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019[5], l'accès administratif aux données de connexion a été rendu possible pour tous les services de renseignement, pour les mêmes motifs que ceux pouvant fonder une interception de sécurité. La personnalité qualifiée accordant les autorisations était désormais placée auprès du Premier ministre. Par dérogation, lorsque les accès aux données de connexion avaient pour objet une géolocalisation en temps réel, l'autorisation était accordée par le Premier ministre lui-même et la commission rendait un avis *a priori* sur les demandes, bien que la loi, comme pour les interceptions de sécurité, ne prévît qu'un contrôle *a posteriori.*

Dans l'hypothèse d'une méconnaissance des dispositions légales, la commission pouvait adresser une recommandation au Premier ministre tendant à ce que la mesure soit interrompue. Le Premier ministre devait l'informer sans délai des suites données à ses recommandations.

4 - Voir, pour une définition de cette notion, le point 2.1.4.1. du présent rapport.

5 - Cette loi sera désormais mentionnée comme « la loi de programmation militaire du 18 décembre 2013 ».

1.1.3. Le contrôle externe exercé par le Parlement

Comme le soulignait la commission des lois de l'Assemblée nationale, dans son rapport du 14 mai 2013 sur l'évaluation du cadre juridique applicable aux services de renseignement[6], le développement d'un contrôle parlementaire sur l'activité de ces services nécessite la conciliation de deux principes potentiellement contradictoires : le contrôle de l'action du Gouvernement par les représentants de la Nation et le respect du secret attaché aux activités de renseignement.

La conciliation s'est d'abord traduite par la nomination de parlementaires au sein de la CNCIS, autorité administrative indépendante, puis par la création d'une commission spécialisée chargée de la vérification des fonds spéciaux, enfin par la création d'une délégation parlementaire au renseignement.

En outre, si le principe de séparation des pouvoirs empêche de soumettre les parlementaires à une enquête d'habilitation au secret de la défense nationale, qui comporte nécessairement une intrusion dans la vie privée et qui est menée par des services relevant du pouvoir exécutif, les lois relatives au contrôle du Parlement sur les services de renseignement ont résolu la difficulté en habilitant ès qualités les parlementaires exerçant une fonction qui nécessite un accès à des informations classifiées.

1.1.3.1. La commission de vérification des fonds spéciaux (CVFS)

L'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002 a institué la Commission de vérification des fonds spéciaux (CVFS), chargée de contrôler *a posteriori* l'utilisation de ces fonds, qui sont presque exclusivement destinés au financement des actions relevant des services de renseignement.

6 - Voir le rapport d'information n° 1022 déposé par la commission des lois de l'Assemblée nationale en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement et présenté par MM. Jean-Jacques URVOAS et Patrice VERCHERE.

Cette commission était, durant ses premières années d'activité, composée de deux sénateurs et deux députés désignés respectivement par le président du Sénat et le président de l'Assemblée nationale, ainsi que de deux magistrats de la Cour des comptes, nommés par décret sur proposition du premier président de cette juridiction. Les magistrats financiers cessèrent toutefois de siéger lorsque Philippe SÉGUIN, alors premier président de la Cour des comptes, eut décidé leur retrait.

Tirant les conséquences de cette situation, la loi de programmation militaire du 18 décembre 2013 a modifié la composition de la commission et en a fait une formation spécialisée de la délégation parlementaire au renseignement. La CVFS est désormais composée de quatre parlementaires issus pour moitié de l'Assemblée nationale et pour moitié du Sénat, tous membres de la délégation parlementaire au renseignement. Sa mission, inchangée, consiste à vérifier que les services ayant bénéficié des fonds spéciaux les ont utilisés conformément à ce que prévoit la loi de finances.

1.1.3.2. La délégation parlementaire au renseignement (DPR)

La loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement a inséré un article 6 *nonies* dans l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires[7] et institué une délégation composée de huit parlementaires, quatre députés et quatre sénateurs. Les présidents des commissions chargées respectivement des affaires de sécurité intérieure et de défense du Sénat et de l'Assemblée nationale en sont membres de droit. Les autres membres de la délégation sont désignés par le président de chaque assemblée de manière à assurer une représentation pluraliste.

7 - Cette ordonnance sera désormais mentionnée comme « l'ordonnance du 17 novembre 1958 ».

La délégation parlementaire avait initialement pour mission de suivre l'activité générale et les moyens des services spécialisés de renseignement[8]. La loi de programmation militaire du 18 décembre 2013 a renforcé ses prérogatives, d'une part en lui rattachant la commission de vérification des fonds spéciaux, d'autre part en élargissant sa mission. La délégation assure dorénavant, de façon générale, le contrôle parlementaire de l'action du gouvernement en matière de renseignement et l'évaluation de la politique publique en ce domaine. Enfin, la loi n° 2015-912 du 24 juillet 2015 relative au renseignement[9] a rendu la délégation compétente sur l'ensemble des services exerçant des activités de renseignement, au-delà des seuls services spécialisés, dits du « premier cercle ».

La délégation peut entendre le Premier ministre, les ministres concernés, le secrétaire général de la défense et de la sécurité nationale ainsi que les directeurs des services de renseignement. Elle peut également entendre le coordonnateur national du renseignement[10], le directeur de l'académie du renseignement, les collaborateurs accompagnant les directeurs des services de renseignement, les personnes placées auprès de ces directeurs et occupant un emploi pourvu en conseil des ministres, enfin les directeurs des autres administrations centrales ayant à connaître des activités des services de renseignement.

Les travaux de la délégation sont couverts par le secret de la défense nationale. Ses membres sont habilités ès qualités à connaître d'informations classifiées, ce qui leur permet d'accéder aux documents et éléments dont la délégation a besoin de connaître.

La loi prévoit toutefois, au I de l'article 6 *nonies* de l'ordonnance du 17 novembre 1958, que la délégation ne peut accéder à des informations ou des éléments d'appréciation portant sur les opérations des services en cours, sur les instructions données par les pouvoirs publics à cet égard, sur les procédures et méthodes opérationnelles, non plus que sur les échanges avec des services étrangers ou avec des organismes internationaux compétents

8 - Voir, pour une liste de ces services, le point 2.1.3 du présent rapport.

9 - Cette loi sera désormais mentionnée comme « la loi du 24 juillet 2015 ».

10 - Voir l'encadré sur la communauté française du renseignement au point 2.1.3 du présent rapport.

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

En outre, la loi a exclu l'accès des membres de la délégation à des données dont la communication pourrait mettre en péril l'anonymat, la sécurité ou la vie d'une personne relevant ou non des services intéressés, ainsi que les modes opératoires propres à l'acquisition du renseignement.

Comme l'a précisé la délégation dans son rapport public d'activité pour l'année 2014, la loi n'a pas entendu faire d'elle un organe de surveillance de l'administration. C'est un organe de contrôle du pouvoir exécutif. « *En cas d'anomalie avérée, les parlementaires membres de la délégation parlementaire au renseignement peuvent alors en imputer la responsabilité au seul Gouvernement et mettre en œuvre les mécanismes prévus par la Constitution en application de la séparation des pouvoirs* » (voir pages 13 et 14 du rapport de la délégation parlementaire).

1.2. Le renforcement des contrôles internes

1.2.1. Le respect de la chaîne hiérarchique dans le cadre de la procédure de validation des demandes

Les procédures appliquées au sein de chaque service pour préparer une demande de mise en œuvre d'une technique de renseignement doivent obéir à un contrôle hiérarchique strict, depuis les unités opérationnelles jusqu'au ministre dont relève le service demandeur. Un contrôle de légalité et d'opportunité doit ainsi être effectué à chaque niveau hiérarchique, jusqu'au Premier ministre, qui décide d'accorder ou non l'autorisation de mettre en œuvre la technique sollicitée.

1.2.2. L'inspection des services de renseignement

Créée par le décret n° 2014-833 du 24 juillet 2014 relatif à l'inspection des services de renseignement et placée sous l'autorité directe du Premier ministre, l'inspection des services de renseignement a pour mission de contrôler, auditer et conseiller les services spécialisés de renseignement ainsi que l'académie du renseignement.

Les inspecteurs qui la composent sont choisis parmi les fonctionnaires habilités à connaître des informations et supports classifiés au niveau Très Secret-Défense au sein de quatre corps d'inspection et de contrôle (inspection générale des finances, inspection générale de l'administration, contrôle général des armées, conseil général de l'économie, de l'industrie, de l'énergie et des technologies).

Dans le cadre d'un mandat établi pour chaque mission par le Premier ministre, les inspecteurs désignés ont accès à l'ensemble des lieux, informations et documents nécessaires à l'accomplissement de leur mission, y compris pour les actions en cours. À l'issue, un rapport est remis au Premier ministre, au ministre dont relèvent les services spécialisés de renseignement objets de l'inspection ainsi qu'au coordonnateur national du renseignement.

L'inspection veille au respect de la légalité, de l'éthique et de la déontologie des services concernés. Elle vérifie la conformité de leur action avec les orientations fixées par le conseil national du renseignement et contribue à l'amélioration de leur performance. Elle peut s'assurer de la bonne utilisation du budget qui leur est alloué.

2e partie

La Commission nationale de contrôle des techniques de renseignement : une nouvelle autorité administrative indépendante aux missions élargies

La Commission nationale de contrôle des techniques de renseignement : une nouvelle autorité administrative indépendante aux missions élargies

La loi du 24 juillet 2015, dont les principales dispositions ont été codifiées au livre VIII du code de la sécurité intérieure, a instauré un cadre juridique général pour l'activité des services de renseignement. Le législateur a notamment fixé les conditions de mise en œuvre des techniques de renseignement avec le souci de renforcer la protection des libertés individuelles tout en sécurisant juridiquement l'action des services. Créée par cette loi, la Commission nationale de contrôle des techniques de renseignement (CNCTR) est chargée du contrôle externe de légalité de l'activité des services de renseignement. Autorité administrative indépendante, elle se substitue à la CNCIS et bénéficie de compétences et de prérogatives élargies par rapport à cette dernière.

2.1. La compétence de la CNCTR

2.1.1. Le respect de la vie privée dans toutes ses composantes

Alors que la loi du 10 juillet 1991 ne mentionnait, à son article 1er, que le « *secret des correspondances émises par la voie des télécommunications* », l'article L. 801-1 du code de la sécurité intérieure, issu de la loi du 24 juillet 2015, garantit plus largement le « *respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des*

données personnelles et l'inviolabilité du domicile ». La CNCTR apprécie donc la légalité, en particulier la proportionnalité, de la mise en œuvre des techniques de renseignement au regard de l'atteinte portée à la vie privée des personnes concernées. Pour exercer ce contrôle, la CNCTR s'appuie sur l'ensemble des textes et jurisprudences pertinents en la matière.

Le respect de la vie privée est, en effet, un principe garanti à tous les degrés de la hiérarchie des normes et quotidiennement invoqué devant les juridictions des ordres judiciaire et administratif, qui se prononcent sur la proportionnalité des atteintes susceptibles de lui être portées. Le Conseil constitutionnel lui a définitivement reconnu une valeur constitutionnelle dans sa décision n° 99-416 DC du 23 juillet 1999, en estimant que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen impliquait le respect de la vie privée (voir le considérant n° 45). En droit international, la notion est reconnue notamment par l'article 12 de la Déclaration universelle des droits de l'homme du 10 décembre 1948[11], par l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950[12] et par l'article 7 de la Charte des droits fondamentaux de l'Union européenne[13]. La loi française l'a, quant à elle, inscrite à l'article 9 du code civil, ainsi qu'il a été dit plus haut[14].

11 - « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ».

12 - « *1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. / 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

13 - « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* ».

14 - Voir le rappel historique au point 1.1.1 du présent rapport.

2.1.2. Les finalités pouvant justifier la mise en œuvre de techniques de renseignement

Les services de renseignement doivent, conformément à l'article L. 811-3 du code de la sécurité intérieure et sous le contrôle de la CNCTR, respecter deux conditions pour solliciter et, le cas échéant, obtenir la mise en œuvre d'une technique de renseignement :

- la demande doit s'inscrire uniquement dans l'exercice de leurs missions respectives ;
- elle doit être motivée par la défense et la promotion d'intérêts fondamentaux de la Nation limitativement énumérés.

Alors que la loi du 10 juillet 1991 rendait possible, à son article 3, le recours aux interceptions de sécurité pour rechercher des renseignements intéressant « *la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous* », la loi du 24 juillet 2015 a renouvelé la liste des finalités pouvant fonder le recours aux techniques de renseignement prévues au titre V du livre VIII du code de la sécurité intérieure.

La nouvelle liste s'inspire, en l'élargissant, de la notion d'intérêts fondamentaux de la Nation définie à l'article 410-1 du code pénal[15]. En outre, le recours aux techniques de renseignement n'est pas borné à la défense de ces intérêts mais peut servir aussi leur promotion.

La première finalité concerne l'indépendance nationale, l'intégrité du territoire et la défense nationale. Revenant sur le concept de sécurité nationale introduit dans la loi du 10 juillet 1991 par référence à l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, le législateur a préféré reprendre des notions figurant dans la Constitution, à ses articles 5, 15 et 21.

15 - « *Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel* ».

La deuxième finalité mentionne 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. Sont ainsi visés aussi bien la contribution des services à vocation extérieure à la diplomatie française que le contre-espionnage.

La troisième finalité porte sur les intérêts économiques, industriels et scientifiques majeurs de la France. Elle permet notamment de lutter contre l'espionnage industriel et de promouvoir les intérêts économiques français face à d'éventuelles pratiques déloyales de concurrents étrangers.

La quatrième finalité, aujourd'hui la plus invoquée, est celle tenant à la prévention du terrorisme. La CNCTR apprécie cette notion par référence aux articles 421-1 et suivants du code pénal, qui définissent les actes de terrorisme.

La cinquième finalité comprend plusieurs branches. Il s'agit de prévenir, en premier lieu, les atteintes à la forme républicaine des institutions, en deuxième lieu, les actions tendant au maintien ou à la reconstitution de groupements dissous, en troisième lieu, les violences collectives de nature à porter gravement atteinte à la paix publique. Cette dernière catégorie comble une lacune de la loi du 10 juillet 1991, qui contraignait à recourir aux notions moins pertinentes de sécurité nationale et de criminalité organisée pour autoriser la surveillance d'individus particulièrement violents, agissant en groupe structuré dans le but de troubler gravement l'ordre public, notamment à l'occasion de manifestations. La CNCTR, particulièrement vigilante sur ce point, considère toutefois que cette finalité ne saurait être interprétée comme permettant la pénétration d'un milieu syndical ou politique ou la limitation du droit constitutionnel de manifester ses opinions, y compris extrêmes, tant que le risque d'une atteinte grave à la paix publique n'est pas avéré.

La sixième finalité reprend la prévention de la criminalité et de la délinquance organisées, mentionnée dans la loi du 10 juillet 1991, qui a longtemps constitué le premier motif de recours aux interceptions de sécurité avant de céder la place à la prévention du terrorisme au cours de l'année 2015. Dans la continuité de la CNCIS, la CNCTR s'appuie, pour rendre ses avis dans ce

domaine, sur la définition de la bande organisée prévue à l'article 132-71 du code pénal, telle qu'elle a été précisée par la jurisprudence de la Cour de cassation[16], ainsi que sur les dispositions du même code qui prévoient les crimes et les délits pouvant être commis par plusieurs personnes agissant en bande organisée[17].

La septième finalité permet de prévenir la prolifération des armes de destruction massive. Encore peu utilisée en droit français, la notion est à rapprocher des dispositions de l'article L. 213-2 du code du patrimoine, qui prohibe la communication d'archives « *susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue* ».

2.1.3. Les services autorisés à mettre en œuvre les techniques de renseignement

Au sein des services de renseignement, on distingue les services spécialisés de renseignement, dits du « premier cercle », des autres services pouvant exercer des activités de renseignement, dits du « second cercle ».

Les services spécialisés de renseignement, dits du « premier cercle », sont mentionnés à l'article L. 811-2 du code de la sécurité intérieure et leur liste établie à l'article R. 811-1 du même code. Il s'agit de la direction générale de la sécurité extérieure (DGSE), de la direction du renseignement et de la sécurité de la défense (DRSD)[18], de la direction du renseignement militaire (DRM), de la direction générale de la sécurité intérieure (DGSI), du service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » (DNRED) et du service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin). À l'exception de la DRM et de Tracfin, ces services ont vocation à accéder à l'ensemble des techniques de renseignements prévues par le livre VIII du code de la sécurité intérieure.

16 - Voir l'arrêt de la Cour de cassation du 8 juillet 2015 (chambre criminelle, n° 14-88329).

17 - Voir, à titre d'exemple, les articles 221-4 ou 222-4 du code pénal.

18 - Cette appellation découle du décret n° 2016-1337 du 7 octobre 2016 portant changement d'appellation de la direction de la protection et de la sécurité de la défense (DPSD).

La communauté française du renseignement

Définie à l'article D. 1122-8-1 du code de la défense, la communauté française du renseignement se compose des services spécialisés dits du « premier cercle », du coordonnateur national du renseignement et de l'académie du renseignement.

Le coordonnateur national du renseignement, dont les missions sont définies à l'article R.* 1122-8 du code de la défense, prépare, avec le concours du secrétaire général de la défense et de la sécurité nationale, les réunions et veille à la mise en œuvre des décisions du conseil national du renseignement, qui constitue une formation spécialisée du conseil de défense et de sécurité nationale comme l'indiquent les articles L. 1121-1 et R.* 1122-6 du code de la défense. Le conseil national du renseignement réunit, sous la présidence du Président de la République, le Premier ministre, les ministres et les directeurs des services spécialisés de renseignement dont la présence est requise par l'ordre du jour ainsi que le coordonnateur lui-même. En outre, ce dernier s'assure de la bonne coopération des services spécialisés, qui lui rendent compte de leur activité, et leur transmet les instructions du Président de la République, obtenant en retour les renseignements destinés au chef de l'État et au Premier ministre.

L'académie du renseignement, instituée par le décret n° 2010-800 du 13 juillet 2010 portant création de l'académie du renseignement, est un service à compétence nationale rattaché au Premier ministre. Elle concourt à la formation du personnel des services de renseignement, au renforcement des liens au sein de la communauté française du renseignement ainsi qu'à la diffusion de la culture du renseignement.

Les services du « second cercle » sont mentionnés à l'article L. 811-4 du code de la sécurité intérieure, qui prévoit que leur liste, les techniques auxquelles ils peuvent être autorisés à recourir et les finalités fondant cette autorisation doivent être définies par décret en Conseil d'État après avis de la CNCTR. C'est l'objet 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.

Les services du « second cercle » sont :

- sous l'autorité du directeur général de la police nationale :
  - l'unité de coordination de la lutte antiterroriste ;
  - à la direction centrale de la police judiciaire : 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, la sous-direction de la lutte contre la cybercriminalité, les directions interrégionales et régionales de police judiciaire, les services régionaux de police judiciaire et les antennes de police judiciaire ;
  - à la direction centrale de la police aux frontières : les unités chargées de la police judiciaire au sein des directions déconcentrées de la police aux frontières et des directions de la police aux frontières d'Orly et de Roissy, les brigades mobiles de recherche zonales, l'office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre de la direction centrale de la police aux frontières, l'unité judiciaire du service national de la police ferroviaire ;
  - à la direction centrale de la sécurité publique : les services du renseignement territorial, les sûretés départementales ;

- sous l'autorité du directeur général de la gendarmerie nationale :
  - à la direction des opérations et de l'emploi : la sous-direction de l'anticipation opérationnelle, la sous-direction de la police judiciaire ;
  - les sections de recherches de la gendarmerie nationale ;
- sous l'autorité du préfet de police de Paris :
  - à la direction du renseignement : la sous-direction de la sécurité intérieure, la sous-direction du renseignement territorial ;
  - à la direction régionale de la police judiciaire de Paris : la sous-direction des brigades centrales, la sous-direction des affaires économiques et financières, la sous-direction des services territoriaux ;
  - à la direction de la sécurité de proximité de l'agglomération de Paris : les sûretés territoriales ;
- 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.

L'avis de la CNCTR sur le projet de décret relatif aux services du « second cercle »[19]

Avant de rendre son avis sur le projet de décret, la CNCTR a entendu l'ensemble des directeurs ou chefs de service concernés afin qu'ils présentent leurs missions, leur organisation, leurs besoins opérationnels en matière de renseignement et leurs moyens techniques de mise en œuvre. Dans une délibération adoptée en formation plénière le 12 novembre 2015, la commission a tout d'abord observé qu'à la différence des services du « premier cercle », les services du « second cercle » n'avaient pas vocation à disposer d'un accès à l'ensemble des techniques ou finalités prévues par le livre VIII du code de la sécurité intérieure. Leurs missions et leurs capacités techniques ont conduit la CNCTR à proposer une approche différenciée, technique par technique.

Les services dont la mission principale est le renseignement (le service du renseignement territorial de la direction centrale de la sécurité publique, la direction du renseignement de la préfecture de police de Paris ou la sous-direction de l'anticipation opérationnelle de la direction générale de la gendarmerie nationale) ont ainsi, selon la commission, vocation à bénéficier d'un accès relativement étendu aux techniques de renseignement.

A contrario, la CNCTR a proposé de limiter l'accès aux techniques pour les services ayant une vocation essentiellement judiciaire, comme la direction centrale de la police judiciaire ou la sous-direction de la police judiciaire de la gendarmerie nationale. Si plusieurs de ces services peuvent mettre en œuvre des techniques similaires dans un cadre judiciaire, la CNCTR a estimé qu'ils n'avaient pas nécessairement vocation à utiliser, dans un cadre administratif, toutes les nouvelles techniques définies par la loi au titre de l'ensemble des finalités. Enfin, la CNCTR a suggéré que des services territoriaux, moins spécialisés encore que les précédents, ne puissent accéder à certaines techniques que de manière plus limitée.

La CNCTR a d'une manière générale souhaité limiter l'accès aux techniques les plus intrusives aux seules unités disposant des capacités à les mettre en œuvre et appelées à y avoir effectivement recours, au sein de directions ou de services dont la recherche du renseignement n'est pas la vocation première.

Enfin, la commission a insisté pour que l'ensemble des données recueillies soient centralisées, afin que la diffusion des informations relevant de la vie privée soit maîtrisée, circonscrite aux seuls agents intéressés et traçable lors des opérations de contrôle *a posteriori* qu'elle effectuera.

19 - Voir l'annexe n° 2 au présent rapport.

Le Gouvernement a finalement souhaité étendre plus largement que ce qu'avait recommandé la CNCTR l'accès des services du « second cercle » aux techniques de renseignement. Pour autant, la commission relève que, depuis l'entrée en vigueur du décret, les services qu'elle considérait ne pas devoir être autorisés à mettre en œuvre tout ou partie des techniques de renseignement n'ont pas eu recours à ces techniques ou n'ont demandé à y recourir que de manière très rare.

La loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement a modifié l'article L. 811-4 du code de la sécurité intérieure et ouvert la possibilité pour le Gouvernement d'élargir à des services du ministère de la justice l'habilitation à recourir aux différentes techniques de renseignement. Le législateur a ainsi permis d'ajouter aux services du « second cercle » un service de renseignement pénitentiaire relevant du ministère de la justice. La CNCTR, saisie pour avis le 7 novembre 2016 par le garde des sceaux du projet de décret en Conseil d'État nécessaire pour mettre en œuvre la loi, instruisait le dossier lors de la rédaction du présent rapport.

2.1.4. Les techniques de renseignement destinées à surveiller le territoire national

Si le cadre juridique antérieur fixait les conditions de mise en œuvre des interceptions de sécurité ainsi que des modalités de recueil des données de connexion, la loi du 24 juillet 2015 a défini un régime applicable à un ensemble beaucoup plus large de techniques de renseignement. Les articles L. 851-1 à L. 851-7 du code de la sécurité intérieure prévoient ainsi plusieurs types d'accès administratif aux données de connexion ainsi qu'à des données de localisation. L'article L. 852-1 concerne deux catégories d'interceptions de sécurité. Les articles L. 853-1 et L. 853-2 portent sur la captation de paroles prononcées à titre privé, la captation d'images dans un lieu privé, ainsi que la captation et le recueil de données informatiques. L'article L. 853-3 fixe les conditions dans lesquelles peut être autorisée la pénétration dans un lieu privé pour mettre en œuvre certaines techniques.

2.1.4.1 Les accès administratifs aux données de connexion

L'article L. 851-1 du code de la sécurité intérieure dispose que les opérateurs de communications électroniques ou les fournisseurs de services sur internet peuvent être requis de communiquer des informations et documents traités ou conservés par leurs réseaux ou services. Il peut s'agir des données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation d'équipements terminaux ou encore à la liste de numéros appelés et appelants, à la durée et à la date des communications. Ces informations ou documents ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, ainsi que le précisent les articles L. 851-7 et R. 851-5 du code de la sécurité intérieure et que l'a rappelé le Conseil constitutionnel dans sa décision n° 2015-713 DC du 23 juillet 2015[20], par laquelle il a jugé que « *le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées* » (voir le considérant n° 55).

Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés (CNIL), de l'Autorité de régulation des communications électroniques et des postes (ARCEP) et de la CNCTR, a fixé les modalités d'application de la nouvelle procédure d'accès administratif aux données de connexion. L'avis de la CNCTR sur le projet de décret a fait l'objet de la délibération n° 1/2016 du 14 janvier 2016 adoptée en formation plénière[21].

L'accès aux données de connexion en temps différé

Dans sa délibération n° 1/2016 du 14 janvier 2016, la CNCTR a estimé que l'article L. 851-1 du code de la sécurité intérieure ne prévoyait qu'un accès en temps différé aux données de connexion, un accès en temps réel ayant été institué à l'article L. 851-2 du même code. Le Gouvernement a suivi cet avis.

20 - Voir l'annexe n° 8 au présent rapport.
21 - Voir l'annexe n° 3 au présent rapport.

La procédure applicable aux données de connexion est désormais identique à celle régissant les autres techniques de renseignement : demande présentée par le ministre concerné, à l'exception des demandes qui peuvent être présentées directement par des agents habilités des services de renseignement (il s'agit des demandes d'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ou des demandes de recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée), avis préalable de la CNCTR, décision du Premier ministre. Cette homogénéisation des procédures constitue une évolution positive, préconisée en son temps par la CNCIS.

L'accès en temps réel aux données de connexion

La rédaction initiale de l'article L. 851-2 du code de la sécurité intérieure prévoyait que, pour les seuls besoins de la prévention du terrorisme, pouvaient être recueillies, en temps réel, les données de connexion relatives à des personnes préalablement identifiées comme présentant une menace. La loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence a étendu l'application de ce dispositif aux personnes « *préalablement identifiée[s] susceptible[s] d'être en lien avec une menace* » et à l'entourage de celles-ci lorsqu'il est susceptible de fournir des informations en lien avec la prévention du terrorisme. Elle a également porté la durée maximale de mise en œuvre de la technique à quatre mois, au lieu des deux mois prévus dans la version initiale de l'article L. 851-2.

Plus intrusif que l'accès aux données de connexion en temps différé mais moins attentatoire à la vie privée qu'une interception de sécurité, dès lors qu'il ne permet pas d'écouter ou de lire les correspondances des personnes concernées, ce dispositif a pour but de détecter des menaces terroristes effectives.

Le traitement des données de connexion par algorithme

L'article L. 851-3 du code de la sécurité intérieure ouvre la possibilité d'imposer la mise en place, sur les réseaux des opérateurs de communications électroniques et des fournisseurs de services sur internet, de traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste, sans

qu'il soit possible de procéder, dans un premier temps, à l'identification des personnes concernées. Ce n'est que lorsque la menace est avérée que le Premier ministre peut, après avis de la CNCTR, autoriser l'identification de la personne en cause et le recueil des données de connexion afférentes.

Saisie d'une demande d'avis par le Premier ministre au titre de l'article L. 833-11 du code de la sécurité intérieure, la commission a examiné le projet d'architecture générale pour la mise en œuvre de ces traitements automatisés. Elle a formulé, par une délibération classifiée adoptée en formation plénière le 28 juillet 2016, des observations et des recommandations sur la procédure de collecte des données de connexion, les caractéristiques des données collectées, la durée de leur conservation, les conditions de leur stockage et la traçabilité des accès. Elle considère notamment que la loi fait obstacle à ce que les agents des services de renseignement puissent accéder aux données collectées tant que le Premier ministre n'a pas autorisé l'identification d'une personne. La commission a rappelé que la collecte ne pouvait s'opérer que sur les données techniques de connexion définies aux articles L. 851-1 et R. 851-5 du code de la sécurité intérieure et ne saurait s'appliquer au contenu des correspondances. Elle a en outre souligné qu'elle devait disposer d'un accès permanent, complet et direct à l'ensemble du dispositif et au mécanisme de traçabilité des accès.

La commission devra être saisie de chaque demande de mise en œuvre d'un traitement automatisé, prévue au I de l'article L. 851-3 du code de la sécurité intérieure, puis de chaque demande d'identification d'une personne et de recueil des données afférentes lorsque ces données sont susceptibles de caractériser l'existence d'une menace terroriste, en application du IV du même article. À la date de publication du présent rapport, la CNCTR n'a été saisie d'aucune demande de cette nature.

La localisation des personnes ou des objets

L'article L. 851-4 du code de la sécurité intérieure prévoit la géolocalisation en temps réel des équipements terminaux de communication : à cette fin, les opérateurs concernés sollicitent leur réseau et transmettent au GIC les données obtenues.

En outre, l'article L. 851-5 du code autorise l'emploi de dispositifs techniques, tels que des balises, pour localiser une personne, un véhicule ou un objet.

Les *IMSI catchers*

Les services de renseignement ont désormais la possibilité, en application de l'article L. 851-6 du code de la sécurité intérieure, de mettre en œuvre des dispositifs techniques, dénommés *IMSI catchers*, pour capter les données de connexion d'appareils téléphoniques mobiles.

Les données de connexion susceptibles d'être recueillies par les *IMSI catchers* sont l'identification d'un équipement terminal ou *IMEI* (*International Mobile Equipment Identity*), l'identification de son utilisateur *via* le numéro de sa carte *SIM* ou *IMSI* (*International Mobile Subscriber Identity*), auxquelles peuvent s'ajouter des informations de localisation de cet équipement.

Le II de l'article L. 851-6 du code de la sécurité intérieure prévoit que le recensement et les caractéristiques techniques de chacun des appareils font l'objet d'une inscription dans un registre spécial tenu à la disposition de la CNCTR. Ce registre a été établi. Il est régulièrement tenu à jour. Par ailleurs, un arrêté du Premier ministre non publié a fixé, après avis de la CNCTR, le nombre maximal de dispositifs pouvant être utilisés simultanément. Cet arrêté a suivi les recommandations de la commission.

2.1.4.2. Les interceptions de sécurité

Les interceptions de sécurité permettent d'accéder au contenu des communications et aux données de connexion qui y sont associées. Pour les interceptions auprès des opérateurs de communications électroniques, prévues au I de l'article L. 851-2 du code de la sécurité intérieure, le GIC, service du Premier ministre, centralise leur exécution et met à la disposition du service demandeur les résultats pour exploitation.

Certains services de renseignement peuvent également être autorisés à recourir à un *IMSI catcher* pour recueillir le contenu d'une communication, conformément au II de l'article L. 852-1 du code de la sécurité intérieure. L'autorisation est accordée par le Premier ministre après avis de la CNCTR pour une durée maximale de quarante-huit heures. Seules deux finalités peuvent alors être invoquées : la prévention du terrorisme, d'une part, l'indépendance nationale, l'intégrité du territoire et la défense nationale, d'autre part. Ce type d'utilisation correspond à des situations opérationnelles exceptionnelles.

2.1.4.3. La captation de paroles, la captation d'images, le recueil et la captation de données informatiques

Lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'article L. 853-1 du code de la sécurité intérieure prévoit la captation de paroles prononcées à titre privé ou confidentiel ainsi que la captation d'images dans des lieux privés. L'autorisation est délivrée pour une durée maximale de deux mois.

Peuvent également être autorisés le recueil et la captation de données informatiques, en application de l'article L. 853-2 du code. Le recueil permet d'accéder à des données informatiques stockées dans un système informatique. La captation s'applique aux données telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels. Le recueil de données peut être autorisé pour une durée maximale de trente jours et la captation de données pour une durée de deux mois.

2.1.4.4. L'introduction dans un lieu privé

La mise en œuvre de certaines techniques peut nécessiter l'introduction dans un lieu privé. Cette mesure n'est pas en elle-même à proprement parler une technique de renseignement mais un moyen de mettre en place, d'utiliser ou de retirer une balise (article L. 851-5 du code de la sécurité intérieure), un dispositif de captation de paroles ou d'images (article L. 853-1 du code) ou un dispositif de recueil ou de captation de données informatiques (article L. 853-2 du code). L'introduction dans un lieu privé doit toutefois faire l'objet d'une demande d'autorisation spécifique, conformément à l'article L. 853-3 du code de la sécurité intérieure. Si le lieu privé est un lieu d'habitation, la CNCTR rend son avis en formation collégiale, en application du même article.

Les durées d'autorisation et de conservation des données collectées en application de la loi du 24 juillet 2015

Accès aux données de connexion			
	Durée maximale d'autorisation	Durée de conservation des données à compter de leur recueil	
			Particularité
Accès aux données de connexion en temps différé : article L. 851-1 du code de la sécurité intérieure	4 mois renouvelables	4 ans	
Accès aux données de connexion en temps réel : article L. 851-2 du code de la sécurité intérieure	4 mois renouvelables	4 ans	
Traitements automatisés des données de connexion : article L. 851-3 du code de la sécurité intérieure	2 mois puis 4 mois renouvelables	60 jours	Durée de conservation des données d'une personne dont l'identification a été autorisée par le Premier ministre après avis de la CNCTR. Les données sont conservées, au-delà de cette durée de 60 jours, dans la limite de 4 ans, si la menace terroriste est confirmée.
Géolocalisation en temps réel : article L. 851-4 du code de la sécurité intérieure	4 mois renouvelables	4 ans	
Balisage : article L. 851-5 du code de la sécurité intérieure	4 mois renouvelables	4 ans	
Dispositif technique permettant l'identification d'un équipement terminal, du numéro d'abonnement de son utilisateur et de sa localisation - *IMSI catcher* : article L. 851-6 du code de la sécurité intérieure	2 mois renouvelables	4 ans	Données détruites dès qu'il apparaît qu'elles ne sont pas en rapport avec l'autorisation, dans un délai maximal de 90 jours

Interceptions de sécurité			
	Durée maximale d'autorisation	Durée de conservation des données à compter de leur recueil	
			Particularité
Interceptions de correspondances émises par la voie des communications électroniques : I de l'article L. 852-1 du code de la sécurité intérieure	4 mois renouvelables	30 jours	
Interceptions de correspondances émises par la voie des communications électroniques à l'aide d'un *IMSI catcher* : II de l'article L. 852-1 du code de la sécurité intérieure	48 heures renouvelables	30 jours	Données détruites dès qu'il apparaît qu'elles ne sont pas en lien avec l'autorisation, dans un délai maximal de 30 jours

Autres techniques			
	Durée maximale d'autorisation	Durée de conservation des données à compter de leur recueil	
			Particularité
Captation de paroles prononcées à titre privé : article L. 853-1 du code de la sécurité intérieure	2 mois renouvelables	30 jours	
Captation d'images dans un lieu privé : article L. 853-1 du code de la sécurité intérieure	2 mois renouvelables	120 jours	
Recueil de données informatiques : article L. 853-2 du code de la sécurité intérieure	30 jours renouvelables	120 jours	
Captation de données informatiques telles qu'elles s'affichent sur un écran, telles que l'utilisateur les y introduit ou telles qu'elles sont reçues et émises par des périphériques audiovisuels : article L. 853-2 du code de la sécurité intérieure	2 mois renouvelables	120 jours	
Introduction dans un véhicule ou dans un lieu privé : article L. 853-3 du code de la sécurité intérieure	30 jours renouvelables	Sans objet	

Nota bene : pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de six ans à compter de leur recueil. Les renseignements collectés qui contiennent des éléments de cyberattaque peuvent être conservés au-delà des durées mentionnées. Les renseignements qui concernent une requête dont le Conseil d'État a été saisi ne peuvent être détruits ; ils sont conservés pour les seuls besoins de la procédure devant le Conseil d'État.

2.1.5. La surveillance des communications électroniques internationales

2.1.5.1. Les principes

La loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales[22] a institué un régime spécial codifié aux articles L. 854-1 à L. 854-9 du code de la sécurité intérieure[23].

Les finalités permettant de surveiller les communications électroniques internationales sont identiques à celles, énumérées à l'article L. 811-3 du code de la sécurité intérieure, qui encadrent l'emploi des techniques pour la seule surveillance du territoire français. La procédure est en revanche différente. La loi a notamment prévu que les autorisations d'interception et d'exploitation des communications sont délivrées par le Premier ministre sans avis préalable de la CNCTR. Le contrôle de la CNCTR devait donc être limité à un contrôle *a posteriori*.

Toutefois, sollicitée par le Premier ministre en avril 2016, la CNCTR a accepté, par deux délibérations classifiées adoptées en formation plénière les 28 avril et 19 mai 2016, d'exercer un contrôle *a priori*, c'est-à-dire avant que le Premier ministre ne rende sa décision, sur les demandes d'exploitation des communications interceptées prévues au III de l'article L. 854-2 du code de la sécurité intérieure. Cette extension des prérogatives de contrôle de la commission est effective depuis fin mai 2016. La commission effectue toutefois ce contrôle *a priori* à titre expérimental. À l'issue de la phase

22 - Cette loi sera désormais mentionnée comme « la loi du 30 novembre 2015 ».

23 - La loi du 24 juillet 2015 avait déjà prévu un régime spécial pour des mesures de surveillance internationale, plus succinct et censuré de ce fait par le Conseil constitutionnel, dans sa décision n° 2015-713 DC du 23 juillet 2015 reproduite en annexe 8 au présent rapport, au motif « *qu'en ne définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1, ni celles du contrôle par la Commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre, le législateur n'a pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » (voir le considérant n° 78). À la suite de cette censure, la loi du 30 novembre 2015 a institué un nouveau régime, déclaré conforme à la Constitution par le Conseil constitutionnel dans sa décision n° 2015-722 DC du 26 novembre 2015, reproduite en annexe 9 au présent rapport.

d'expérimentation, dont elle a fixé le terme au 31 mars 2017, la commission se prononcera sur la pérennisation de ce contrôle, notamment au regard des conditions dans lesquelles il intervient et de l'intérêt qu'il présente pour la protection des libertés publiques. Les conditions de cet avis préalable n'étant pas déterminées par la loi, il a été convenu avec le Premier ministre que la commission serait saisie de toutes les demandes faites en application du III de l'article L. 854-2 du code de la sécurité intérieure et que le contrôle serait effectué au regard des critères de légalité énumérés à l'article L. 801-1 du même code. La CNCTR vérifie donc *a priori* que les demandes de mise en œuvre de la surveillance internationale procèdent d'une autorité compétente, sont présentées selon une procédure régulière, relèvent des missions confiées aux services requérant, sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation et que les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués.

2.1.5.2 La mise en œuvre

Les communications électroniques internationales concernées sont celles émises ou reçues à l'étranger, ainsi que l'énonce le premier alinéa de l'article L. 854-1 du code de la sécurité intérieure. En outre, en application du troisième alinéa du même article, les mesures de surveillance ne peuvent porter, de manière individuelle, sur les communications de personnes utilisant des numéros de téléphone ou des identifiants techniques rattachables au territoire national, sauf si ces personnes communiquent depuis l'étranger et soit faisaient l'objet d'une interception de sécurité au moment où elles ont quitté la France, soit sont identifiées comme présentant une menace au regard des intérêts fondamentaux de la Nation. Sous réserve de cette exception, dès qu'il apparaît que des communications interceptées sont échangées entre des personnes ou des équipements utilisant des numéros de téléphone ou des identifiants techniques rattachables au territoire national, y compris lorsqu'elles transitent par des équipements situés à l'étranger, ces communications sont instantanément détruites, conformément au dernier alinéa de l'article L. 854-1 du code de la sécurité intérieure.

La surveillance peut porter sur les données de connexion, à savoir les données techniques définies aux articles L. 851-1 et R. 851-5 du code de la sécurité intérieure, ou sur les correspondances, à savoir le contenu des communications.

Elle suppose la délivrance de deux types d'autorisations successives, l'une d'interception, l'autre d'exploitation, chaque autorisation accordée étant communiquée à la CNCTR en application de l'article L. 854-9 du code de la sécurité intérieure ainsi que de l'accord précédemment évoqué entre la commission et le Premier ministre relatif aux modalités de contrôle *a priori*.

En premier lieu, le Premier ministre autorise, en application du I de l'article L. 854-2 du code de la sécurité intérieure, l'interception de communications sur des réseaux qu'il désigne, par décision motivée, sans pouvoir déléguer sa signature.

En second lieu, les communications interceptées sur les réseaux désignés en application du I de l'article L. 854-2 du code ne peuvent être exploitées par un service sans une nouvelle autorisation. Celle-ci peut être une autorisation d'exploitation individualisée ou non. Seuls les services spécialisés de renseignement, dits du « premier cercle », peuvent être autorisés à exploiter des communications interceptées.

Les autorisations d'exploitation non individualisée, prévues au II de l'article L. 854-2 du code de la sécurité intérieure, ne peuvent porter que sur des données de connexion. Leur durée de validité est limitée à un an. Elles doivent préciser les types de traitements automatisés pouvant être mis en œuvre sur les données exploitées.

Les autorisations d'exploitation individualisée, prévues au III de l'article L. 854-2 du code de la sécurité intérieure, peuvent porter aussi bien sur des données de connexion que sur des correspondances. Leur durée de validité est limitée à quatre mois. Elles doivent par ailleurs être circonscrites à des zones géographiques, des organisations, des groupes de personnes ou des personnes. Comme il a été indiqué plus haut, la CNCTR émet depuis mai 2016, à titre expérimental jusqu'au 31 mars 2017, un avis préalable sur ces demandes d'exploitation individualisée.

La loi a prévu des durées de conservation distinctes selon que les communications interceptées ont été exploitées ou non, constituent des correspondances ou des données de connexion, mais aussi selon qu'un numéro de téléphone ou un identifiant technique rattachable au territoire national est utilisé ou non à l'une des extrémités de ces communications.

Lorsqu'aucun numéro de téléphone ou identifiant technique rattachable au territoire national n'apparaît, les correspondances sont détruites dans un délai de douze mois à compter de leur première exploitation, à défaut dans un délai de quatre ans à compter de leur recueil. Les données de connexion peuvent se voir appliquer des délais plus longs : elles sont détruites au plus tard six ans à compter de leur recueil. Ces durées sont fixées à l'article L. 854-5 du code de la sécurité intérieure.

Lorsqu'un numéro de téléphone ou un identifiant technique rattachable au territoire national est utilisé à l'une des extrémités des communications, l'article L. 854-8 du code de la sécurité intérieure prévoit l'application de durées de conservation proches de celles applicables aux techniques de renseignement mises en œuvre pour la surveillance du territoire national. Les correspondances sont ainsi détruites dans un délai de trente jours à compter de leur première exploitation, à défaut dans un délai de six mois à compter de leur recueil. Les données de connexion sont détruites au plus tard quatre ans à compter de leur recueil.

Les dispositions législatives décrites ci-dessus, ne nécessitant pas de textes d'application particuliers, sont entrées en vigueur le 2 décembre 2015, lendemain de la publication de la loi du 30 novembre 2015 au *Journal officiel* de la République française.

2.1.6. La limite de la compétence de la commission : « l'exception hertzienne »

La loi du 10 juillet 1991 avait exclu de la compétence de la CNCIS, à son article 20, « *les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne* ». Ces dispositions ont été reprises à l'identique dans le nouveau cadre juridique issu de la loi du 24 juillet 2015, à l'article L. 811-5 du code de la sécurité intérieure.

Soustraites à tout mécanisme d'autorisation par le Premier ministre et de contrôle par une autorité indépendante, motivées par une notion d'intérêts nationaux large et non définie, les mesures entrant dans le champ de « l'exception hertzienne » ont été strictement circonscrites par la CNCIS.

Dès son premier rapport d'activité pour les années 1991 et 1992, la CNCIS a en effet indiqué que les mesures ne pouvaient se rattacher qu'à une mission générale de police des ondes. Par la suite, s'appuyant sur les travaux parlementaires ayant précédé l'adoption de la loi du 10 juillet 1991, elle a exclu qu'elles puissent participer de recherches ciblées destinées à intercepter des communications individualisables. Dans son rapport d'activité pour l'année 1998, après avoir analysé les évolutions technologiques intervenues depuis 1991, notamment l'apparition et la montée en puissance des communications par téléphones portables empruntant en tout ou partie la voie hertzienne, la CNCIS a estimé que de telles communications ne pouvaient être interceptées sur le fondement de l'article 20 de la loi du 10 juillet 1991 mais étaient protégées par le secret des correspondances de la même manière que les conversations empruntant la voie filaire[24]. Dans ses deux derniers rapports d'activité, la CNCIS a finalement estimé que la définition de l'exception par la loi était obsolète et recommandé sa suppression.

Ayant pris acte du maintien de « l'exception hertzienne » dans la loi du 24 juillet 2015 et des travaux parlementaires menés à cette occasion[25], la CNCTR a fait sienne la conception restrictive de la CNCIS et a en particulier considéré que l'article L. 811-5 du code de la sécurité intérieure ne saurait en aucun cas être utilisé pour recueillir des renseignements susceptibles d'être collectés au moyen de techniques de renseignement prévues par le livre VIII du même code et soumises à autorisation du Premier ministre sous le contrôle de la commission.

---

24 - Cette approche a été confirmée par le juge pénal, dans un jugement du tribunal correctionnel de Paris du 8 avril 2014 rendu à l'encontre d'un ancien directeur central du renseignement intérieur.

25 - Voir le rapport n° 460 déposé le 20 mai 2015 par M. Philippe BAS au nom de la commission des lois du Sénat. Selon le rapporteur, la disposition vise « *les capteurs hertziens des armées* », qui « *permettent de recueillir des signaux techniques et des communications électromagnétiques émis depuis l'étranger, par exemple ceux engendrés par des mouvements de troupes, d'aéronefs ou de navires dans une zone donnée. Ces interceptions hertziennes qui résultent du balayage de l'ensemble des gammes de fréquences du spectre électromagnétique, ne concernent pas des identifiants rattachables au territoire national (…) Elles sont aussi par nature aléatoires et non ciblées sur une communication* ».

Appelé, par la voie d'une question prioritaire de constitutionnalité soulevée à l'occasion d'instances en cours devant le Conseil d'État[26], à se prononcer sur la conformité à la Constitution de l'article L. 811-5 du code de la sécurité intérieure, le Conseil constitutionnel a, dans sa décision n° 2016-590 QPC du 21 octobre 2016[27], censuré cet article comme portant « *une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* » (voir le paragraphe n° 9). Il a en effet estimé que les dispositions censurées « *ne définissent pas la nature des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre* » et qu'elles « *ne soumettent le recours à ces mesures à aucune condition de fond ni de procédure et n'encadrent leur mise en œuvre d'aucune garantie* » (voir le paragraphe n° 8).

Différant l'abrogation des dispositions censurées au 31 décembre 2017, le Conseil constitutionnel a néanmoins entendu faire cesser l'inconstitutionnalité constatée à compter de la publication de sa décision en jugeant que, durant la période transitoire, « *les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne sauraient être interprétées comme pouvant servir de fondement à des mesures d'interception de correspondances, de recueil de données de connexion ou de captation de données informatiques soumises à l'autorisation prévue* » aussi bien pour la surveillance du territoire national que pour celle des communications électroniques internationales. En outre, « *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* » (voir le paragraphe n° 12).

---

26 - Il s'agit de quatre recours attaquant le décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, 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, 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, et le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

27 - Voir l'annexe 10 au présent rapport.

Afin de tirer les conséquences de la décision du Conseil constitutionnel, la CNCTR a adopté en formation plénière le 10 novembre 2016 une délibération[28] :

- recommandant au Premier ministre de veiller à ce que toutes les techniques de renseignement prévues au titre V du livre VIII du code de la sécurité intérieure soient mises en œuvre dans le respect de la procédure d'autorisation et de contrôle instituée à ce même livre ;
- recommandant que chacun des ministres dont relèvent les services de renseignement concernés définisse, dans des instructions soumises à son avis, les conditions dans lesquelles ces services pourront appliquer les dispositions de l'article L. 811-5 du code de la sécurité intérieure au plus tard jusqu'au 31 décembre 2017[29], en particulier le champ et la nature des mesures mises en œuvres ainsi que les motifs invoqués pour y recourir ;
- prévoyant que soient examinées avec chacun des services de renseignement concernés les modalités précises permettant à la commission d'être régulièrement informée des mesures prises par eux en application de l'article L. 811-5 du code, cette information devant mettre la CNCTR à même de vérifier la conformité de ces mesures à la réserve d'interprétation formulée par le Conseil constitutionnel, de recommander, si elle les estime non conformes à cette réserve, leur interruption et la destruction des renseignements collectés et, dans l'hypothèse où sa recommandation ne serait pas ou insuffisamment suivie, de saisir le Conseil d'État d'un recours en application de l'article L. 833-8 du code[30].

28 - Voir l'annexe n° 4 au présent rapport.

29 - L'article L. 811-5 du code de la sécurité intérieure demeure applicable, dans les conditions définies par le Conseil constitutionnel, jusqu'à ce qu'une nouvelle disposition législative se conformant aux exigences énoncées dans la déclaration d'inconstitutionnalité s'y substitue et au plus tard jusqu'au 31 décembre 2017.

30 - Voir, pour une présentation de cette faculté de recours, le point 5.2 du présent rapport.

2.2. Les procédures et délais de traitement de la CNCTR

Les lois du 24 juillet et du 30 novembre 2015 ont renforcé l'État de droit en conciliant la protection de la vie privée et les besoins des services de renseignement pour accomplir leurs missions. À cette fin, la procédure d'autorisation de mise en œuvre des techniques de renseignement a été conçue pour que les demandes soient traitées dans les meilleurs délais tout en garantissant l'efficacité du contrôle.

2.2.1. La procédure d'autorisation de droit commun

Les demandes tendant à la mise en œuvre des techniques de renseignement émanent, comme le prévoient les articles L. 821-1 et L. 821-2 du code de la sécurité intérieure, des ministres dont relèvent les services de renseignement, puis sont transmises à la CNCTR pour avis avant que le Premier ministre ne statue. Par dérogation, le deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure a prévu que les agents individuellement désignés et habilités des services puissent transmettre directement à la commission, sans passer par l'autorité ministérielle, les demandes d'accès aux données de connexion les moins attentatoires à la vie privée : il s'agit des demandes d'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, ainsi que des demandes de recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée.

Une fois la CNCTR saisie, l'article L. 821-3 du code de la sécurité intérieure lui donne un délai de vingt-quatre heures pour statuer si l'avis est rendu par un membre de la commission. Ce délai est porté à soixante-douze heures, si la commission est appelée à se prononcer en formation collégiale.

Après instruction par un ou plusieurs chargés de mission de la commission, les avis sur les demandes sont généralement émis par un membre de la commission, qui ne peut être que l'un de ceux issus du Conseil d'État ou de la Cour de cassation. C'est la procédure suivie pour la majorité des demandes. La commission se réunit en outre en formation collégiale, restreinte ou plénière au sens de l'article L. 831-2 du code de la sécurité intérieure[31], pour rendre certains avis :

31 - Voir, pour la composition de ces formations collégiales, le point 2.3.1 du présent rapport.

- ceux dont la loi impose la délibération en formation collégiale ;
- ceux dont l'intérêt doctrinal ou la complexité technique le justifie.

Ne peuvent ainsi être examinées qu'en formation plénière les demandes ciblant les personnes qui exercent des professions protégées (parlementaire, magistrat, avocat, journaliste), en vertu de l'article L. 821-7 du code de la sécurité intérieure.

Ne peuvent être en outre examinées qu'en formation restreinte ou plénière, selon l'article L. 853-3 du même code, les demandes d'introduction dans un lieu d'habitation ou, lorsqu'elles ont pour but le recueil de données informatiques, les demandes d'introduction dans tout lieu privé.

Par ailleurs, l'article L. 832-3 du code de la sécurité intérieure impose de renvoyer en formation collégiale toute question nouvelle ou sérieuse, ce qui explique notamment que tous les avis émis par la CNCTR sur les textes d'application de la loi du 24 juillet 2015 ont été adoptés en formation plénière. Le même article du code donne enfin la faculté à tout membre pouvant émettre seul un avis de convoquer une réunion collégiale lorsqu'il estime incertaine la légalité d'une demande.

Pour garantir la continuité et l'efficacité de l'action des services de renseignement, l'article L. 821-3 du code de la sécurité intérieure a prévu qu'en l'absence d'avis exprès rendu dans les délais légaux, la CNCTR est réputée avoir rendu un avis implicite et le Premier ministre peut statuer. Ce cas de figure ne s'est jamais présenté, la commission ayant veillé à rendre un avis exprès dans les délais légaux sur l'intégralité des demandes qui lui ont été soumises. Afin de respecter les délais impartis par la loi tout en assurant pleinement son contrôle *a priori*, la commission a en particulier décidé de se réunir en formation restreinte plusieurs fois par semaine pendant l'année écoulée, ce qui a représenté plus de 130 séances entre le 3 octobre 2015 et le 2 octobre 2016. Elle organise en outre une réunion plénière par mois, conformément à l'obligation que lui fait l'article L. 832-3 du code de la sécurité intérieure, sans préjudice des réunions extraordinaires en formation plénière convoquées dès que l'examen d'une demande le requiert.

Les professions protégées au sens de l'article L. 821-7 du code de la sécurité intérieure

Sont protégés de manière particulière par la loi les parlementaires, magistrats, avocats et journalistes, dès lors qu'une technique de renseignement ne peut être mise en œuvre sur le territoire national à leur encontre à raison de l'exercice de leurs professions. Toute demande de mise en œuvre d'une technique à leur encontre doit par ailleurs être examinée par la commission en formation plénière. Le Premier ministre ne peut recourir à la procédure en urgence absolue pour autoriser une telle technique. Enfin, le produit de la mise en œuvre des techniques, à savoir les transcriptions des renseignements collectés, doit être transmis à la commission pour que celle-ci effectue un contrôle spécifique sur les atteintes portées le cas échéant aux garanties s'attachant à l'exercice de ces professions protégées.

Pour appliquer l'ensemble de ces dispositions, la CNCTR a estimé nécessaire, par une délibération adoptée en formation plénière le 29 octobre 2015[32], de préciser la définition des quatre professions protégées.

La CNCTR a tout d'abord considéré que la protection de la loi bénéficiait, sur le territoire national, à toute personne, quelle que soit sa nationalité, qui, en France, dans son pays d'origine ou dans le cadre international, exerce l'une des professions mentionnées par la loi ou détient un mandat de même nature que celui des parlementaires français.

1) Au titre du mandat de parlementaire, sont ainsi protégés les députés et les sénateurs français, les députés européens ainsi que toute personne qui, dans son pays, tient du suffrage universel direct ou indirect un mandat national ou fédéral.

2) Sont protégés les magistrats en fonction dans une juridiction de l'ordre judiciaire ou de l'ordre administratif français, les membres du Conseil d'État, les magistrats en fonction dans les juridictions financières françaises.

32 - Voir l'annexe n° 1 au présent rapport.

Sont assimilés à des magistrats, au sens de l'article L. 821-7 du code de la sécurité intérieure, les membres du Conseil constitutionnel, les juges de proximité, les juges consulaires et les conseillers prud'homaux. Sont également magistrats les juges des juridictions de l'Union européennes, ceux des juridictions internationales et, plus généralement, tout juge qui, dans son pays ou dans un cadre international, détient d'un État ou d'une organisation interétatique, le pouvoir de trancher en toute indépendance des différends ou de prononcer des sanctions par des décisions exécutoires au moyen de la force publique.

3) Sont protégés tous avocats inscrits au barreau d'un tribunal de grande instance français, les avocats membre de l'ordre des avocats au Conseil d'État et à la Cour de cassation et les ressortissants européens qui exercent la profession d'avocat en France sous leur titre professionnel d'origine et sont inscrits sur la liste spéciale d'un barreau. D'une manière générale, sont considérés comme avocats les personnes, quel que soit leur titre, qui, au bénéfice d'une qualification reconnue, tiennent de la loi le pouvoir de représenter ou d'assister une personne devant une juridiction instituée par un État et sont astreintes à des obligations professionnelles et déontologiques.

4) Est journaliste toute personne qui, exerçant sa profession dans une ou plusieurs entreprises de presse ou d'édition, de communication au public en ligne, de communication audiovisuelle ou auprès d'une ou de plusieurs agences de presse, en France ou à l'étranger, y pratique, à titre régulier et rétribué, le recueil d'informations et leur diffusion au public[33].

Ces définitions ont vocation à s'appliquer dans le cadre de la surveillance des communications électroniques internationales. L'article L. 854-3 du code de la sécurité intérieure a en effet également conféré une protection particulière aux personnes exerçant en France l'une des quatre mêmes professions, les mesures de surveillance ne pouvant être mises en œuvre à leur encontre à raison de l'exercice de celles-ci.

33 - Cette définition s'inspire de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse, qui protège le secret des sources des journalistes.

2.2.2. La procédure en cas d'urgence absolue

En cas d'urgence absolue concernant soit l'indépendance nationale, l'intégrité du territoire et la défense nationale, soit la prévention du terrorisme, soit encore la prévention des atteintes à la forme républicaine des institutions, l'article L. 821-5 du code de la sécurité intérieure autorise le Premier ministre à statuer sans avis préalable de la CNCTR[34].

Dans un contexte marqué par une menace terroriste persistante, ayant notamment entraîné l'instauration et la prorogation de l'état d'urgence, le Premier ministre n'a recouru qu'une fois à la procédure en cas d'urgence absolue, pour une demande de mise en œuvre de techniques de renseignement fondée sur la prévention du terrorisme. Conformément à la loi, la commission en a été immédiatement informée (le délégué du Premier ministre avait de surcroît informellement prévenu la CNCTR avant même que la décision ne soit effectivement prise) et tous les éléments de fait et de droit lui ont été communiqués pour justifier le recours à cette procédure exceptionnelle.

34 - La loi du 24 juillet 2015 avait également prévu, en cas d'urgence dite « opérationnelle », la possibilité pour les agents des services de renseignement de recourir à des balises ou à des *IMSI catchers* sans autorisation préalable du Premier ministre ni avis *a priori* de la CNCTR, lorsque était avérée une menace imminente ou un risque très élevé de ne pouvoir effectuer l'opération ultérieurement. Une information sans délai du Premier ministre et de la CNCTR, suivie d'une autorisation *a posteriori*, au vu des éléments de motivation apportés par le service, était censée régulariser la mise en œuvre de ces techniques. Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil Constitutionnel a censuré cette disposition comme portant une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances.

2.3. L'organisation et le fonctionnement de la CNCTR

2.3.1. Une instance collégiale

La CNCTR se compose de neuf membres, en vertu de l'article L. 831-1 du code de la sécurité intérieure[35] : quatre parlementaires (deux députés et deux sénateurs désignés par leur assemblée respective), deux membres du Conseil d'État nommés par le vice-président de cette institution, deux magistrats de la Cour de cassation nommés conjointement par le premier président et le procureur général de la cour, ainsi qu'une personnalité qualifiée en raison de sa connaissance en matière de communications électroniques (la personnalité est nommée par le Président de la République sur proposition du président de l'Autorité de régulation des communications électroniques et des postes). Conformément à la loi, les nominations ont assuré une égale représentation des femmes et des hommes au sein de la commission. En outre, les parlementaires comptent pour moitié des élus de la majorité et pour moitié des élus de l'opposition.

La CNCTR peut siéger en deux formations collégiales, conformément à l'article L. 831-2 du code de la sécurité intérieure. La formation plénière comprend tous les membres de la commission. La formation restreinte comprend les deux membres du Conseil d'État, les deux magistrats de la Cour de cassation et la personnalité qualifiée. Trois de ses membres, dont le président, exercent leurs fonctions à plein temps, les deux autres à temps partiel.

Nourrie du débat entre membres de formations et d'expériences diverses et complémentaires, la CNCTR attache, dans son fonctionnement quotidien, la plus grande importance au respect de la collégialité, gage de qualité du contrôle exercé.

35 - Voir, pour la composition du collège de la CNCTR, l'annexe 6 au présent rapport.

2.3.2. Une instance soumise à des règles d'indépendance et de déontologie

Afin de garantir l'indépendance des membres de la commission, l'article L. 832-1 du code de la sécurité intérieure dispose que ceux-ci ne reçoivent d'instruction d'aucune autorité.

La prévention des conflits d'intérêts est assurée par l'application aux membres de la CNCTR de l'article 11 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique ainsi que de l'article L. 832-2 du code de la sécurité intérieure, qui interdit aux membres la prise d'intérêts, directs ou indirects, dans les services de renseignement ou chez les opérateurs de communications électroniques ainsi que les fournisseurs de services sur internet.

La règle d'incompatibilité entre un mandat de membre et une autre activité professionnelle exercée à temps plein est respectée par tous ceux auxquels elle s'applique, la loi ayant logiquement exempté les parlementaires du respect de cette disposition.

Enfin, le règlement intérieur de la commission[36], adopté en formation plénière le 29 octobre 2015, précise les obligations et règles déontologiques que les membres mais aussi les agents de la CNCTR doivent respecter. Outre la prévention des conflits d'intérêts, dont la nécessité est rappelée, le règlement intérieur énonce, à ses articles 1er à 5, les obligations de loyauté, de confidentialité, d'impartialité et de neutralité, qui s'imposent aux membres et aux agents à tout moment de leurs travaux et après la cessation de leurs fonctions au sein de la CNCTR.

36 - Voir l'annexe n° 5 au présent rapport.

La protection du secret de la défense nationale

Les travaux de la CNCTR, couverts par le secret de la défense nationale en vertu de l'article L. 832-5 du code de la sécurité intérieure, exigent le respect de mesures de sécurité particulières, découlant des articles 413-9 et suivants du code pénal et des textes pris pour leur application.

Les membres de la CNCTR sont habilités ès qualités par la loi à connaître des informations classifiées utiles à l'exercice de leurs fonctions. Les agents doivent, quant à eux, faire l'objet d'une procédure d'habilitation afin d'accéder à ces mêmes informations.

Les locaux de la commission sont régulièrement inspectés par le service compétent pour vérifier leur conformité aux dispositions de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

Le règlement intérieur de la commission rappelle en outre, à son article 3, les règles régissant le besoin de connaître d'informations couvertes par le secret : si les membres et agents ont accès à toute l'information nécessaire à l'accomplissement de leurs missions, le partage d'informations avec les interlocuteurs extérieurs à la commission doit s'effectuer dans le strict respect du besoin d'en connaître.

2.3.3. Les moyens humains et matériels de la CNCTR

Dès son installation le 3 octobre 2015, date d'entrée en vigueur du décret du 1er octobre 2015 relatif à la composition de la Commission nationale de contrôle des techniques de renseignement, la CNCTR a pu débuter ses travaux grâce au personnel et aux moyens précédemment attachés à la CNCIS et à la personnalité qualifiée placée auprès du Premier ministre[37].

37 - La CNCIS comptait six agents au moment de la cessation de ses activités (une déléguée générale, trois chargés de mission et deux agents affectés à des fonctions de soutien). Ils ont été tous intégrés au sein de la CNCTR. La personnalité qualifiée, chargée d'examiner les demandes d'accès aux données de connexion, était assistée de deux adjoints (ces deux agents ainsi qu'un troisième « équivalent temps plein » ont été affectés à la CNCTR). En outre, la CNCIS a légué à la nouvelle commission les outils informatiques mis à sa disposition par le GIC pour mener à bien ses missions de contrôle *a priori* et *a posteriori*.

Au 2 octobre 2016, le collège de la CNCTR s'appuyait sur une équipe de quinze agents, fonctionnaires titulaires ou contractuels. Cette équipe se compose du secrétaire général, nommé par le président en application de l'article L. 832-4 du code de la sécurité intérieure, d'un conseiller placé auprès du président, de dix chargés de mission et de quatre agents affectés aux fonctions de soutien. Eu égard aux missions d'instruction et de contrôle qui leur sont confiées, les agents de la commission, aux parcours divers, sont essentiellement recrutés pour leurs connaissances juridiques ou techniques.

Pour effectuer ses missions de contrôle, en particulier *a priori* mais le cas échéant également *a posteriori*, la CNCTR s'appuie sur des outils informatiques mis à disposition par le GIC.

Les crédits de la CNCTR, composés des dépenses de personnel et des dépenses de fonctionnement autres que de personnel, sont inscrits, dans un souci de rationalisation de l'exécution budgétaire, au budget des services du Premier ministre (mission « Direction de l'action du Gouvernement », programme 308 « Protection des droits et des libertés », action 7 « Sécurité et protection des libertés »), sans que cela ait un quelconque impact sur la nature d'autorité administrative indépendante de la commission. L'article L. 832-4 du code de la sécurité intérieure prévoit à cet égard que le président de la CNCTR est l'ordonnateur des dépenses de la commission, que la Cour des comptes a compétence pour contrôler.

Les crédits alloués à la CNCTR par la loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016 s'élèvent à 2 957 641 euros, dont 2 564 755 euros pour les dépenses de personnel et 392 886 euros pour les autres dépenses de fonctionnement. Leur progression par rapport à ceux de la CNCIS est justifiée par l'élargissement des missions attribuées à la CNCTR. ◘

3e partie

L'intense activité de contrôle préalable lors d'une première année d'activité marquée par une forte menace terroriste

L'intense activité de contrôle préalable lors d'une première année d'activité marquée par une forte menace terroriste

La CNCTR, par les avis préalables qu'elle rend sur les demandes tendant à la mise en œuvre de techniques de renseignement, est l'un des maillons de la chaîne opérationnelle conduisant au recueil du renseignement. Ses avis, émis dans des délais courts, constituent une étape qui, sans nuire à la réactivité attendue des services de renseignement, a pour but de garantir que les éventuelles atteintes portées à la vie privée sont proportionnées à la gravité des menaces ou au caractère fondamental des enjeux invoqués.

Dans les faits, si l'article L. 821-3 du code de la sécurité intérieure impartit à la CNCTR de se prononcer en vingt-quatre heures ou, en cas de convocation d'une formation collégiale, en soixante-douze heures, la plupart des demandes sont traitées dans des délais inférieurs.

À cela s'ajoute un traitement plus rapide des demandes présentées comme prioritaires. Il s'agit, pour l'essentiel, de demandes motivées par la prévention du terrorisme. Non prévue par la loi, pratiquée à l'époque de la CNCIS et reprise à titre également informel par la CNCTR pour s'adapter dans la mesure du possible à l'urgence, la procédure prioritaire conduit la commission à rendre des avis en moins d'une heure en moyenne. Confrontée aux attaques terroristes du 13 novembre 2015 par exemple, la commission a pu ainsi rendre certains avis en quelques minutes lorsque les circonstances l'exigeaient et que les éléments soumis à son appréciation le permettaient. Cette forte réactivité, dont la commission ne fait usage que dans la mesure où elle est compatible avec le plein exercice de son contrôle, est par ailleurs la preuve que la procédure en cas d'urgence absolue prévue à l'article L. 821-5 du code de la sécurité intérieure, par laquelle le Premier ministre autorise directement la mise en œuvre d'une technique sans solliciter l'avis de la commission, doit être réservée à des cas exceptionnels.

3.1. Les fondements et principes de l'avis préalable de la CNCTR

La mission de contrôle *a priori* confiée par la loi à la CNCTR consiste à examiner la légalité des demandes tendant à la mise en œuvre de techniques de renseignement, notamment au regard des critères énoncés à l'article L. 801-1 du code de la sécurité intérieure.

Il s'agit tout d'abord d'un examen de la légalité externe : compétence de l'auteur de la demande, régularité de la procédure et, surtout, caractère suffisant de la motivation, qui doit être circonstanciée et, si elle peut être concise, ne saurait être stéréotypée.

L'essentiel du contrôle porte toutefois sur la légalité interne :

- adéquation de la demande aux missions confiées au service de renseignement demandeur ;
- sincérité de la motivation et exactitude des faits sur lesquels elle s'appuie ;
- justification de la demande au regard des finalités invoquées, qui ne peuvent être que celles prévues à l'article L. 811-3 du code de la sécurité intérieure ;
- proportionnalité des atteintes portées à la vie privée aux motifs invoqués et aux buts poursuivis ;
- impossibilité de recueillir les renseignements recherchés par un autre moyen légalement autorisé, ce critère dit de « subsidiarité » n'étant prévu que pour les techniques les plus intrusives que sont 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), la captation et le recueil de données informatiques (I de l'article L. 853-2 du code) et l'introduction dans un lieu privé (article L. 853-3 du code).

Un tel contrôle, outre qu'il apporte au Premier ministre un avis juridique indépendant sur la légalité d'atteintes à la vie privée, permet à la CNCTR de mener un dialogue constructif avec les services de renseignement. Ainsi la commission peut, après avoir reçu une demande qu'elle estime insuffisamment motivée, difficile à apprécier ou d'une légalité incertaine, demander des informations complémentaires au ministre et, partant, au service de renseignement dont elle émane. Les délais impartis par la loi à la commission pour se prononcer courent alors à compter de la réception des éléments complétant la demande[38].

La commission rend des avis favorables ou défavorables. Les avis défavorables sont motivés, de façon à faire apparaître la doctrine de la commission sur l'application du cadre légal. Les avis favorables peuvent être assortis d'observations ou de restrictions.

Les observations peuvent consister à indiquer au Premier ministre et au service demandeur qu'en l'état des éléments fournis à la commission, la mise en œuvre de la technique ne devrait être autorisée qu'une seule fois ou, en cas de renouvellement d'une autorisation, que ce renouvellement pourrait être le dernier qu'approuverait la commission.

Les restrictions peuvent principalement porter sur la durée de validité de l'autorisation, l'avis recommandant alors une durée inférieure au maximum prévu par la loi pour la technique concernée. Une telle restriction peut être motivée par la volonté de limiter l'usage de la technique à la durée d'un événement ponctuel, qui seul justifie cet usage, ou d'inciter le service bénéficiaire à identifier rapidement une personne surveillée mais dont l'identité était inconnue lors de la première mise en œuvre d'une technique.

En outre, au nom de la séparation des pouvoirs, la CNCTR émet un avis défavorable à la mise en œuvre de techniques de renseignement lorsque les faits motivant la demande font l'objet d'une procédure judiciaire ou qu'il apparaît que le service de renseignement dispose de toutes les informations nécessaires pour saisir le procureur de la République des faits concernés[39].

---

38 - Faute de réponse du ministre dans un délai de quinze jours, le GIC adresse à ce dernier une invitation à produire les éléments réclamés par la CNCTR dans un nouveau délai quinze jours. Si cette invitation demeure également sans réponse, la demande est réputée abandonnée.

39 - À cet égard, la CNCTR rappelle qu'aux termes de l'article L. 811-2 du code de la sécurité intérieure, la mise en œuvre des techniques de renseignement s'effectue sans préjudice des dispositions de l'article 40 du code de procédure pénale : le second alinéa de cet article prévoit que « *toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* ».

3.2. La présentation statistique des demandes de mise en œuvre de techniques de renseignement

Dans l'attente des applications informatiques en cours de développement par le GIC pour dématérialiser et unifier l'ensemble de la procédure de demande de mise en œuvre de techniques de renseignement, la CNCTR ne dispose pas encore d'outils fournissant de manière automatisée des chiffres consolidés. Les éléments statistiques figurant dans le présent rapport sont donc le résultat d'un travail d'extraction et d'agrégation de données mené conjointement avec le GIC, puis de fiabilisation des résultats.

Au cours de la première année de fonctionnement de la CNCTR, du 3 octobre 2015 au 2 octobre 2016, les avis préalables émis, dont le nombre est égal à celui de demandes reçues[40], se répartissent comme indiqué dans le tableau général ci-dessous.

Technique de renseignement	Nombre d'avis préalables rendus
Accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure)	48 208
Géolocalisation en temps réel (article L. 851-4 du code de la sécurité intérieure)	2 127
Interceptions de sécurité (I de l'article L. 852-1 du code de la sécurité intérieure)	8 538
Autres techniques	7 711

40 - S'agissant toutefois des accès aux données de connexion en temps différé, les demandes ont été traitées, entre le 3 octobre 2015 et le 31 janvier 2016, par la personnalité qualifiée placée auprès du Premier ministre. À compter du 1er février 2016, date à laquelle est entré en vigueur le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, ces demandes ont été soumises à la CNCTR pour avis avant décision du Premier ministre.

Sur cette même période, la commission a rendu, hors demandes d'accès aux données de connexion en temps différé, 1 263 avis défavorables, soit un pourcentage de 6,9 % du nombre d'avis rendus. Ce taux, plus élevé que celui résultant du contrôle opéré par la CNCIS, peut s'expliquer par le fait que les nouvelles techniques de renseignement sont, pour certaines d'entre elles, plus intrusives que celles prévues par le cadre juridique antérieur, ce qui entraîne un niveau de contrôle d'autant plus rigoureux. Le taux est susceptible d'évoluer au fur et à mesure que les services de renseignement se conformeront à la doctrine de la CNCTR.

Le Premier ministre n'a accordé, à la date de publication du présent rapport, aucune autorisation après un avis défavorable de la commission.

3.2.1. Les accès aux données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure)

Alors que 42 374 demandes d'accès aux données de connexion en temps différé avaient été présentées à la personnalité qualifiée placée auprès du Premier ministre en 2015[41], 48 208 demandes similaires ont été traitées entre le 3 octobre 2015 et le 2 octobre 2016[42], ce qui représente une augmentation de 14 %.

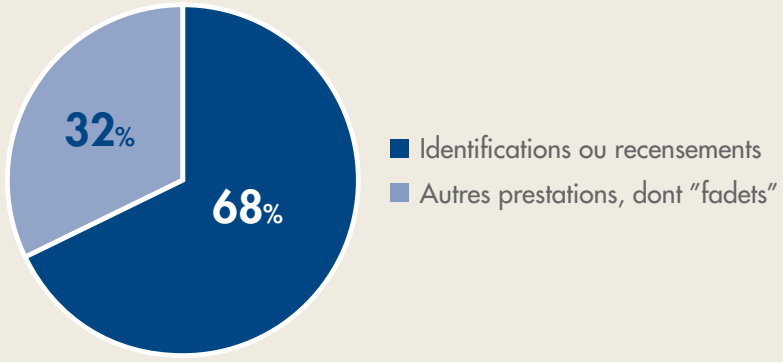
La grande majorité des demandes a pour but l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ou, à l'inverse, le recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée : ces demandes,

41 - Ce chiffre figure dans le rapport, non public, adressé au Premier ministre par la personnalité qualifiée pour rendre compte de son activité en 2015. Par ailleurs, des comparaisons chiffrées avec les années antérieures à 2015 paraissent malaisées, les régimes d'accès aux données de connexion alors en vigueur n'ayant pas le même champ d'application (un premier régime, institué par l'article 6 de la de la loi n° 2006-64 du 20 janvier 2006 relative à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers permettait aux services de renseignement relevant du ministre de l'intérieur de recueillir, dans le seul cas de lutte contre le terrorisme, des données de connexion auprès des opérateurs de communications électroniques ou auprès des fournisseurs de services sur internet ; un deuxième régime, prévu à l'article 22 de la loi du 10 juillet 1991 et ouvert à tous les services de renseignement, permettait de recueillir les données de connexion nécessaires pour la réalisation et l'exploitation des interceptions de sécurité).

42 - Entre le 3 octobre 2015 et le 31 janvier 2016, les demandes ont été traitées par la personnalité qualifiée placée auprès du Premier ministre. À compter du 1er février 2016, date à laquelle est entré en vigueur le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, les demandes ont été soumises à la CNCTR pour avis avant décision du Premier ministre.

qui s'élèvent à 32 997, représentent près de 68,5 % du total des demandes fondées sur l'article L. 851-1 du code de la sécurité intérieure. Pour le surplus, à savoir 15 211 demandes, il s'agit essentiellement d'obtenir la liste des appels et des correspondants de la personne surveillée, généralement dénommée « facture détaillée » ou « fadet ».

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



Le taux d'avis défavorables concernant ces demandes ne s'élève qu'à 0,14 % (il s'élevait à 0,06 % entre le 1er janvier et le 31 décembre 2015). Ces avis sont principalement fondés sur le caractère incomplet des demandes ou l'absence de lien avec l'une des finalités limitativement prévues à l'article L. 811-3 du code de la sécurité intérieure pour recourir à une technique de renseignement.

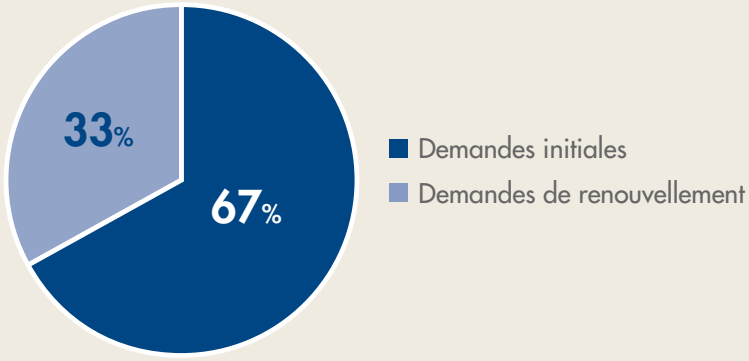
3.2.2. Les géolocalisations en temps réel (article L. 851-4 du code de la sécurité intérieure)

Autorisée depuis le 1er janvier 2015 et reprise dans le nouveau cadre légal applicable aux techniques de renseignement, les demandes de géolocalisation en temps réel, qui avaient vu leur nombre croître au cours de l'année 2015 pour atteindre 1 140 au 31 décembre 2015, ont continué leur forte progression en 2016 : 2 127 demandes ont été soumises à la CNCTR durant sa première année d'activité, entre le 3 octobre 2015 et le 2 octobre 2016, ce qui représente une augmentation de 87 %. Cette évolution traduit l'appropriation par les services de la technique nouvelle.

3.2.3. Les interceptions de sécurité (I de l'article L. 852-1 du code de la sécurité intérieure)

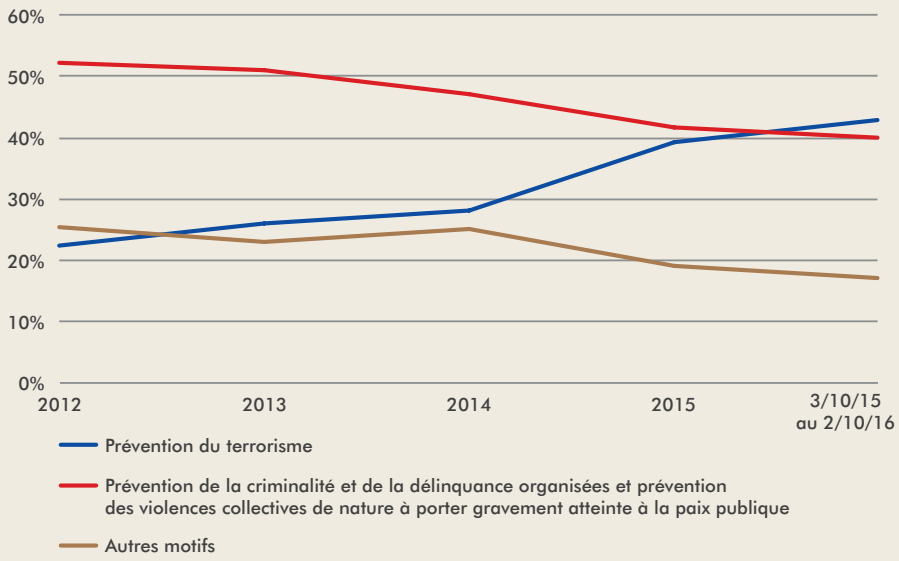
Depuis le 3 octobre 2015, la CNCTR a rendu 8 538 avis sur des demandes d'interceptions de sécurité, dont 67 % de demandes initiales et 33 % de demandes de renouvellement. Par comparaison, la CNCIS avait émis 6 628 avis sur des demandes similaires en un an en 2014. En outre, 7 703 avis avait été rendus en 2015 (ces avis avaient été rendus par la CNCIS jusqu'au 2 octobre 2015 et par la CNCTR entre le 3 octobre et le 31 décembre 2015). Ces chiffres traduisent un recours accru mais maîtrisé à cette mesure, dans un contexte fortement marqué par la menace terroriste.

La répartition des demandes d'interceptions de sécurité

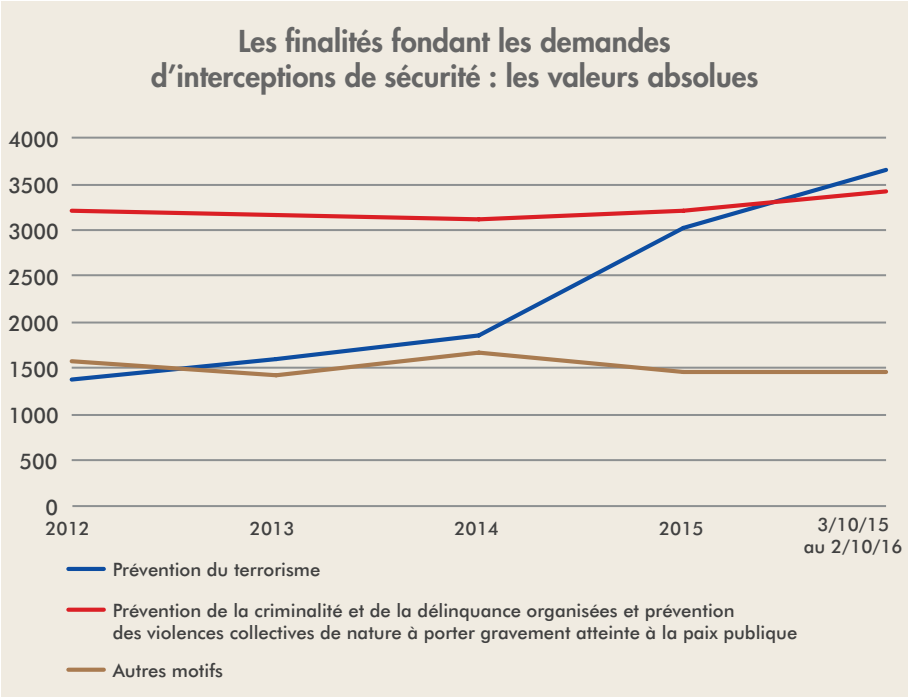


Le fait marquant concernant les interceptions de sécurité a trait aux finalités invoquées pour fonder la mise en œuvre de cette technique. Alors qu'en 2014, 47 % des demandes d'interceptions de sécurité étaient présentées sur le fondement de la prévention de la criminalité et de la délinquance organisées et 28 % sur celui de la prévention du terrorisme, ce rapport s'est inversé au cours de l'année 2015. Entre le 3 octobre 2015 et le 2 octobre 2016, 43 % des demandes ont été motivées par la prévention du terrorisme et 40 % par la prévention de la criminalité et de la délinquance organisées ainsi que des violences collectives de nature à porter gravement atteinte à la paix publique[43]. L'analyse des chiffres mensuels des demandes montre que c'est au mois de janvier 2015 que la prévention du terrorisme a, pour la première fois, été le fondement légal le plus fréquemment invoqué.

Les finalités fondant les demandes d'interceptions de sécurité : les pourcentages



43 - Les demandes présentées, avant le 3 octobre 2015, sur le fondement de la prévention de la criminalité organisée ont été comparées avec celles présentées, après le 3 octobre 2015, sur ce même fondement ainsi que sur celui de la prévention des violences collectives portant gravement atteinte à la paix publique. Les demandes désormais fondées sur ce dernier motif étaient en effet principalement rattachées à la lutte contre la criminalité organisée dans l'ancien cadre légal.



Les interceptions de sécurité sont en outre caractérisées par l'existence d'un contingentement du nombre d'interceptions pouvant être réalisées simultanément. Prévu au VI de l'article L. 852-1 du code de la sécurité intérieure, ce contingentement avait été à l'origine instauré par une décision du Premier ministre du 28 mars 1960 en raison de contraintes techniques (il correspondait à la capacité maximale d'enregistrement de conversations sur des magnétophones). Conservé par la loi du 10 juillet 1991, le contingentement a été alors conçu comme une incitation pour les services bénéficiaires à supprimer les interceptions inutiles avant de pouvoir en effectuer de nouvelles, mais aussi à ne recourir à cette technique que « *dans les seuls cas de nécessité d'intérêt public prévus par la loi* », ainsi que l'énonce, dans le cadre légal actuel, l'article L. 801-1 du code de la sécurité intérieure à propos de toutes les atteintes à la vie privée que peut porter l'autorité publique aux fins de recueil de renseignements.

En pratique, le contingentement signifie que le nombre d'interceptions de sécurité en cours de réalisation doit à tout moment respecter un maximum fixé par ministère par un arrêté du Premier ministre pris après avis de la CNCTR. La répartition du contingentement entre services de renseignement à l'intérieur d'un même ministère relève de la compétence du ministre concerné.

Le contingentement n'a pas été modifié depuis l'entrée en vigueur de la loi du 24 juillet 2015.

L'évolution du contingentement des interceptions de sécurité[44]

	1991	1997	2003	2005	2009[45]	2014	2015
Défense	232	330	400	450	285	285	320
Intérieur	928	1190	1190	1290	1455	1785	2235
Budget	20	20	80	100	100	120	145
Total	1180	1540	1670	1840	1840	2190	2700

3.2.4. Les autres techniques de renseignement

Sont concernées les demandes d'accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure), celles de mise en œuvre de traitements automatisés sur des données de connexion (article L. 851-3 du code)[46], celles de balisage (article L. 851-5 du code), celles de recueil de données de connexion par *IMSI catcher* (article L. 851-6 du code),

44 - Les dates figurant dans le tableau sont celles auxquelles le Premier ministre a pris une décision fixant les chiffres du contingentement. Aucune nouvelle décision n'a été prise depuis le 3 octobre 2015.

45 - Pour mémoire, en 2009, la gendarmerie nationale a été rattachée au ministère de l'intérieur, ce qui a conduit à une évolution de la répartition du contingentement entre le ministère de la défense et celui de l'intérieur.

46 - Comme il a été déjà été indiqué au point 2.1.4.1 du présent rapport, aucune demande de mise en œuvre de traitements automatisés sur des données de connexion n'a encore été présentée à la CNCTR sur le fondement de l'article L. 851-3 du code de la sécurité intérieure.

celles d'interceptions de sécurité par *IMSI catcher* (II de l'article L. 852-1 du code), celles de captation de paroles prononcées à titre confidentiel ou d'images dans un lieu privé (article L. 853-1 du code), celles de recueil et de captation de données informatiques (article L. 853-2 du code) et celles d'introduction dans un lieu privé (article L. 853-3 du code).

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

Les techniques concernées ont fait l'objet de 7 711 demandes de mise en œuvre entre le 3 octobre 2015 et le 2 octobre 2016. La CNCTR a constaté que les services de renseignement s'étaient progressivement approprié ces techniques nouvelles. Le chiffre indiqué ne reflète donc sans doute pas une année de mise en œuvre ordinaire.

3.3. La création d'un nouvel outil d'évaluation : le nombre de personnes surveillées

La loi a confié à la CNCTR un pouvoir de contrôle se traduisant notamment par la réception de toutes les demandes et autorisations de mise en œuvre de techniques de renseignement ainsi que par un accès permanent, complet et direct aux relevés de mise en œuvre, en application de l'article L. 833-2 du code de la sécurité intérieure. La commission a souhaité exploiter ces prérogatives légales pour déterminer, en l'état des outils informatiques disponibles, le nombre de personnes ayant, entre le 3 octobre 2015 et le 2 octobre 2016, fait l'objet d'au moins une technique de renseignement autorisée en application de la loi du 24 juillet 2015.

Le calcul de cet indicateur a supposé la résolution de difficultés dès lors que les demandes de mise en œuvre de techniques sont présentées par technique et non par personne, que le traitement informatique des demandes n'a pas encore été entièrement harmonisé, enfin que certaines personnes ne sont pas nommément identifiées.

En égard aux considérations qui précèdent, les chiffres obtenus ne sauraient être regardés comme dépourvus de toute marge d'erreur. Ils peuvent toutefois donner une mesure des atteintes portées à la vie privée de personnes pour les motifs tenant à la défense ou à la promotion des intérêts fondamentaux de la Nation limitativement prévus à l'article L. 811-3 du code de la sécurité intérieure. La commission se propose de préciser et fiabiliser cette mesure dans les prochains rapports, lorsque l'évolution des outils informatiques le permettra.

Du 3 octobre 2015 au 2 octobre 2016, 20 282 personnes ont fait l'objet d'une technique de renseignement au moins[47]. Ce chiffre ne comprend pas les accès aux données de connexion en temps différé prévus au deuxième alinéa de l'article L. 851-1 du code de la sécurité intérieure, principalement l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ainsi que le recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée. Cette technique, la moins intrusive de toutes celles prévues au livre VIII du code de la sécurité intérieure, est en effet conçue non tant comme une mesure de surveillance que comme une mesure préparatoire à des mesures de surveillance, à commencer par l'obtention des « fadets » de la personne concernée en application du premier alinéa de l'article L. 851-1 du code de la sécurité intérieure.

Dans ce cadre :

- 9 624 personnes, soit 47 % du total, ont été surveillées au titre de la prévention du terrorisme ;
- 5 848 personnes, soit 29 % du total, ont été surveillées au titre de la prévention de la criminalité et de la délinquance organisées ainsi que de la prévention des violences collectives de nature à porter gravement atteinte à la paix publique.

47 - La CNCTR a évalué la marge d'erreur à moins de 10 %.

4e partie

Les défis du contrôle *a posteriori*

Les défis du contrôle *a posteriori*

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. En conséquence, si elle rend un avis sur chaque demande de mise en œuvre de technique préalablement à la décision du Premier ministre, il lui appartient également de contrôler l'existence d'une autorisation avant toute mise en œuvre ainsi que l'exécution des techniques autorisées.

Pour mener cette mission de contrôle *a posteriori*, la CNCTR dispose notamment, en application de l'article L. 833-2 du code de la sécurité intérieure, d'un accès permanent, complet et direct aux relevés de mise en œuvre, aux registres prévus par la loi, comme celui des *IMSI catchers* mentionnés au II de l'article L. 851-6 du code, aux renseignements collectés ainsi qu'aux transcriptions et extractions effectuées par les services bénéficiaires. En outre, la commission accède dans les mêmes conditions aux dispositifs de traçabilité des renseignements collectés et aux locaux où ceux-ci sont collectés.

4.1. Des capacités de contrôle performantes sur les accès aux données de connexion, les géolocalisations en temps réel et les interceptions de sécurité

Les recueils de données de connexion en temps différé (article L. 851-1 du code de la sécurité intérieure), les géolocalisations en temps réel (article L. 851-4 du code) et les interceptions de sécurité (I de l'article L. 852-1 du code) sont exécutés de façon centralisée par le GIC, qui recueille les données ou les correspondances concernées auprès des opérateurs de communications électroniques ou des fournisseurs de services sur internet.

Le GIC conserve ainsi l'intégralité des renseignements collectés et les met, par des applications informatiques, à la disposition de la commission qui peut vérifier leur conformité au livre VIII du code de la sécurité intérieure et à l'autorisation du Premier ministre.

Par ailleurs, conformément à sa demande formulée dans sa délibération n° 1/2016 du 14 janvier 2016[48], la CNCTR a obtenu que lui soit garanti dans les locaux du GIC un accès permanent, complet, direct et immédiat à l'ensemble des données de connexion recueillies en temps réel sur le fondement de l'article L. 851-2 du code de la sécurité intérieure.

Dans le cas particulier des interceptions de sécurité, le système de contrôle hérité de la loi du 10 juillet 1991 a été maintenu. Il comporte plusieurs niveaux de vérifications.

Le GIC effectue lui-même un premier contrôle, en vérifiant que les lignes téléphoniques sur lesquelles portent les interceptions sont actives et utilisées par la personne mentionnée dans la demande. Une fois les correspondances transcrites, le GIC vérifie que ces transcriptions ne comportent que des renseignements liés à la finalité fondant l'autorisation : ce n'est qu'après cette vérification que le service bénéficiaire est autorisé à diffuser en son sein les transcriptions aux agents habilités.

La CNCTR, quant à elle, s'assure, en prenant connaissance des correspondances interceptées et des transcriptions effectuées à partir d'elles, non seulement que les renseignements sont effectivement et exclusivement recueillis pour la finalité fondant l'autorisation mais aussi que l'interception, eu égard à ses résultats, n'est pas disproportionnée par rapport à l'atteinte qu'elle porte à la vie privée de la personne surveillée. Ce suivi permet d'enrichir l'instruction des éventuelles demandes de renouvellement d'interception. Il met la commission en mesure de recommander, le cas échéant, l'interruption d'une interception en cours.

48 - Voir l'annexe n° 3 au présent rapport.

Outre ce suivi, le contrôle de la CNCTR sur les interceptions de sécurité peut consister à se rendre dans des centres dépendant du GIC (les centres sont implantés sur tout le territoire national pour rapprocher des services bénéficiaires le lieu d'exploitation des interceptions). Ces déplacements, qui permettent de rencontrer les agents exploitants au niveau local, ont pour but d'expliquer et diffuser la doctrine de la commission sur l'ensemble des techniques de renseignement, mais aussi d'évoquer et de clarifier le cas d'interceptions problématiques.

4.2. L'approfondissement du contrôle sur les nouvelles techniques de renseignement

4.2.1. Une question essentielle : la centralisation des renseignements recueillis

Les nouvelles techniques de renseignement mises en œuvre depuis l'entrée en vigueur de la loi du 24 juillet 2015, à savoir le balisage (article L. 851-5 du code de la sécurité intérieure), le recueil de données de connexion par *IMSI catchers* (article L. 851-6 du code), les interceptions de sécurité par *IMSI catchers* (II de l'article L. 852-1 du code), la captation de paroles prononcées à titre privé ou d'images dans un lieu privé (article L. 853-1 du code), le recueil et la captation de données informatiques (article L. 853-2 du code) et l'introduction dans un lieu privé (article L. 853-3 du code), se caractérisent toutes par une collecte décentralisée des renseignements, c'est-à-dire effectuée le plus souvent localement pour les services disposant d'administrations déconcentrées comme la DGSI ou la police et la gendarmerie nationales. Or, pour que la CNCTR puisse réellement disposer de l'accès permanent, complet et direct aux renseignements collectés prévu par la loi et, partant, pour qu'elle puisse effectivement contrôler la mise en œuvre des nouvelles techniques, la centralisation des renseignements collectés est indispensable.

La centralisation des renseignements collectés est au demeurant exigée par la loi : l'article L. 822-1 du code de la sécurité intérieure prévoit en effet que le Premier ministre organise la traçabilité de l'exécution des techniques autorisées et définit les modalités de la centralisation des renseignements collectés.

La centralisation ne peut être réussie qu'aux trois conditions suivantes.

- **En premier lieu**, eu égard au volume et à la sensibilité des données concernées, la centralisation suppose de mettre en place des systèmes d'information et d'exploiter des réseaux de communications solides, capables d'une part d'acheminer de façon harmonisée vers un lieu de stockage des données d'un volume important telles que des images ou des vidéos, d'autre part de satisfaire les exigences de sécurité régissant la transmission informatique d'informations couvertes par le secret de la défense nationale. Ce dernier point impose notamment l'utilisation de réseaux dédiés ou de dispositifs sûrs de chiffrement des données.
- **En deuxième lieu**, les renseignements collectés de façon décentralisée ont vocation à être exploités de même : dès lors, les réseaux de communications assurant la remontée des renseignements vers un lieu de stockage doivent également permettre aux agents habilités des services bénéficiaires, en particulier ceux accomplissant leurs missions à un niveau territorial, d'accéder à distance aux renseignements qui les concernent et de les exploiter sous le contrôle de la commission. Il ne saurait, en effet, être prévu que soient centralisés les renseignements bruts collectés tandis que l'exploitation aurait lieu sur une copie des données stockée localement, un tel système recréant la difficulté que la centralisation a précisément pour but d'éviter, à savoir une diffusion non maîtrisée, au sein des services, d'informations concernant la vie privée ainsi que l'impossibilité de contrôler que l'exploitation est conforme à la finalité fondant l'autorisation et que les données sont détruites dans les délais fixés par la loi.

- **En troisième lieu**, s'il peut être envisagé de mettre en place plusieurs lieux de stockage centralisés, cette centralisation ne conserve de sens que si le nombre de lieux demeure limité et que ces lieux sont suffisamment regroupés pour être aisément accessibles aux agents de la commission. La solution retenue consiste à faire du GIC l'organe de centralisation des renseignements collectés par les services dits du « second cercle » ainsi que par les services spécialisés dits du « premier cercle » qui le souhaiteraient, tandis que la DGSI et la DGSE centraliseraient les renseignements recueillis pour leur propre compte ainsi que, dans le cas de la DGSE, pour le compte des autres services spécialisés relevant du ministre de la défense.

La CNCTR est consciente que la construction d'un tel système de centralisation peut durer plusieurs années[49]. Des solutions transitoires devront être trouvées : ainsi pourraient être constitués des lieux de stockage au sein des administrations centrales des services de renseignement, prenant la forme de serveurs sécurisés aux droits d'accès rigoureusement encadrés. Durant cette période transitoire, la nécessité pour la commission de se déplacer dans les unités territoriales des services de renseignement pour assurer pleinement son contrôle demeurera entière.

4.2.2. Les contrôles sur pièce et sur place

À raison d'un contrôle sur pièce et sur place par semaine entre le 3 octobre 2015 et le 1er mai 2016 puis de deux contrôles par semaine à partir de cette date, la CNCTR a mis à profit le recrutement de nouveaux agents pour renforcer son action.

Les premiers déplacements effectués par la commission ont eu pour but principal de présenter les dispositions du nouveau cadre légal ainsi que de faire connaître les solutions adoptées par la CNCTR pour résoudre les premières et nombreuses questions suscitées par son application. La commission a ainsi pu recueillir les observations des services de

49 - Une première étape était, à la date de parution du présent rapport, en cours de réalisation par le GIC pour centraliser le recueil de la quasi-totalité des données de balisage au profit de la DNRED et des services dits du « second cercle ».

renseignement, au niveau tant national que local, et mieux apprécier leurs difficultés opérationnelles. Les contrôles ultérieurs ont été consacrés à l'examen de la mise en œuvre de techniques de renseignement dans des affaires sélectionnées par la commission en fonction de leur importance, de leur caractère représentatif ou des difficultés qu'elles soulèvent.

Les nouvelles techniques de renseignement dont la mise en œuvre a été le plus fréquemment contrôlée sur pièce et sur place sont le balisage, le recueil de données de connexion par *IMSI catchers*, la captation de paroles prononcées à titre privé, la captation d'images dans un lieu privé ainsi que le recueil de données informatiques. Tous les services de renseignement du premier comme du second cercle ont fait l'objet de contrôles *a posteriori*. La commission a relevé la forte mobilisation des services contrôlés et leur haut niveau de coopération lors de ces contrôles.

Des difficultés ont pu toutefois apparaître, s'agissant de la durée de conservation des données de connexion recueillies par *IMSI catchers*, et ont fait l'objet d'une attention particulière. Le III de l'article L. 851-6 du code de la sécurité intérieure prévoit que seules les données de connexion recueillies qui se rapportent à l'autorisation accordée se voient appliquer la durée de droit commun de conservation en cas de recueil de données de connexion, soit quatre ans à compter de leur recueil en application du 3° de l'article L. 822-2 du code. En revanche, les données de connexion recueillies qui sont sans rapport avec l'autorisation doivent être détruites au terme d'un délai spécial plus bref de quatre-vingt-dix jours. Le respect de ce délai particulier, au cours duquel le service bénéficiaire détermine les données recueillies qui ne se rapportent pas à l'autorisation, a nécessité la mise en place de procédures internes rigoureuses. La CNCTR a donc mené des contrôles répétés sur ce point et constaté que les services concernés se conformaient en définitive à ses préconisations.

La gestion des extractions et des transcriptions de renseignements bruts recueillis paraît également susceptible d'être améliorée. Si les extractions et les transcriptions des interceptions de sécurité font, comme il a été dit plus haut, l'objet d'un suivi rigoureux par le GIC, celles produites lors de l'exploitation d'informations recueillies par la mise en œuvre de nouvelles

techniques de renseignement méritent d'être encadrées par des procédures plus strictes. Il en est ainsi des données extraites des captations sonores ou vidéo, des recueils et captations de données informatiques. À cet égard, la CNCTR rappelle qu'elle doit être en mesure, sur le fondement de l'article L. 822-3 du code de la sécurité intérieure, de contrôler que ces transcriptions et extractions n'ont été produites que pour les finalités limitativement prévues à l'article L. 811-3 du code et qu'elles sont détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités.

4.3. La construction du contrôle *a posteriori* sur la surveillance des communications électroniques internationales

Par une délibération classifiée, adoptée en formation plénière le 26 février 2016, la commission a fixé un cadre pour définir les modalités de son contrôle sur les mesures de surveillance des communications électroniques internationales[50].

L'article L. 854-9 du code de la sécurité intérieure, qui régit de façon spéciale les pouvoirs de contrôle de la CNCTR sur la surveillance des communications électroniques internationales, prévoit que la commission dispose d'un accès permanent, complet et direct aux dispositifs de traçabilité des interceptions et exploitations de communications, aux renseignements collectés, aux extractions et transcriptions ainsi qu'aux relevés obligatoirement effectués sur ces opérations d'extraction et de transcription ainsi que sur celles de destruction des renseignements.

À raison de deux contrôles par mois, menés dès l'entrée en vigueur de la loi du 30 novembre 2015, la commission vérifie que les communications concernées sont interceptées, conservées et exploitées conformément aux dispositions des articles L. 854-1 à L. 854-8 du code de la sécurité intérieure. Les contrôles effectués les premiers mois ont eu pour objet principal de

50 - Voir, pour l'analyse des dispositions de la loi du 30 novembre 2015, le point 2.1.5 du présent rapport.

familiariser les membres et les agents de la commission avec les outils de la surveillance internationale. Depuis, la commission utilise des outils informatiques spécifiques destinés à lui permettre de vérifier la conformité des données stockées et des exploitations avec le cadre légal. Elle dispose également d'un accès aux outils informatiques utilisés par les agents des services spécialisés de renseignement bénéficiaires. Les agents de la CNCTR s'emploient notamment à vérifier, dans la durée, le bon fonctionnement et la bonne configuration de ces outils.

4.4. Les recommandations et observations de la CNCTR

La faculté ouverte à la CNCTR de formuler des recommandations au Premier ministre est prévue à l'article L. 833-6 du code de la sécurité intérieure, selon lequel la commission peut recommander que la mise en œuvre d'une technique de renseignement soit interrompue et les informations collectées détruites, lorsqu'elle estime que le cadre légal prévu au livre VIII du code a été méconnu. Ces recommandations peuvent également être adressées au ministre responsable de l'exécution de la technique concernée ou au service bénéficiaire.

Ces dispositions générales sont par ailleurs reprises dans les articles concernant la captation de paroles prononcées à titre privé ou la captation d'images dans un lieu privé (IV de l'article L. 853-1 du code de la sécurité intérieure), le recueil et la captation de données informatiques (IV de l'article L. 853-2 du code) ou encore l'introduction dans un lieu privé (IV de l'article L. 853-3 du code).

Selon l'article L. 833-7 du code de la sécurité intérieure, le Premier ministre informe sans délai la commission des suites données à ses recommandations.

Enfin, la commission dispose, plus généralement, de la possibilité d'adresser à tout moment au Premier ministre les observations qu'elle juge utiles, en application de l'article L. 833-10 du code de la sécurité intérieure.

Entre le 3 octobre 2015 et le 2 octobre 2016, la commission n'a pas eu à faire usage de son pouvoir de recommandation pour que soit interrompue la mise en œuvre d'une technique de renseignement ou que soient détruits des renseignements collectés. Elle a en revanche formulé plusieurs recommandations de portée générale.

Deux de ces recommandations ont déjà été évoquées. L'une porte sur l'architecture générale du dispositif consistant à mettre en œuvre, en application de l'article L. 851-3 du code de la sécurité intérieure, des traitements automatisés sur les réseaux des opérateurs de communications électroniques et des fournisseurs de services sur internet[51]. L'autre tire les conséquences de la décision du Conseil constitutionnel du 21 octobre 2016 sur la surveillance et le contrôle des transmissions empruntant la voie hertzienne[52].

Une troisième recommandation de portée générale a été émise dans une délibération classifiée du 28 avril 2016, par laquelle la CNCTR a souhaité clarifier les dispositions applicables aux différents types de recueils de données de connexion et s'est prononcée sur l'application de l'article L. 871-2 du code de la sécurité intérieure. Survivance de l'ancien article 22 de la loi du 10 juillet 1991, cette disposition permet notamment au Premier ministre de requérir, sans avis préalable de la CNCTR, auprès des opérateurs de communications électroniques et des fournisseurs de services sur internet les données de connexion nécessaires à la réalisation et à l'exploitation des interceptions autorisées par la loi. La CNCTR a constaté toutefois que le III de l'article L. 852-1 du code, qui concerne les interceptions de sécurité, prévoyait lui-même des dispositions spéciales, selon lesquelles l'autorisation de mettre en œuvre une interception de sécurité vaut autorisation de recueil des données de connexion « *nécessaires* »[53] à son exécution et à son exploitation.

51 - Voir, pour le détail de cette recommandation, le point 2.1.4.1 du présent rapport.

52 - Voir, pour le détail de cette recommandation, le point 2.1.6 du présent rapport et l'annexe n° 4.

53 - La loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence a modifié la rédaction du III de l'article L. 852-1 en substituant le mot « *associées* » au mot « *nécessaires* ».

La CNCTR a déduit de l'existence des dispositions spéciales prévues au III de l'article L. 852-1 du code que les dispositions de l'article L. 871-2 ne pouvaient trouver à s'appliquer en matière d'interception de sécurité. De la même façon et d'une manière plus générale, elle a considéré que l'existence d'un cadre juridique propre aux accès aux données de connexion, prévu aux articles L. 851-1 et suivants du code, privait d'utilité le recours à l'article L. 871-2 en matière de police administrative.

Pour respecter l'esprit de la loi du 24 juillet 2015 qui, pour assurer une meilleure protection des libertés individuelles, soumet à un avis préalable de la CNCTR les autorisations d'accès aux données de connexion, la commission a recommandé au Premier ministre de ne plus recourir aux dispositions de l'article L. 871-2 du code de la sécurité intérieure, qui ne prévoient pas cet avis préalable.

Par une note du 20 mai 2016, le Premier ministre a décidé de suivre la recommandation de la CNCTR et fait savoir aux services de renseignement qu'aucune autorisation de mise en œuvre de l'article L. 871-2 du code ne serait accordée à l'avenir en matière de police administrative.

4.5. Un dispositif particulier pour protéger les « lanceurs d'alerte »

Pour garantir, sans menacer le secret de la défense nationale, 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 sont transmis, de faire usage le cas échéant de ses pouvoirs de contrôle, en particulier *a posteriori*, et d'adresser au Gouvernement toutes recommandations ou observations nécessaires pour faire cesser la violation constatée, voire de saisir le Conseil d'État en application de l'article L. 833-8 du code de la sécurité intérieure[54].

Par ailleurs, lorsque la violation en cause est susceptible de constituer une infraction, la CNCTR saisit le procureur de la République. Tous les éléments portés à la connaissance de la commission sont alors adressés à la Commission consultative du secret de la défense nationale, qui rend un avis au Premier ministre sur la possibilité de déclassifier tout ou partie des éléments couverts par le secret de la défense nationale en vue de leur transmission au procureur.

Afin de protéger les agents ayant alerté de bonne foi la CNCTR, le II de l'article L. 861-3 du code de la sécurité intérieure défend de les sanctionner ou de prendre à leur encontre des mesures discriminatoires. Les termes de la loi en la matière sont similaires à ceux des autres dispositifs applicables aux « lanceurs d'alerte »[55].

À la date de publication du présent rapport, la CNCTR n'a pas été saisie sur le fondement de l'article L. 861-3 du code de la sécurité intérieure. ◘

54 - Voir, pour une analyse de cette faculté de recours, le point 5.2 du présent rapport.

55 - Voir notamment l'article L. 1351-1 du code de la santé publique ou les articles 6 *bis*, 6 *ter* A, 6 *ter* et 6 *quinquies* de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

5e partie

Les voies de recours à l'égard de la mise en œuvre des techniques de renseignement

Les voies de recours à l'égard de la mise en œuvre des techniques de renseignement

Le droit d'exercer un recours devant une juridiction, y compris en matière administrative, revêt un caractère constitutionnel depuis que le Conseil constitutionnel a jugé qu'il découlait de l'article 16 de la Déclaration des droits de l'homme et du citoyen de 1789 « *qu'en principe il ne doit pas être porté d'atteintes substantielles au droit des personnes intéressées d'exercer un recours effectif devant une juridiction* » (voir notamment le considérant n° 83 de la décision n° 96-373 DC du 9 avril 1996).

Un droit similaire a été reconnu par la Cour européenne des droits de l'homme, qui a jugé que « *le droit d'accès [au juge] constitue un élément inhérent au droit qu'énonce* » le paragraphe 1 de l'article 6 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales (voir notamment le paragraphe n° 36 de l'arrêt n° 4451/70 du 21 février 1975, affaire Golder contre Royaume-Uni).

En conséquence, les lois du 24 juillet et du 30 novembre 2015 ont institué des voies de recours spéciales permettant de faire vérifier par le juge administratif qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à l'égard d'une personne.

L'existence de telles voies de recours doit toutefois être conciliée avec la protection du secret de la défense nationale, conformément à la jurisprudence du Conseil constitutionnel qui a jugé que « *tant le principe de la séparation des pouvoirs que l'existence d'autres exigences constitutionnelles (...) imposent [au législateur] d'assurer une conciliation qui ne soit pas déséquilibrée entre le droit des personnes intéressées à exercer un recours juridictionnel effectif, le droit à un procès équitable ainsi que la recherche des auteurs d'infractions et les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation* », dont participe

le secret de la défense nationale (voir les considérants n° 20 et n° 22 de la décision n° 2011-192 QPC du 10 novembre 2011). De même, la Cour européenne des droits de l'homme a affirmé que « *les intérêts de la sécurité nationale (...) doivent être mis en balance avec le droit général à une procédure contradictoire* » (voir notamment le paragraphe n° 187 de l'arrêt n° 26839/05 du 18 mai 2010, affaire Kennedy contre Royaume-Uni).

5.1. Les recours exercés par les particuliers

5.1.1. La procédure préalable de réclamation devant la CNCTR

La CNCTR peut être saisie par toute personne souhaitant vérifier qu'aucune technique de renseignement n'est ou n'a été irrégulièrement mise en œuvre à son égard, selon l'article L. 833-4 du code de la sécurité intérieure ou, s'agissant de la surveillance des communications électroniques internationales, l'article L. 854-9 de ce même code.

Le pouvoir de vérification confié par la loi à la CNCTR porte sur les seules techniques de renseignement prévues au titre V du livre VIII du code de la sécurité intérieure, à savoir des techniques mises en œuvre par des services de renseignement pour des finalités de police administrative. La commission ne peut donc connaître des mesures de surveillance ordonnées par l'autorité judiciaire, qui relèvent du contrôle de cette seule autorité. Par ailleurs, la mise en œuvre de mesures de surveillances illégales par une personne privée constitue un délit qui ne ressortit également qu'à la seule autorité judiciaire.

La CNCTR ne peut être saisie par voie électronique, pour des motifs de sécurité nationale, en vertu du 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. Les réclamations ne peuvent donc être valablement adressées à la commission que par lettre.

L'instruction des réclamations ne débute que lorsque la commission dispose de tous les éléments permettant de procéder aux vérifications. L'auteur de la saisine doit justifier de son identité. Il lui est en outre recommandé, lorsqu'il invoque la mise en œuvre d'une technique consistant à surveiller des modes de communication électroniques, d'indiquer les numéros et éléments identifiants à partir desquels il souhaite que soit conduit le contrôle. Il doit alors établir, par les pièces justificatives correspondantes, qu'il est bien le titulaire des lignes ou des abonnements concernés.

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

Une fois les vérifications terminées, la commission se borne à indiquer leur achèvement à l'intéressé. Les articles L. 833-4 et L. 854-9 du code de la sécurité intérieure lui défendent en effet de confirmer ou d'infirmer la mise en œuvre d'une technique, cette information étant couverte par le secret de la défense nationale.

Toutefois, la CNCTR rappelle que, dans le cas où une technique de renseignement serait ou aurait été mise en œuvre de manière illégale, l'article L. 833-6 du code de la sécurité intérieure lui permettrait d'adresser au Premier ministre, au ministre responsable et au service de renseignement concerné une recommandation tendant à ce que cette mise en œuvre soit interrompue et les renseignements collectés détruits. Au cas où une telle recommandation ne serait pas ou insuffisamment suivie, le président ou trois membres au moins de la commission pourraient, en application de l'article L. 833-8 du code, saisir le Conseil d'État d'un recours tendant à ce que soient ordonnées l'interruption de la mise en œuvre et la destruction des renseignements collectés.

Les réclamations reçues par la CNCTR

Depuis l'entrée en vigueur du nouveau cadre légal, le nombre de réclamations est en baisse par rapport à l'époque de la CNCIS. Tandis que 110 personnes avaient saisi cette dernière en 2014 et 55 durant les neuf premiers mois de l'année 2015 pour des vérifications ne concernant que des interceptions de sécurité, la CNCTR a reçu 51 réclamations pendant sa première année d'exercice, du 3 octobre 2015 au 2 octobre 2016.

5.1.2. Le recours contentieux devant le Conseil d'État

Dans l'ancien cadre légal, la mise en œuvre de techniques de renseignement ne pouvait être contestée que dans les conditions de droit commun devant le juge administratif ou le juge pénal, auxquels pouvait être opposé le secret de la défense nationale, sous réserve d'une déclassification décidée par le ministre compétent après avis de la Commission consultative du secret de la défense nationale, en application des articles L. 2312-1 et suivants du code de la défense.

Pour renforcer le caractère effectif du droit au recours, les lois du 24 juillet et du 30 novembre 2015 ont institué une procédure contentieuse spéciale, prévue aux articles L. 773-1 et suivants du code de justice administrative, à savoir l'examen en premier et dernier ressort des requêtes concernant la mise en œuvre des techniques de renseignement par une formation spécialisée[56] du Conseil d'État, dont les membres et le rapporteur public sont habilités ès qualités à connaître d'informations couvertes par le secret de la défense nationale.

La formation spécialisée du Conseil d'État peut être saisie, sur le fondement de l'article L. 841-1 du code de la sécurité intérieure, par toute personne justifiant avoir préalablement exercé son droit de réclamation devant la CNCTR. Toutefois, en matière de surveillance des communications électroniques internationales, seul le président ou trois membres au moins de la commission peuvent soumettre une requête au Conseil d'État : cette limitation a été jugée conforme à la Constitution par le Conseil constitutionnel (voir le considérant n° 18 de la décision n° 2015-722 DC du 26 novembre 2015[57]).

56 - Toute requête peut toutefois être également renvoyée par cette formation devant la section ou l'assemblée du contentieux du Conseil d'État siégeant en formation restreinte.

57 - « *18. Considérant que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure ; qu'en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale ; que les dispositions des quatrième et cinquième alinéas de l'article L. 854-9 doivent être déclarées conformes à la Constitution* ».

Au cours de l'instance, le Conseil d'État peut inviter la CNCTR à produire des observations. Lorsque le secret de la défense nationale est en cause, il peut aménager le caractère contradictoire de la procédure en siégeant à huis clos, en entendant les parties séparément ou en occultant, lors de leur communication au requérant, certains passages des mémoires en défense ou des observations de la CNCTR. Pour compenser l'inégalité d'information entre les parties, inhérente à ce contentieux, le Conseil d'État peut relever d'office tout moyen à l'encontre des autorisations de mise en œuvre des techniques de renseignement.

La décision du Conseil d'État mentionne seulement l'existence ou l'absence d'illégalité. Elle peut annuler les autorisations jugées illégales et ordonner la destruction des renseignements irrégulièrement collectés. Saisi de conclusions en ce sens, le Conseil d'État peut également indemniser l'éventuel préjudice subi par un requérant.

En cas d'illégalité susceptible de constituer une infraction, le Conseil d'État en avise le procureur de la République et soumet les pièces du dossier à la Commission consultative du secret de la défense nationale pour qu'elle rende au Premier ministre un avis sur la possibilité de déclassifier certaines informations en vue de leur transmission à l'autorité judiciaire.

Depuis le 3 octobre 2015, le Conseil d'État a été saisi par neuf requérants. La CNCTR a produit ou s'apprête à produire des observations dans chaque affaire. Un recours s'est achevé par un désistement, quatre ont donné lieu à des décisions lues le 19 octobre 2016, quatre étaient encore en cours d'instance lors de la publication du présent rapport.

Trois des décisions rendues le 19 octobre 2016[58] portent sur les techniques de renseignement destinées à surveiller le territoire national. Le Conseil d'État a jugé qu'il appartenait à la formation de jugement, « *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 ont été communiqués hors la procédure contradictoire, si le requérant fait ou non l'objet d'une telle technique* » et, en cas de mise en œuvre, d'en apprécier la régularité. En

58 - Voir les décisions du Conseil d'État du 19 octobre 2016 n° 396958, n° 398354 et n° 398356.

l'espèce, le Conseil d'État a indiqué dans les trois cas que la vérification sollicitée « *[avait] été effectuée et n'appel[ait] aucune mesure de la part du Conseil d'État* ».

Dans l'une de ces trois affaires[59], le Conseil d'État a précisé le champ d'application temporel de ses vérifications et, par voie de conséquence, de celles conduites par la CNCTR en réponse aux réclamations préalables. Les techniques de renseignement concernées sont celles mises en œuvre à compter de l'entrée en vigueur de la loi du 24 juillet 2015, y compris celles dont la mise en œuvre a débuté avant cette date et a continué après (voir le point 2 de la décision). Sont donc recevables les recours « *qui se rapportent à la mise en œuvre éventuelle de techniques de renseignement postérieurement à l'entrée en vigueur, le 3 octobre 2015, de la loi du 24 juillet 2015, (...) que la décision de les mettre en œuvre ait été prise avant comme après cette date* » (voir le point 4 de la décision).

Une quatrième décision[60] porte sur la surveillance des communications électroniques internationales. Saisi par une requérante souhaitant que fût vérifié qu'aucune mesure de cette nature n'était irrégulièrement mise en œuvre à son encontre, le Conseil d'État a déclaré la requête irrecevable, en relevant que l'article L. 854-9 du code de la sécurité intérieure, qui régit de façon spéciale les recours en la matière, ne permettait qu'au président ou à trois membres de la CNCTR de présenter une requête sur son fondement. À cet égard, « *alors même que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale, ainsi que l'a jugé le Conseil constitutionnel dans sa décision n° 2015-722 DC du 26 novembre 2015* » (voir le point 1 de la décision du Conseil d'État).

59 - Voir la décision du Conseil d'État n° 396958 mentionnée dans la note précédente et reproduite en annexe 11 au présent rapport.

60 - Voir la décision du Conseil d'État du 19 octobre 2016 n°397623, reproduite en annexe 12 au présent rapport.

5.2. Les recours ouverts à la CNCTR

Outre la voie de recours contentieux ouverte aux particuliers, le livre VIII du code de la sécurité intérieure a prévu que la CNCTR puisse introduire des instances de sa propre initiative.

Lorsque le Premier ministre ne donne pas suite aux avis de la CNCTR, le président de la commission ou trois de ses membres au moins peuvent saisir le Conseil d'État d'un recours, en application de l'article L. 833-8 du code de la sécurité intérieure.

En outre, comme cela a déjà été évoqué plus haut[61], le même article prévoit que le président ou trois membres au moins de la CNCTR peuvent saisir le Conseil d'État lorsqu'ils estiment que le Premier ministre n'a pas ou insuffisamment suivi les recommandations de la commission concernant l'interruption de la mise en œuvre d'une technique ou la destruction de renseignements collectés. Un tel cas pourrait se produire dans le cadre d'une réclamation présentée par un requérant, mais aussi à la suite de contrôles *a posteriori* menés indépendamment de toute réclamation.

Par ailleurs, lorsque le Premier ministre autorise par une décision spécialement motivée, sur le fondement du III de l'article L. 853-3 du code, l'introduction dans un lieu d'habitation malgré un avis défavorable de la CNCTR, le Conseil d'État est obligatoirement et immédiatement saisi de l'affaire.

Enfin, selon l'article L. 854-9 du code de la sécurité intérieure, le président ou trois membres de la commission disposent seuls de la faculté de saisir le Conseil d'État aux fins de vérifier si une mesure de surveillance des communications électroniques internationales est régulièrement mise en œuvre à l'égard d'une personne.

À la date de publication du présent rapport, aucune instance n'a été ouverte devant le Conseil d'État en application de ces dispositions. ◘

61 - Voir les points 4.5 et 5.1.1 du présent rapport.

6e partie

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

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

La CNCTR estime qu'il lui appartient, dans le respect du secret de la défense nationale par lequel ses travaux sont couverts en application de l'article L. 832-5 du code de la sécurité intérieure, de développer un dialogue institutionnel avec le Parlement, d'échanger son expérience et ses pratiques avec des autorités de contrôle étrangères, notamment européennes, et de rendre compte au public de son activité.

6.1. Les relations entre la CNCTR et le Parlement

6.1.1. L'avis préalable des commissions parlementaires sur la nomination du président de la CNCTR

Par la loi organique n° 2015-911 du 24 juillet 2015 relative à la nomination du président de la Commission nationale de contrôle des techniques de renseignement, le législateur a décidé de soumettre cette nomination à la procédure prévue au dernier alinéa de l'article 13 de la Constitution : le Président de la République, qui dispose du pouvoir de nommer le président de la CNCTR, doit préalablement consulter les commissions permanentes du Parlement, lesquelles peuvent s'opposer à son choix si elles réunissent au moins trois cinquièmes des suffrages exprimés en leur sein. En l'espèce, ces commissions sont celles compétentes en matière de libertés publiques, conformément à la loi n° 2010-838 du 23 juillet 2010 relative à l'application du cinquième alinéa de l'article 13 de la Constitution.

Nouveauté par rapport aux conditions de nomination du président de la CNCIS, le candidat aux fonctions de président de la CNCTR a été entendu le 29 septembre 2015 par les commissions des lois de l'Assemblée nationale et du Sénat, qui ont confirmé le choix du Président de la République.

6.1.2. Un dialogue institutionnel régulier et constructif

La CNCTR répond aux demandes d'avis du président de l'Assemblée nationale, du président du Sénat et de la délégation parlementaire au renseignement, comme le prévoit l'article L. 833-11 du code de la sécurité intérieure.

Dans ce cadre, le président de la CNCTR a été entendu par la délégation parlementaire au renseignement le 5 novembre 2015 afin d'évoquer les conditions d'installation de la commission et les étapes du développement de son activité.

Par la suite, un premier bilan de l'activité de la CNCTR a pu être présenté au Parlement lorsque le président de la commission a été entendu, le 10 février 2016, par le comité de suivi de l'état d'urgence, institué par la commission des lois du Sénat, puis, le 18 mai 2016, par la commission d'enquête créée par l'Assemblée nationale, relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015.

Invité à exposer devant les sénateurs les conséquences de l'état d'urgence sur l'activité de la CNCTR, le président de la commission a rappelé que la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence prévoit, à son article 6-1 résultant de la loi n° 2015-1501 du 20 novembre 2015, une nouvelle finalité que les services de renseignement peuvent invoquer afin de demander au Premier ministre l'autorisation de recourir aux techniques de renseignement, à savoir la prévention des actions tendant au maintien ou à la reconstitution des associations ou groupements dissous en application du régime de l'état d'urgence. Par ailleurs, l'importance de la menace terroriste, qui a fondé la déclaration de l'état d'urgence, a notablement modifié, parmi les demandes de mise en œuvre des techniques, la proportion de celles fondées sur la prévention du terrorisme.

La CNCTR a en outre été saisie pour avis par le Parlement, au printemps 2016, lors de la discussion de deux propositions de loi émanant du Sénat, l'une, organique, relative aux autorités administratives indépendantes et autorités publiques indépendantes et l'autre, ordinaire, portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes.

Enfin, le présent rapport a été présenté à la délégation parlementaire au renseignement avant sa diffusion au public.

6.2. Les relations de la CNCTR avec les services de renseignement

6.2.1. L'audition des directeurs et chefs de services de renseignement

Au cours de sa première année d'activité, la CNCTR a reçu les chefs de tous les services de renseignement du premier et du second cercles ainsi que le directeur du GIC, lors de réunions en formation plénière. Il leur a été demandé de rappeler l'organisation et les missions des administrations placées sous leur autorité, puis présenter tant leur stratégie que leurs interrogations concernant l'application du nouveau cadre juridique applicable aux techniques de renseignement. En retour, la CNCTR a pu exposer ses premiers éléments de doctrine ainsi que ses exigences, notamment en matière de centralisation des informations recueillies.

6.2.2. Les rencontres régulières avec les services de renseignement

Le président de la CNCTR, accompagné d'un autre membre et d'un agent de la commission ainsi que d'un représentant du GIC, s'est rendu, outre Paris, dans les sièges de toutes les zones de défense et de sécurité métropolitaines (Lille, Rennes, Bordeaux, Marseille, Lyon, Strasbourg et Metz) ainsi qu'à

Toulouse, afin de rencontrer les directions déconcentrées des services de renseignement, d'évoquer le nouveau cadre légal et d'indiquer des solutions aux premières difficultés nées de son application. Un déplacement a également eu lieu à Fort-de-France à la fin de l'année 2015 et un autre déplacement outre-mer est prévu à La Réunion en novembre 2016.

Au niveau national, la CNCTR est en contact continu avec les services de renseignement, que ce soit par le biais d'échanges quotidiens entre ses agents et ceux des services ou lors de réunions que la commission organise ou auxquelles elle participe afin de préciser sa doctrine et traiter les questions de droit que pose l'application du livre VIII du code de la sécurité intérieure.

6.2.3. La participation aux formations des cadres des services de renseignement

La CNCTR a souhaité contribuer à l'effort de formation des agents des services de renseignement mené depuis l'entrée en vigueur du nouveau cadre légal. Aussi est-elle intervenue plusieurs fois devant les auditeurs de l'académie du renseignement, qui forme les cadres des services de renseignement.

6.3. Le partage d'expérience avec les autorités de contrôle étrangères et le dialogue avec les institutions internationales chargées de la promotion des droits fondamentaux

La CNCTR estime bénéfique de développer la coopération avec les organes de pays étrangers, en particulier européens, dont le statut et les compétences sont assimilables aux siens, ne serait-ce qu'en partie. Des rencontres bilatérales se sont ainsi tenues avec les autorités de contrôle britannique,

allemande, belge, néerlandaise et suisse depuis la création de la commission[62]. Confrontés aux mêmes menaces et aux mêmes enjeux de libertés publiques que la France, certains pays européens, tels que le Royaume-Uni et l'Allemagne ont également choisi de rénover leur législation sur le renseignement. Les rencontres avec la CNCTR ont ainsi permis de faire connaître les solutions retenues par chaque pays.

La CNCTR a par ailleurs été conviée à un colloque international organisé à Oslo le 12 avril 2016, à l'occasion du vingtième anniversaire de la commission parlementaire norvégienne chargée de contrôler l'action des services de renseignement. La CNCTR a pu y présenter les deux nouvelles lois adoptées en 2015 en France pour encadrer le recours aux techniques de renseignement.

La commission a également adressé au printemps 2016 une contribution à l'Agence de l'Union européenne pour les droits fondamentaux, afin d'actualiser l'étude comparative menée par cette dernière sur les législations relatives au renseignement au sein des États européens.

Enfin, la CNCTR a participé le 11 octobre 2016 à une rencontre internationale organisée à Bucarest par le rapporteur spécial des Nations unies sur le droit à la vie privée, cette rencontre ayant pour thème le contrôle des services de renseignement.

6.4. L'information du public

Outre la publication du présent rapport d'activité, prévue à l'article L. 833-9 du code de la sécurité intérieure, et la parution au *Journal officiel* de la République française de ses avis non couverts par le secret de la défense nationale, la CNCTR entend promouvoir la connaissance du nouveau cadre légal du renseignement auprès du public, notamment des professionnels du droit. Dans cette perspective, elle a débuté un dialogue avec le monde universitaire.

La CNCTR envisage enfin la mise en place d'un site internet sur lequel elle pourra publier ses avis et ses recommandations non couverts par le secret de la défense nationale.

62 - Voir, pour la liste des autorités de contrôle étrangères rencontrées, l'annexe 7 au présent rapport.

Annexes

Annexe n° 1

Délibération de la CNCTR n° 1/2015 du 29 octobre 2015

La Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, est d'avis de fonder la position qu'elle prendra, au cas par cas, sur les demandes de mise en œuvre d'une technique de renseignement concernant une personne mentionnée à l'article L. 821-7 du code de la sécurité intérieure[1], sur les considérations suivantes :

1. La protection de la loi bénéficie, sur le territoire national, à toute personne, quelle que soit sa nationalité qui, en France, dans son pays d'origine ou dans le cadre international, exerce l'une des professions mentionnées par la loi ou détient un mandat de même nature que celui des parlementaires français.

2. La commission se prononce au regard des informations communiquées par le service demandeur et des définitions qu'elle a adoptées. Elle se réserve la possibilité de demander, le cas échéant, des informations complémentaires.

3. Au titre du mandat de parlementaire, bénéficient de la protection de l'article L. 821-7 du code de la sécurité intérieure :

3.1. Les députés et sénateurs français ;

3.2. Les députés européens, quelle que soit leur nationalité ;

3.3. Toute personne qui, dans son pays, détient du suffrage universel direct ou indirect un mandat national ou fédéral.

---

1 - L'article L. 821-7 du code de la sécurité intérieure, créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, prévoit : « *Un parlementaire, un magistrat, un avocat ou un journaliste ne peut être l'objet d'une demande de mise en œuvre, sur le territoire national, d'une technique de recueil de renseignement mentionnée au titre V du présent livre à raison de l'exercice de son mandat ou de sa profession. Lorsqu'une telle demande concerne l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles, l'avis de la Commission nationale de contrôle des techniques de renseignement est examiné en formation plénière. L'article L. 821-5 n'est pas applicable. / La commission est informée des modalités d'exécution des autorisations délivrées en application du présent article. / Les transcriptions des renseignements collectés en application du présent article sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats* ».

4. Sont magistrats pour l'application de l'article L. 821-7 du code de la sécurité intérieure :

4.1. Les magistrats en fonction dans une juridiction de l'ordre judiciaire français, qu'ils relèvent du siège ou du parquet ;

4.2. Les magistrats en fonction dans les juridictions de l'ordre administratif français, tribunaux administratifs et cours administratives d'appel ;

4.3 Les membres du Conseil d'État en fonction à la section du contentieux ;

4.4. Les magistrats en fonction dans les juridictions financières françaises.

5. Sont assimilés à des magistrats pour l'application de l'article L. 821-7 du code de la sécurité intérieure :

5.1. Les membres du Conseil constitutionnel ;

5.2. Les juges de proximité, les juges consulaires, y compris ceux composant les juridictions commerciales mixtes, et les conseillers prud'homaux ;

5.3. Les juges des juridictions européennes (Cour de justice de l'Union européenne[2], Cour européenne des droits de l'homme, Cour de justice de l'Association européenne de libre-échange) ;

5.4. Les juges des juridictions internationales (Cour internationale de justice, Cour pénale internationale, Tribunal international du droit de la mer, Tribunal pénal international pour l'ex-Yougoslavie, Tribunal pénal international pour le Rwanda, Tribunal spécial pour le Liban, Tribunal spécial pour la Sierra Leone, Chambres extraordinaires au sein des tribunaux cambodgiens) ;

5.5. Les juges qui, dans leur pays ou dans un cadre international, détiennent de l'État ou d'une organisation interétatique, le pouvoir de trancher en toute indépendance des différends ou de prononcer des sanctions par des décisions exécutoires au moyen de la force publique.

2 - La Cour de justice de l'Union européenne comprend, au 29 octobre 2015, la cour de justice, le tribunal et le tribunal de la fonction publique.

6. Sont avocats pour l'application de l'article L. 821-7 du code de la sécurité intérieure :

6.1. Les avocats français inscrits au barreau d'un tribunal de grande instance français et les avocats ressortissants d'un autre pays de l'Union européenne inscrits à un barreau français en application de la directive 89/48/CEE du Conseil du 21 décembre 1988 relative à un système général de reconnaissance des diplômes d'enseignement supérieur qui sanctionnent des formations professionnelles d'une durée minimale de trois ans ;

6.2. Les avocats membres de l'ordre des avocats au Conseil d'État et à la Cour de cassation ;

6.3. Les avocats non français ressortissants européens qui sont inscrits sur la liste spéciale d'un barreau français et exercent en France sous leur titre professionnel d'origine en application de la directive 98/5/CE du Parlement européen et du Conseil du 16 février 1998 visant à faciliter l'exercice permanent de la profession d'avocat dans un État membre autre que celui où la qualification a été acquise ;

6.4. Les personnes, quel que soit leur titre, qui, au bénéfice d'une qualification reconnue, tiennent de la loi le pouvoir de représenter une personne devant une juridiction instituée par un État et sont astreints à des obligations professionnelles et déontologiques.

7. Est journaliste, pour l'application de l'article L. 821-7 du code de la sécurité intérieure, toute personne, de nationalité française ou étrangère, qui, exerçant sa profession dans une ou plusieurs entreprises de presse ou d'édition, de communication au public en ligne, de communication audiovisuelle ou auprès d'une ou de plusieurs agences de presse, en France ou à l'étranger, y pratique, à titre régulier et rétribué, le recueil d'informations et leur diffusion au public.

Annexe n° 2

Délibération de la CNCTR n° 2/2015 du 12 novembre 2015

Saisie pour avis par le ministre de l'intérieur d'un projet de décret 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, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

1) Remarques de portée générale

La loi n° 2015-912 du 24 juillet 2015 relative au renseignement a ouvert aux six services spécialisés de renseignement, désignés par le décret n°2015-1185 du 28 septembre 2015, la possibilité de recourir, pour le seul exercice de leurs missions et pour les finalités limitativement fixées par l'article L. 811-3 du code de la sécurité intérieure (CSI), à des techniques de renseignement mentionnées au titre V du livre VIII du CSI. Le recours à ces techniques est strictement encadré par la loi : il est autorisé par le Premier ministre après avis de la CNCTR. La CNCTR s'assure que les techniques de renseignement sont légalement autorisées puis mises en œuvre. Elle opère à cette fin un contrôle *a priori* sur les demandes et *a posteriori* sur l'exécution de la technique.

La loi du 24 juillet 2015, codifiée sur ce point à l'article L. 811-4 du CSI, a également prévu qu'un décret en Conseil d'État, pris après avis de la CNCTR, désigne les services, autres que les services spécialisés de renseignement, — communément appelés « services du second cercle », par opposition au « premier cercle » qui est celui des six services spécialisés — qui peuvent

recourir, pour des finalités prévues par l'article L. 811-3 du CSI, à certaines des techniques de renseignement mentionnées au titre V du livre VIII du CSI. C'est l'objet du projet du décret dont la CNCTR est saisie pour avis et qui ne concerne que des services relevant du ministre de l'intérieur.

- La CNCTR déduit de la loi du 24 juillet 2015 que les services spécialisés du « premier cercle » ont vocation, dans le cadre de leurs missions, à avoir recours à toute la gamme des techniques de renseignement prévues par cette loi, sous réserve que celles-ci correspondent à l'une des finalités prévues par l'article L. 811-3 du CSI et qu'elles soient proportionnées à l'objectif poursuivi. Il en est différemment pour les services du « second cercle » qui n'ont pas tous une vocation exclusive de recherche de renseignement et ne disposent pas toujours de l'expertise technique requise pour mettre en œuvre de manière sûre les techniques de renseignement les plus intrusives. La CNCTR en conclut que les techniques les plus intrusives, qui passent par une pénétration dans un lieu d'habitation, ne peuvent être accessibles qu'aux services du « second cercle » se consacrant exclusivement au renseignement et justifiant d'un besoin avéré et d'une expertise spécifique pour y recourir.

- D'une manière générale, la CNCTR estime qu'il convient de moduler l'accès des services du « second cercle » aux techniques de renseignement selon la catégorie à laquelle ils appartiennent :

  - Accès le plus étendu pour les services spécialisés de renseignement (SCRT, DRPP, SDAO) ;
  - Accès moins étendu pour les services de police judiciaire (DCPJ, DPJPP, SDPJ et SR) qui peuvent mettre en œuvre des techniques équivalentes dans le cadre d'une procédure judiciaire;
  - Accès restreint pour les services territoriaux généralistes (SD, ST et services d'investigation de la DCPAF).

- La loi autorise le recours aux *IMSI catchers* pour l'accès à des données de connexion (L. 851-6) et, dans des conditions restrictives, pour intercepter des correspondances (II de l'article L. 852-1). La CNCTR estime que l'utilisation de ces appareils pour intercepter des

correspondances doit être strictement réservée à des services spécialisés en matière de renseignement. Pour les services de police judiciaire, c'est dans le cadre judiciaire que cette technique a vocation à être mise en œuvre, moyennant d'éventuelles adaptations au code de procédure pénale.

- La CNCTR observe par ailleurs que l'article L. 811-4 du CSI, dont le projet de décret fait application, prévoit que ce décret a pour objet de désigner les services « *qui peuvent être autorisés à recourir aux techniques* » mentionnées au titre V du livre VIII du CSI. Elle estime que cette rédaction permet au service auteur de la demande soit d'assurer lui-même la mise en œuvre effective de la technique, s'il en a la capacité, soit de faire réaliser l'opération par un opérateur[1] relevant de ce service ou de la direction de rattachement du service, techniquement mieux à même de la mener à bien. La CNTR souhaite même que les opérations les plus délicates soient réalisées par un opérateur technique spécialisé disposant de l'expérience et des compétences requises. Les agents du service opérateur devront être individuellement désignés et habilités à mettre en œuvre la technique de renseignement, dans les conditions prévues par l'article L. 853-3, si cette technique implique la pénétration dans un véhicule ou un lieu privé.

- L'article 1er de la loi du 24 juillet 2015, codifié à l'article L. 801-1 du CSI, prévoit qu'il ne peut être porté atteinte au respect de la vie privée, dans toutes ses composantes, que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. Il impose ainsi que la capacité d'avoir recours à des techniques de renseignement soit strictement et précisément limitée aux services qui ont légalement mission de recourir à des actions de prévention relevant de la police administrative. De l'avis de la CNCTR, il exclut que cette capacité soit, sans discrimination, donnée à l'ensemble d'une direction non spécialisée en matière de renseignement, dont une partie des services seulement répondent à cette exigence.

1 - Par exemple le GIGN pour la gendarmerie, le SIAT pour la police.

- La CNCTR souligne enfin que l'effectivité de la mission de contrôle qui lui est confiée par la loi nécessite qu'elle puisse, au-delà du contrôle *a priori*, mener à bien un contrôle *a posteriori* sur les données de renseignement recueillies. L'exercice effectif de ce contrôle *a posteriori* impose une centralisation des données recueillies auxquelles la CNCTR doit avoir un accès libre et permanent. Pour les « services du second cercle », cette centralisation devrait, de son point de vue, de préférence être réalisée par le GIC qui assure déjà, pour tous les services, spécialisés ou non, la centralisation des données recueillies par les interceptions de sécurité. 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 nationale (DGGN) et la préfecture de police (PP). La CNCTR appelle l'attention du Gouvernement sur l'urgence de la mise en œuvre de cette centralisation qui impliquera l'élaboration d'infrastructures et de réseaux de communication robustes et répondant aux exigences de sécurité requises pour le stockage et le transport des données de renseignement.

2) Observations détaillées

Pour la lisibilité de son avis, la CNCTR livrera ses commentaires pour chaque service demandeur, sans suivre l'ordre des articles du projet de décret.

2.1) Services de la direction générale de la police nationale (DGPN)

2.1.1) La direction centrale de la police judiciaire (DCPJ)

Observation liminaire : Le projet prévoit en l'état d'autoriser la DCPJ à recourir à des techniques de renseignement pour certaines finalités, sans autre précision sur les services centraux ou territoriaux concernés. Cette proposition, insuffisamment définie dans son champ d'application, qui concerne une direction dont la mission principale est la police judiciaire, ne pourrait que se heurter à un avis défavorable de la CNCTR. Le ministère de

l'intérieur a cependant communiqué informellement à la CNCTR une proposition modifiée qui précise les services centraux et les services territoriaux concernés. Il s'agit, au niveau central, des sous-directions ou services suivants :

- Sous-direction de la lutte contre la criminalité organisée et la délinquance financière (SDLCODF),
- Sous-direction anti-terroriste (SDAT),
- Sous-direction de la lutte contre la cybercriminalité (SDLC),
- Service central des courses et des jeux (SCCJ).

Au niveau territorial, il s'agit des onze directions interrégionales ou régionales de la police judiciaire (DIPJ/DRPJ) et des huit services régionaux de police judiciaire (SRPJ).

C'est sur le fondement de ces indications que la CNCTR rend son avis.

Finalités[2] : Les deux finalités invoquées (4 et 6) n'appellent pas d'objections de la part de la CNCTR. Elles doivent cependant être précisées pour chacun des sous-directions et services habilités :

- SDLCODF : finalité 6,
- SDAT : finalité 4,
- SDLC : finalité 4 et 6,
- SCCJ : finalité 6,
- Services territoriaux : finalités 4 et 6.

2 - Liste des finalités énumérées par l'article L. 811-3 du CSI :

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

Techniques : Le recours proposé à l'accès aux données de connexion en temps différé (L. 851-1 du CSI), à la géolocalisation en temps réel (L. 851-4) et aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) peut, de l'avis de la CNCTR, être ouvert à tous les services centraux et territoriaux ci-dessus mentionnés. La CNCTR admet que soit autorisé pour ces mêmes services le recours à la technique du balisage (L. 851-5) mis en œuvre sur la voie publique ou dans un lieu privé, hors locaux d'habitation. L'utilisation d'*IMSI catchers* pour recueillir des données de connexion (L. 851-6) peut être admise par la CNCTR à condition que la mise en œuvre soit réalisée par le SIAT, qui dispose de la compétence technique nécessaire. La captation d'images et de son demandée (L. 853-1) peut être admise à la condition qu'elle s'effectue sans pénétration dans un lieu d'habitation. La CNCTR n'est pas favorable à ce que les services centraux ou territoriaux de la DCPJ puissent, dans un cadre de police administrative, avoir recours au recueil et à la captation de données informatiques (L. 853-2) et à la possibilité de s'introduire dans un lieu d'habitation (L. 853-3). Elle est également défavorable à ce que soit ouverte à ces services de police judiciaire, la possibilité d'interception, dans un cadre de police administrative, des correspondances par un *IMSI catcher* (II de L. 852-1).

2.1.2) Unité de coordination de la lutte contre le terrorisme (UCLAT)

Selon l'arrêté du 8 octobre 1984, l'UCLAT est chargée d'une mission de coordination, d'animation et d'orientation des directions et services actifs de police en matière de lutte contre le terrorisme. Elle n'a pas de rôle opérationnel justifiant que lui soit donné accès à des techniques de renseignement. La CNCTR émet donc un avis défavorable à la proposition de lui donner un accès aux données de connexion (L. 851-1). Elle estime que cet accès, dont l'UCLAT dispose aujourd'hui, n'est pas justifié et doit donc être supprimé.

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

L'accès à des techniques de renseignement est demandé pour l'office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre (OCRIEST) et pour les services d'investigation de la direction.

2.1.3.1) OCRIEST

Créé par le décret n° 96-691 du 6 août 1996, au sein de la DCPAF, l'OCRIEST exerce à titre principal une mission de police judiciaire en matière de lutte contre l'immigration irrégulière, les filières clandestines et l'emploi d'étrangers sans titre. Il est également chargé d'une mission de prévention. Cette mission se rattache à la police administrative, peut à ce titre justifier le recours à certaines techniques de renseignement et permet à l'OCRIEST de préparer la « judiciarisation » de certaines affaires.

Finalités : La finalité 6 invoquée n'appelle pas d'observations.

Techniques : L'accès aux données de connexion (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1), techniques déjà accessibles à l'OCRIEST, n'appelle pas d'observations. L'accès au balisage (L. 851-5), qui, selon les indications communiquées à la CNCTR par l'OCRIEST, serait exclusivement réalisé sur la voie publique, n'en appelle pas davantage. La CNCTR pourrait cependant admettre que la pose de balises soit effectuée dans des lieux privés autres que des lieux d'habitation. L'utilisation d'*IMSI catchers* pour recueillir des données de connexion (L. 851-6) peut être admise par la CNCTR à condition que la mise en œuvre soit réalisée par le SIAT, qui dispose de la compétence technique nécessaire. La captation d'images et de son demandée (L. 853-1) peut être admise à la condition qu'elle s'effectue sans pénétration dans un lieu d'habitation. La CNCTR n'est pas favorable à ce que l'OCRIEST, qui est un service de police judiciaire, puisse, dans un cadre de police administrative, avoir recours au recueil et à la captation de données informatiques (L. 853-2) et à la possibilité de s'introduire dans un lieu d'habitation (L. 853-3).

2.1.3.2) Services d'investigation

Les services concernés sont les unités chargées de la police judiciaire au sein des directions déconcentrées de la police aux frontières et des directions de la police aux frontières d'Orly et de Roissy, les brigades mobiles de recherche (49) et l'unité judiciaire du service national de la police ferroviaire de la DCPAF.

La DCPAF met en place une procédure de « guichet unique » qui fera transiter toutes les demandes des services déconcentrés par l'OCRIEST qui en examinera le bien-fondé technique et la pertinence avant de les transmettre au directeur de la DCPAF. Cette procédure de contrôle interne est bienvenue eu égard au nombre et à la dispersion des unités demanderesses.

La CNCTR estime que les services d'investigation sus-évoqués peuvent avoir recours, pour la finalité 6, au balisage (L. 851-5) à la condition qu'il soit réalisé exclusivement sur la voie publique et par du personnel qualifié. Elle admet qu'ils aient accès aux données de connexion en temps différé (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I du L. 852-1). Elle n'est pas favorable à la possibilité demandée d'introduction dans un véhicule ou un lieu privé (L. 853-3), qui doit à son avis, être réservée à l'OCRIEST.

2.1.4) Direction centrale de la sécurité publique (DCSP)

L'accès à certaines techniques de renseignement est demandé pour les services du renseignement territorial et les sûretés départementales.

2.1.4.1) Services du renseignement territorial

Créé par un arrêté du 1er février 2011, le service central du renseignement territorial (SCRT), qui fait partie de la DCSP, a un échelon central d'environ 150 personnes et des services déconcentrés dans le cadre des zones de défense et des départements, à l'exception de la zone de défense de Paris et des quatre départements de cette zone de défense (qui relèvent de la préfecture de police). Il a une mission exclusive de renseignement destinée à compléter, au niveau territorial, celle de la DGSI.

Finalités : Les finalités invoquées 4, 5 et 6 ne soulèvent pas d'observations eu égard aux missions des services concernés. La CNCTR admet également la finalité 1, invoquée pour la mise en œuvre d'une partie des techniques, qui pourrait fonder la prévention de l'atteinte à des infrastructures d'importance vitale.

Techniques : Une division du SCRT (division D7) sera le guichet unique d'entrée de toutes les demandes de techniques de renseignement du service.

Cette organisation, que la CNCTR juge bienvenue, permettra d'assurer le contrôle et la coordination des demandes émanant de l'ensemble du territoire et d'organiser de manière rationnelle et sûre la mise en œuvre des techniques par un opérateur disposant des compétences requises. Eu égard, d'une part, à la mission exclusive de renseignement assurée par l'échelon central et par les services territoriaux et, d'autre part, à l'organisation interne ci-dessus mentionnée, la CNCTR n'a pas d'objections sur le recours demandé à l'accès aux données de connexion en temps différé (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) et au balisage (L. 851-5) mis en œuvre sur la voie publique ou dans un lieu privé. Elle admet l'utilisation d'*IMSI catchers* pour intercepter les données de connexion (L. 851-6). Elle admet également la sonorisation et la captation d'images dans un lieu privé (L.853-1), le recueil et la captation de données informatiques (L. 853-2). S'agissant de la possibilité de pénétration dans un lieu d'habitation, la CNCTR admet qu'elle soit ouverte exclusivement au service central du renseignement territorial (SCRT), au titre de la seule finalité 4 (prévention du terrorisme) eu égard au rôle particulier joué par ce service en matière de lutte contre le terrorisme. Elle peut admettre, avec la même restriction s'appliquant à la finalité 4 et au SCRT, l'utilisation d'*IMSI catchers* destinés à intercepter des correspondances (II de L. 852-1).

2.1.4.2) Sûretés départementales (SD)

Eu égard aux missions des sûretés départementales qui sont, pour l'essentiel, de police judiciaire et qui visent à lutter, au niveau local, contre la moyenne et la petite délinquance, et compte-tenu des missions spécifiques de renseignement remplies, au sein de la même direction et sur les mêmes territoires par le SCRT, la CNCTR estime, compte tenu des besoins opérationnels de la prévention de la délinquance que les SD puissent avoir recours au balisage (L. 851-5), à condition qu'il soit réalisé exclusivement sur la voie publique et par du personnel qualifié. La CNCTR admet que les SD aient, pour la finalité 6, accès aux données de connexion en temps différé (L. 851-1), aux géolocalisations en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1). Elle n'est pas favorable à l'accès à la technique de sonorisation et de captation d'images (L. 853-1) qui doit, de son point de vue, être réservé aux services du renseignement territorial.

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

2.2.1) Sous-direction de l'anticipation opérationnelle (SDAO)

Créée par un arrêté du 6 décembre 2013, la SDAO exerce une compétence exclusive de prévention des menaces dans les domaines de la défense, de l'ordre public et de la sécurité nationale. Elle contribue à la mise en œuvre de la mission de renseignement fixée à la gendarmerie par l'article L. 421-1 du CSI.

Finalités : Les finalités 1, 4 et 5 proposées n'appellent pas d'observations.

Techniques : L'accès aux données de connexion en temps différé (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) et au balisage (L. 851-5) mis en œuvre sur la voie publique ou dans un lieu privé n'appellent pas d'observations. La CNCTR admet l'utilisation d'*IMSI catchers* pour intercepter les données de connexion (L. 851-6). Elle admet également la sonorisation et la captation d'images dans un lieu privé, et le recueil et la captation de données informatiques. S'agissant de la possibilité de pénétration dans un lieu d'habitation, la CNCTR admet qu'elle soit ouverte à la SDAO, au titre de la seule finalité 4. Elle peut admettre, avec la même restriction à la finalité 4, l'utilisation d'*IMSI catchers* destinés à intercepter des correspondances (II de L. 852-1).

2.2.2) Sous-direction de la police judiciaire (SDPJ)

La vocation de la SDPJ est essentiellement de police judiciaire. Ce n'est qu'à titre accessoire qu'elle exerce une mission de prévention relevant de la police administrative.

Finalités : Les finalités 1, 4 et 6 invoquées n'appellent pas d'observations.

Techniques : L'accès aux données de connexion en temps différé (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) et au balisage (L. 851-5) mis en œuvre sur la voie publique ou dans un lieu privé (hors lieux d'habitation) n'appellent pas d'observations. La CNCTR admet l'utilisation d'*IMSI catchers* pour intercepter les données de connexion (L. 851-6). Elle n'est en revanche pas favorable à ce que la SDPJ, qui est un service de police judiciaire, puisse, dans

un cadre de police administrative, avoir recours au recueil et à la captation de données informatiques (L. 853-2) et à la possibilité de s'introduire dans un lieu d'habitation (L. 853-3). Pour les motifs exprimés dans ses observations générales, elle est défavorable à l'utilisation d'*IMSI catchers* destinés à intercepter des correspondances (II de L. 852-1). Elle estime que l'accès à la technique de sonorisation et de captation d'images demandée (L. 853-1) peut être admise si elle ne requiert pas la pénétration dans un lieu d'habitation.

2.2.3) Sections de recherches de gendarmerie spécialisées

Destinées à contribuer à la protection des bases de défense maritimes et aériennes et 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. Eu égard aux enjeux de sécurité nationale de leur mission, la CNCTR estime justifié de leur accorder un accès à certaines techniques de renseignement.

Finalités : Les finalités 1, 4 et 6 invoquées n'appellent pas d'observations.

Techniques : L'accès aux données de connexion en temps différé (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) et au balisage (L. 851-5) mis en œuvre sur la voie publique ou dans un lieu privé (hors lieux d'habitation) n'appellent pas d'observations. La CNCTR admet l'utilisation d'*IMSI catchers* pour intercepter les données de connexion (L. 851-6), à la condition que cette technique soit mise en œuvre par un opérateur disposant des qualifications requises. Elle estime que l'accès à la technique de sonorisation et de captation d'images demandée (L. 853-1) peut être admise si elle ne requiert pas la pénétration dans un lieu d'habitation. Elle est défavorable au recueil et à la captation de données informatiques (L. 853-2), cet accès devant, au sein de la gendarmerie, être réservé au SDAO, dans les conditions fixées ci-dessus. Elle est également défavorable à l'utilisation d'*IMSI catchers* destinés à intercepter des correspondances (II de L. 852-1).

2.2.4) Sections de recherche de la gendarmerie (SR)

Un effort particulier de centralisation et de sécurisation du dispositif territorial est proposé par la gendarmerie pour la formulation des demandes, leur contrôle et leur mise en œuvre par un opérateur technique de haute compétence.

Finalités : Les finalités 4 et 6 invoquées n'appellent pas d'observations.

Techniques : L'accès aux données de connexion en temps différé (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) au balisage (L. 851-5), mis en œuvre sur la voie publique ou dans un lieu privé (hors lieu d'habitation), n'appellent pas d'observations. La CNCTR admet l'utilisation d'*IMSI catchers* pour intercepter les données de connexion (L. 851-6). Pour les motifs exprimés dans ses observations générales, elle est défavorable à l'utilisation d'*IMSI catchers* destinés à intercepter des correspondances (II de L. 852-1). La CNCTR estime que l'accès à la technique de sonorisation et de captation d'images demandée (L. 853-1) peut être admise si elle ne requiert pas la pénétration dans un lieu d'habitation. Elle n'est pas favorable à ce que les SR, qui sont des services de police judiciaire, puissent, dans un cadre de police administrative, avoir recours au recueil et à la captation de données informatiques (L. 853-2) et à la possibilité de s'introduire dans un lieu d'habitation (L. 853-3).

2.3) Services de la préfecture de police (PP)

La préfecture de police exerce à Paris et dans les trois départements de la « petite couronne » (Hauts de Seine, Seine Saint-Denis, Val de Marne), les compétences de la DGPN.

2.3.1) Direction du renseignement de la préfecture de police (DRPP)

La DRPP exerce, sous l'autorité du préfet de police, une mission de renseignement. L'accès à certaines techniques de renseignement est proposé pour deux services de la DRPP, le service du renseignement intérieur et le service du renseignement territorial. Les mêmes finalités et les mêmes techniques sont, dans les deux cas, proposées.

Finalités : Les finalités proposées 4, 5 et 6 n'appellent pas d'observations. La CNCTR admet également la finalité 1 qui pourrait être invoquée, pour le recours à certaines techniques de renseignement demandées, notamment pour prévenir l'atteinte à des infrastructures d'importance vitale.

Techniques : Eu égard à la mission exclusive de renseignement assurée par les deux services, la CNCTR n'a pas d'objections sur le recours demandé à l'accès aux données de connexion en temps différé (L. 851-1), à la géolocalisation en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) et au balisage (L. 851-5) mis en œuvre sur la voie publique ou dans un lieu privé. Elle admet l'utilisation d'*IMSI catchers* pour intercepter les données de connexion (L. 851-6). Elle admet également la sonorisation et la captation d'images dans un lieu privé, et le recueil et la captation de données informatiques. S'agissant de la possibilité de pénétration dans un lieu d'habitation, la CNCTR admet qu'elle soit ouverte exclusivement au service du renseignement intérieur de la DRPP, au titre de la seule finalité 4 (prévention du terrorisme), eu égard au rôle particulier joué par ce service en matière de lutte contre le terrorisme. Elle peut également admettre, avec la même restriction à la finalité 4 et au seul service du renseignement intérieur, l'utilisation d'*IMSI catchers* destinés à intercepter des correspondances (II de L. 852-1).

2.3.2) Direction régionale de la police judiciaire (DPJPP)

Observation liminaire : Le projet prévoit en l'état d'autoriser la DPJPP à recourir à des techniques de renseignement pour certaines finalités, sans autre précision sur les services concernés. Cette proposition, insuffisamment définie dans son champ d'application, qui concerne une direction dont la mission principale est la police judiciaire, ne peut en l'état que se heurter à un avis défavorable de la CNCTR.

Il appartient au Gouvernement de définir précisément les services de la DPJPP habilités à recourir aux techniques de renseignement. La CNCTR estime que cette habilitation ne pourra s'appliquer qu'à des entités de la direction, précisément identifiées, qui ont une vocation opérationnelle, exercent une mission de prévention se rattachant à la police administrative

et aux finalités énoncées par la loi et qui peuvent justifier d'un besoin en matière de techniques de renseignement. Devra être prise en compte, pour chaque technique, la capacité de l'entité à la mettre en œuvre dans des conditions en garantissant la maîtrise technique et juridique ou la nécessité de recourir à un opérateur de la préfecture de police disposant des compétences nécessaires. La référence faite à cet égard, dans le projet de décret, à la direction opérationnelle des services techniques et logistiques (DOSTL) de la préfecture de police, devra être précisée par référence à une entité spécifique de cette direction, compétente pour la mission opérationnelle envisagée.

Finalités : Sous réserve de l'observation liminaire, les deux finalités invoquées (4 et 6) n'appelleraient pas d'objections de la part de la CNCTR. Elles doivent cependant être précisées pour chacune des sous-directions de la DPJPP :

- Sous-direction des brigades centrales : finalités 4 et 6,
- Sous-direction des affaires économiques et financières : finalité 6,
- Sous-direction des services territoriaux : finalités 4 et 6.

Techniques : Le recours à l'accès aux données de connexion en temps différé (L. 851-1 du CSI), à la géolocalisation en temps réel (L. 851-4) et aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1) peut, de l'avis de la CNCTR, être ouvert à tous les services de la DPJPP ci-dessus mentionnés. La CNCTR admet que soit autorisé pour ces mêmes services le recours à la technique du balisage (L. 851-5) mis en œuvre sur la voie publique ou dans un lieu privé, hors locaux d'habitation. L'utilisation d'*IMSI catchers* pour recueillir des données de connexion (L. 851-6) peut être admise par la CNCTR. La captation d'images et de son (L. 853-1) peut également être admise à la condition qu'elle s'effectue sans pénétration dans un lieu d'habitation. La CNCTR n'est pas favorable à ce que les services de la DPJPP puissent, dans un cadre de police administrative, avoir recours au recueil et à la captation de données informatiques (L. 853-2) et à la possibilité de s'introduire dans un lieu d'habitation (L. 853-3). Elle est également défavorable à ce que soit ouverte à ces services de police judiciaire, la possibilité d'interception, dans un cadre de police administrative, des correspondances par un *IMSI catcher* (II de L. 852-1).

2.3.3) Direction de la sécurité de proximité de l'agglomération parisienne (DSPAP)

La DSPAP exerce dans Paris et la « petite couronne » les compétences qu'exercent sur le reste du territoire la DCSP. Le projet de décret prévoit d'autoriser les quatre sûretés territoriales (ST) rattachées à la DSPAP à recourir aux mêmes techniques de renseignement que celles proposées pour les sûretés départementales et pour les mêmes finalités.

Eu égard aux missions des sûretés territoriales, identiques à celles des sûretés départementales dans le reste du territoire, qui sont, pour l'essentiel, de police judiciaire et qui visent à lutter contre la moyenne et la petite délinquance, et compte-tenu des missions spécifiques de renseignement remplies, au sein de la même préfecture de police et sur les mêmes territoires, par la DRPP, la CNCTR estime que les ST peuvent avoir recours au balisage (L. 851-5), à condition qu'il soit réalisé exclusivement sur la voie publique et par du personnel qualifié. La CNCTR admet que les ST aient, pour la finalité 6, accès aux données de connexion en temps différé (L. 851-1), aux géolocalisations en temps réel (L. 851-4), aux interceptions de sécurité réalisées *via* le GIC (I de L. 852-1). Elle n'est pas favorable à l'accès à la technique de sonorisation et de captation d'images (L. 853-1) qui doit, de son point de vue, être réservé aux services de la DRPP.

Annexe n° 3

Délibération de la CNCTR n° 1/2016 du 14 janvier 2016

Saisie pour avis par le Premier ministre[1] d'un projet de décret relatif aux techniques de renseignement, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes.

I. Remarques de portée générale

La CNCTR relève que le projet de décret est pris pour l'application du livre VIII du code de la sécurité intérieure ainsi que pour celle de l'article 226-3 du code pénal.

En particulier, l'article 2 du projet précise le cadre juridique applicable aux accès administratifs aux données de connexion prévus aux articles L. 851-1, L. 851-2 et L. 851-4 du code de la sécurité intérieure.

À titre liminaire, la CNCTR souligne que les accès administratifs aux données de connexion, prévus au chapitre Ier du titre V du livre VIII du code de la sécurité intérieure, sont désormais soumis à la même procédure que les autres techniques de renseignement : leur mise en œuvre suppose une autorisation du Premier ministre accordée, sauf urgence absolue[2], après avis de la commission. Cette unification de procédure, que la Commission nationale de contrôle des interceptions de sécurité (CNCIS) avait préconisée, constitue, pour la CNCTR également, une évolution positive. Elle permettra d'éviter le risque de doctrines divergentes entre deux instances, l'accès

1 - Le secrétariat général de la défense et de la sécurité nationale (SGDSN) a adressé à la commission une saisine initiale reçue le 3 décembre 2015 et une saisine rectificative reçue le 7 janvier 2016.

2 - La procédure en urgence absolue, régie par l'article L. 821-5 du code de la sécurité intérieure, n'est toutefois pas applicable aux accès administratifs aux données de connexion prévus aux articles L. 851-2 et L. 851-3 du même code.

administratif aux données de connexion étant jusqu'à présent soumis soit à l'autorisation d'une personnalité qualifiée lorsqu'il a lieu en temps différé, soit à celle du Premier ministre après avis de la CNCIS lorsqu'il a lieu en temps réel. À compter de l'entrée en vigueur du projet de décret, le nécessaire contrôle préalable à la mise en œuvre des techniques pourra donc être pleinement assuré par la CNCTR, autorité administrative indépendante.

La CNCTR observe en outre que le titre V du livre VIII du code de la sécurité intérieure présente les techniques de renseignement selon l'atteinte qu'elles peuvent porter à la vie privée, en partant de la technique réputée la moins intrusive, en l'espèce le recueil administratif des données de connexion. Si la CNCTR considère qu'un tel recueil est effectivement moins attentatoire à la vie privée que d'autres techniques, elle rappelle que les données de connexion sont des données sensibles et que le degré d'intrusion doit être apprécié au regard du mode de recueil mis en œuvre et, partant, de la nature et de la quantité des données collectées.

Les flux de communications électroniques sont aujourd'hui tels que le recueil des données de connexion permet de connaître ou de déduire de très nombreuses informations sur les personnes visées. Prises dans leur ensemble, ces données peuvent fournir des indications sur la vie privée, comme les habitudes de la vie quotidienne, les lieux de séjours ou les déplacements. À cet égard, un recueil en temps réel augmente l'atteinte portée à la vie privée, ce pourquoi le législateur a expressément décidé, sous le contrôle du Conseil constitutionnel, de limiter, en fonction du motif invoqué, de la durée de surveillance ou de la nature des données recueillies, la possibilité d'un tel recueil, qui n'est prévu qu'aux articles L. 851-2 et L. 851-4 du code de la sécurité intérieure.

II. Observations détaillées

1. Sur la définition des données de connexion

a) La CNCTR rappelle tout d'abord que l'article L. 851-1 du code de la sécurité intérieure définit les données de connexion susceptibles d'être recueillies non seulement en application de cet article mais aussi en application des articles L. 851-2 et L. 851-3, qui s'y réfèrent. Ces données sont les « *informations ou documents traités ou conservés* » par les « *réseaux* » ou les « *services de communications électroniques* » des opérateurs de communications électroniques, des hébergeurs et des fournisseurs de services sur internet, « *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* »[3].

L'article L. 851-1 du code de la sécurité intérieure prévoit en outre qu'un décret en Conseil d'État fixe les modalités d'application de ses dispositions, après avis de la Commission nationale de l'informatique et des libertés (CNIL) et de la CNCTR.

La CNCTR estime que le décret d'application prévu à l'article L. 851-1 du code de la sécurité intérieure doit préciser la nature des données de connexion mentionnées par la loi. Elle considère, sous réserve des observations ci-dessous, que le projet de décret remplit cet objectif en créant un nouvel article R. 851-5 dans le code de la sécurité intérieure.

b) La CNCTR rappelle en outre que les données de connexion, par opposition au contenu de correspondances échangées ou d'informations consultées, désignent le « contenant », c'est-à-dire les données permettant l'acheminement d'une communication électronique[4].

---

3 - Ces formulations sont reprises de l'article L. 246-1 du code de la sécurité intérieure, créé par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019, lui-même inspiré de l'article L. 34-1-1 du code des postes et des communications électroniques, issu de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

4 - La notion de communication électronique s'entend au sens du 1° de l'article L. 32 du code des postes et des communications électroniques, à savoir « *les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique* ». Selon cette définition, une communication électronique peut consister en un échange entre deux personnes, entre une personne et une machine ou entre des machines.

Cette distinction de principe a été clairement énoncée au cours des travaux qui ont conduit à l'adoption de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement. Dès l'étude d'impact du projet de loi, le Gouvernement indiquait en effet : « *En application du nouveau régime juridique et comme cela était déjà le cas sous l'empire du régime précédent, l'accès aux données de connexion ne permet pas de connaître le contenu des échanges effectués par les personnes surveillées (...) Il ne s'agit donc que de la collecte de toutes les « traces » d'une connexion ou d'un appel, des factures détaillées dont dispose chaque abonné. Jamais l'accès au contenu d'une connexion ou d'un appel n'est permis* ».

Dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel a par ailleurs jugé que la notion de données de connexion, telle qu'elle figure à l'article L. 851-1 du code de la sécurité intérieure, « *ne peut être entendue comme comprenant le contenu de correspondances ou les informations consultées* » (considérant 55).

La CNCTR note que l'interdiction d'accéder, par le biais d'un recueil de données de connexion, au contenu des correspondances échangées ou des informations consultées est en tout état de cause garanti par la loi, en l'occurrence par l'article L. 851-7 du code de la sécurité intérieure, qui subordonne le recueil des données de connexion au respect de l'article 226-15 du code pénal[5]. La CNCTR approuve néanmoins le rappel exprès de cette exclusion de principe dans le projet de décret, qui introduit dans le code de la sécurité intérieure un nouvel article R. 851-5 définissant les données de connexion « *à l'exclusion du contenu des correspondances échangées ou des informations consultées* » ainsi qu'un nouvel article R. 851-9, aux termes duquel : « *Les informations ou documents recueillis en application du présent chapitre ne peuvent, sans l'autorisation prévue à l'article L. 852-1[6], être exploités aux fins d'accéder au contenu de correspondances échangées ou d'informations consultées* ».

5 - L'article 226-15 du code pénal réprime d'un an d'emprisonnement et de 45 000 euros d'amende l'atteinte au secret des correspondances, y compris celles empruntant la voie électronique.

6 - L'autorisation prévue à l'article L. 852-1 est celle autorisant le recueil du contenu des communications, dénommé « interception de sécurité ».

c) La CNCTR souhaite apporter des précisions sur les conséquences de cette exclusion.

Techniquement, une émission électronique se matérialise par une suite d'enveloppes protocolaires, dites « couches », incluses les unes dans les autres, dont les plus intérieures, souvent appelées « couches hautes » sont transmises telles quelles au destinataire tandis que les extérieures, souvent appelées « couches basses », sont utilisées pour l'acheminement de l'émission.

Dans le modèle de référence défini par l'Union internationale des télécommunications (UIT), dans sa recommandation X.200 portant sur l'interconnexion de systèmes ouverts[7], les couches sont numérotées de 1 à 7, la première étant la plus extérieure et la septième la plus intérieure.

Afin de distinguer, au sein des émissions, les données de connexion du contenu des communications, la CNCTR considère que les données se trouvant dans les couches 1 à 3 (physique, liaison de données et réseau) du modèle de l'UIT font partie des données de connexion puisqu'elles sont destinées aux équipements des réseaux ou produites par eux. En outre, la CNCTR constate que des données de connexion sont présentes dans les couches 4 à 7 (transport, session, présentation, application).

Examinée à la lumière de ces éléments, la liste des données de connexion figurant au I du nouvel article R. 851-5 du code de la sécurité intérieure doit être, selon la CNCTR, interprétée de la façon suivante :

- Les données mentionnées au 1°, à savoir celles que les opérateurs de communications électroniques, les hébergeurs et les fournisseurs de services sur internet doivent conserver[8], constituent des données de connexion ;

- Les données mentionnées au 2° sont celles « *permettant de localiser les équipements terminaux* » non nécessairement conservées, comme les coordonnées *GPS* d'un *smartphone* transmises automatiquement à des serveurs distants par les logiciels qu'il embarque, sans même qu'une correspondance humaine (voix,

7 - Voir notamment l'article 6 de la recommandation.

8 - Cette obligation de conservation résulte, pour les opérateurs de communications électroniques, de l'article L. 34-1 du code des postes et des communications électroniques et, pour les hébergeurs et les fournisseurs de services sur internet, de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

synchronisation de courrier électronique ou autres) soit acheminée. Les données relatives à la localisation des équipements terminaux utilisés étant expressément incluses dans les données de connexion mentionnées par la loi à l'article L. 851-1 du code de la sécurité intérieure, la CNCTR les considère comme des données de connexion.

- Les données mentionnées au 3°, à savoir celles « *relatives à l'accès des équipements terminaux aux réseaux ou aux services en ligne* », peuvent être des données techniques envoyées par un équipement terminal pour manifester son existence à un réseau ou à un service en ligne afin d'établir une connexion. Par exemple, lorsqu'un utilisateur désactive le mode avion de son *smartphone* après un atterrissage, son équipement émet des signaux afin d'accéder aux réseaux présents dans son environnement.

  Cette catégorie de données comprend également les adresses internet ou *URL*[9]. La CNCTR note que, dans sa délibération n° 2015-455 du 17 décembre 2015 portant sur le projet de décret, la CNIL a décrit les *URL* comme « *nécessaire[s] à l'acheminement d'une communication* » tout en étant « *porteuse[s] par nature des informations consultées* ». La CNCTR considère également les *URL* comme des données mixtes, qui peuvent comporter à la fois des données de connexion et des mots faisant référence au contenu de correspondances échangées ou d'informations consultées. Elle souligne que le recueil de ces données dans le cadre des accès administratifs aux données de connexion ne saurait permettre de recueillir un tel contenu. Le recueil ne peut avoir pour objet que de reconstituer, grâce aux seules parties d'*URL* pertinentes, le chemin informatique utilisé pour échanger des correspondances ou consulter des informations.

  En conséquence, la CNCTR estime que, lorsque des données de cette catégorie se trouvent dans les couches 4 à 7 du modèle de l'UIT, leur recueil ne peut être autorisé que si une analyse approfondie, conduite sous son contrôle par type de données,

9 - *Uniform resource locator.*

permet, en l'état des possibilités techniques, d'en éliminer le contenu des communications. Ainsi, en ce qui concerne les URL, seuls les éléments qui déterminent le chemin utilisé pour échanger des correspondances ou consulter des informations peuvent être recueillis, les autres éléments devant être éliminés. C'est à cette condition que la CNCTR admet le recueil d'*URL* dans le cadre d'accès administratifs aux données de connexion.

- Les données mentionnées au 4°, à savoir celles « *relatives à l'acheminement des communications électroniques par les réseaux* », permettent de reconstituer le trajet de communications découpées en paquets susceptibles d'emprunter des routes différentes en fonction de l'encombrement du trafic, de la qualité du service offert, des accords entre opérateurs ou d'autres paramètres. Elles sont, pour la CNCTR, à destination exclusive des équipements des réseaux intermédiaires traversés et constituent donc des données de connexion.

- Les données mentionnées au 5°, à savoir celles « *relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service en ligne* », incluent les *login* et mots de passe des personnes. La CNCTR estime que ces données sont exemptes de contenu de communications et constituent des données de connexion.

- Les données mentionnées au 6°, à savoir « *les caractéristiques techniques des équipements terminaux et les données de configuration de leurs logiciels* », désignent notamment des informations émises par un *smartphone* sans que son utilisateur le demande, telle celles relatives à leurs paramètres d'affichage (taille d'écran, format audio, capacités de mémoire, type de système d'exploitation, liste des applications et numéros de version, *etc.*). La CNCTR estime que ces données sont exemptes de contenu de communications et constituent des données de connexion.

La CNCTR souligne que les développements ci-dessus sur la nature des données de connexion constituent une analyse globale, empirique, non exhaustive et non définitive. Cette analyse a vocation à être approfondie, en particulier lors de la rédaction de l'arrêté tarifaire prévu au nouvel article

R. 873-2 du code de la sécurité intérieure, qui doit énumérer les prestations pouvant être demandées aux opérateurs de communications électroniques, aux hébergeurs et aux fournisseurs de services sur internet pour recueillir les données de connexion. La CNCTR révisera en outre périodiquement l'analyse en fonction des évolutions techniques. Elle demande en conséquence que les nouveaux types de données qui pourraient être regardées comme faisant partie des données de connexion fassent l'objet d'un avis de sa part avant toute autorisation de recueil, afin qu'elle puisse s'assurer qu'aucun contenu de communications ne sera collecté.

2. Sur le mode de recueil des données de connexion

a) S'agissant de l'accès administratif aux données de connexion prévu à l'article L. 851-1 du code de la sécurité intérieure, la CNCTR considère que la loi, eu égard tant à sa rédaction qu'aux travaux parlementaires qui ont précédé son adoption, n'a ni pour objet ni pour effet de permettre le recueil en temps réel des données, qui doit être expressément prévu, comme il l'est aux articles L. 851-2 et L. 851-4 du code. Le recueil autorisé sur le fondement de l'article L. 851-1 du code ne peut donc intervenir qu'en temps différé.

À cet égard, dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel, après avoir analysé les dispositions des articles L. 851-1 et L. 851-2 du code de la sécurité intérieure, a jugé « *qu'en outre, lorsque le recueil des données a lieu en temps réel, il ne pourra être autorisé que pour les besoins de la prévention du terrorisme, pour une durée de deux mois renouvelable, uniquement à l'égard d'une personne préalablement identifiée comme présentant une menace et sans le recours à la procédure d'urgence absolue prévue à l'article L. 821-5 du même code* » (considérant 56), c'est-à-dire dans les conditions prévues à l'article L. 851-2.

En conséquence, les données de connexion susceptibles d'être recueillies en application de l'article L. 851-1 du code de la sécurité intérieure ne peuvent être que des données préalablement conservées par les opérateurs de communications électroniques, les hébergeurs et les fournisseurs de services sur internet. Il s'agit, par définition, des données mentionnées au 1° du I du nouvel article R. 851-5 du code.

La CNCTR souhaite que le cadre juridique exposé ci-dessus ressorte clairement des dispositions du projet de décret. Elle note que, dans sa saisine rectificative, le Premier ministre indique garantir que « *les données de connexion traitées par les réseaux mais non conservées ne peuvent pas être recueillies dans le cadre de l'article L. 851-1* » du code de la sécurité intérieure. Cette garantie est censée être apportée par le II du nouvel article R. 851-5 du code, aux termes duquel : « *Les informations énumérées aux 2° à 6° du I ne peuvent être recueillies qu'en application des articles L. 851-2 à L. 851-6, dans les conditions et limites prévues par ces articles* ».

La CNCTR préconise une rédaction plus directe, plus complète et, partant, plus sûre. Elle propose que le II du nouvel article R. 851-5 du code de la sécurité intérieure soit ainsi rédigé :

« II. - Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé. ».

Si le Gouvernement souhaitait conserver au surplus l'alinéa du II figurant dans la saisine rectificative, la CNCTR recommanderait de modifier les références qu'il contient. Seuls les articles L. 851-2 et L. 851-3 du code de la sécurité intérieure se réfèrent en effet à l'ensemble des données de connexion mentionnées à l'article L. 851-1 du même code, dont la nature doit être précisée par décret en Conseil d'État. En revanche, les articles L. 851-4 à L. 851-6 du code définissent chacun de façon autonome les données susceptibles d'être recueillies sur leur fondement : il s'agit des « *données techniques relatives à la localisation des équipements terminaux utilisés* » à l'article L. 851-4, des données permettant « *la localisation en temps réel d'une personne, d'un véhicule ou d'un objet* » à l'article L. 851-5 et des « *données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que [d]es données relatives à la localisation des équipements terminaux utilisés* » à l'article L. 851-6. La CNCTR propose dès lors que la référence aux articles L. 851-4 à L. 851-6 soit supprimée et que l'alinéa soit ainsi rédigé :

« Les informations énumérées aux 2° à 6° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3, dans les conditions et limites prévues par ces articles. ».

b) En ce qui concerne l'accès administratif aux données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure, la CNCTR observe que ce recueil s'effectue, aux termes de la loi, « *sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1* » du code.

Au nouvel article R. 851-7 du code de la sécurité intérieure, le projet de décret dispose que lorsque le recueil en temps réel est demandé par des services de renseignement dits « du second cercle », il est effectué par le groupement interministériel de contrôle (GIC). La CNCTR estime cette procédure conforme à la loi.

Par ailleurs, pour le bon déroulement des contrôles *a posteriori* dont la loi l'a chargée, la CNCTR demande qu'un accès permanent, complet, direct et immédiat à l'ensemble des données de connexion recueillies en application de l'article L. 851-2 du code de la sécurité intérieure, quel que soit le service demandeur, lui soit garanti dans les locaux du GIC.

3. Sur les services de renseignement dits « du second cercle » pouvant être autorisés à recueillir les données de connexion en temps réel en application de l'article L. 851-2 du code de la sécurité intérieure

Dans sa saisine rectificative, le Premier ministre ouvre à certains services de renseignement dits « du second cercle » la possibilité de recueillir les données de connexion en temps réel en application de l'article L. 851-2 du code de la sécurité intérieure. En créant un nouvel article R. 851-1-1 dans le code, le Gouvernement souhaite ainsi modifier la liste des services du second cercle pouvant être autorisés à mettre en œuvre les techniques de renseignement prévues au livre VIII du code, sur laquelle s'était prononcée la CNCTR par sa délibération n° 2/2015 du 12 novembre 2015[10].

10 - Le projet de décret sur lequel a porté la délibération de la CNCTR 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.

S'agissant d'une technique de renseignement que le Gouvernement n'avait initialement pas destinée aux services du second cercle et qui suppose une expertise technique spécifique, la CNCTR préconise une approche restrictive.

En premier lieu, la CNCTR rappelle que l'unité de coordination de la lutte contre le terrorisme (UCLAT) est chargée, par l'arrêté du 8 octobre 1984 qui la crée, d'une mission de coordination, d'animation et d'orientation des directions et services actifs de police en matière de lutte contre le terrorisme. Comme dans sa délibération du n° 2/2015 du 12 novembre 2015, la CNCTR estime que l'UCLAT n'a pas de rôle opérationnel justifiant que lui soit donné accès à des techniques de renseignement. Elle émet donc un avis défavorable à la proposition de lui donner un accès aux données de connexion en temps réel sur le fondement de l'article L. 851-2 du code de la sécurité intérieure.

En second lieu, la CNCTR estime que le caractère intrusif du recueil de données de connexion prévu à l'article L. 851-2 du code de la sécurité intérieure aussi bien que les ressources qu'il exige de mobiliser conduit à en faire un dispositif centralisé, réservé à quelques services de portée principalement nationale.

Pour cette raison, la CNCTR émet un avis favorable concernant les seuls services suivants :

1° Services placés sous l'autorité du directeur général de la police nationale :

a) À la direction centrale de la police judiciaire : la sous-direction anti-terroriste et la sous-direction de la lutte contre la cybercriminalité ;

b) À la direction centrale de la sécurité publique : l'unité nationale de recherche et d'appui des services du renseignement territorial ;

2° Unités placées sous l'autorité du directeur général de la gendarmerie nationale :

À la direction des opérations et de l'emploi : la sous-direction de l'anticipation opérationnelle et la sous-direction de la police judiciaire ;

3° Services placés sous l'autorité du préfet de police de Paris :

a) À la direction du renseignement : la sous-direction de la sécurité intérieure et la sous-direction du renseignement territorial ;

b) À la direction régionale de la police judiciaire de Paris : la section antiterroriste de la brigade criminelle de la sous-direction des brigades centrales.

4. Sur les missions du groupement interministériel de contrôle

La CNCTR estime que la rédaction du nouvel article R. 822-1 du code de la sécurité intérieure, qui définit les missions du GIC, doit être complétée.

La CNCTR rappelle, comme elle l'a déjà indiqué dans sa délibération n° 2/2015 du 12 novembre 2015, que le GIC lui paraît devoir jouer, d'une manière générale, un rôle essentiel dans la traçabilité de la mise en œuvre des techniques de renseignement et dans la centralisation des informations recueillies, auxquelles elle doit disposer d'un accès libre et permanent pour exercer le contrôle *a posteriori* dont elle est chargée par la loi. Elle souhaite donc que le nouvel article R. 822-1 du code de la sécurité intérieure confie explicitement au GIC des missions dans ces deux domaines. Elle suggère d'ajouter dans le projet d'article les deux alinéas suivants :

« 5° Contribuer à la centralisation des renseignements collectés lors de la mise en œuvre des techniques de renseignement autres que celles mentionnées aux 3° et 4° ;

« 6° Concourir à la traçabilité de l'exécution des techniques de renseignement. ».

La CNCTR appelle en outre à nouveau l'attention du Gouvernement sur l'urgence s'attachant à organiser cette traçabilité et à définir les modalités de cette centralisation, ainsi que l'exigent les articles L. 822-1 et L. 854-4 du code de la sécurité intérieure.

5. Sur l'autorisation de plein droit accordée à certains services de l'État pour fabriquer des appareils et dispositifs techniques permettant de porter atteinte à la vie privée

La CNCTR relève que le Gouvernement souhaite modifier l'article R. 226-5 du code pénal pour accorder de plein droit à certains services de l'État désignés par arrêté du Premier ministre l'autorisation de fabriquer des appareils et dispositifs techniques permettant de porter atteinte à la vie privée et, en l'espèce, de mettre en œuvre des techniques de renseignement prévues au livre VIII du code de la sécurité intérieure.

La CNCTR, comme la CNCIS avant elle, souligne qu'un contrôle efficace des atteintes portées à la vie privée suppose non seulement de vérifier la légalité des demandes de mise en œuvre des techniques de renseignement par les services de l'État, mais également de réguler les opérations de commercialisation et d'acquisition par des sociétés privées ou par les services de l'État des appareils et dispositifs techniques qui permettent d'intercepter des communications électroniques ou de capter des données personnelles.

En conséquence, si elle admet que soit accordée l'autorisation de plein droit évoquée ci-dessus, la CNCTR recommande que le registre prévu à l'article R. 226-10 du code pénal et défini par arrêté du 16 août 2006 soit modifié afin de retracer non seulement les opérations de commercialisation portant sur les appareils et dispositifs techniques contrôlés mais également celles de fabrication. Le registre ainsi tenu devra attester, même succinctement, les fonctionnalités des appareils et dispositifs techniques fabriqués ainsi que leur adéquation aux missions confiées aux services bénéficiaires de l'autorisation de plein droit.

Annexe n° 4

Délibération de la CNCTR n° 2/2016 du 10 novembre 2016

La Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière le 10 novembre 2016, a adopté la présente délibération sur les mesures de contrôle et de surveillance des transmissions empruntant la voie hertzienne, prévues à l'article L. 811-5 du code de la sécurité intérieure.

Dans sa décision n° 2016-590 QPC du 21 octobre 2016, le Conseil constitutionnel a déclaré contraire à la Constitution l'article L. 811-5 du code de la sécurité intérieure, dans sa rédaction issue de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement. Cet article permet aux pouvoirs publics de prendre, aux seules fins de défense des intérêts nationaux, des mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne sans que ces mesures soient soumises aux dispositions relatives au renseignement figurant au livre VIII du code, qui définissent les techniques de recueil de renseignement soumises à autorisation délivrée par le Premier ministre après avis préalable de la CNCTR. Le Conseil constitutionnel a jugé que, faute de garanties appropriées et de précisions suffisantes sur leur champ d'application qui, selon lui, n'exclut pas l'interception ou le recueil de données individualisables, ces dispositions portent une « *atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances* ».

Estimant qu'une abrogation immédiate priverait les pouvoirs publics de toute possibilité de surveillance des transmissions empruntant la voie hertzienne et entraînerait à cet égard des conséquences manifestement excessives, le Conseil constitutionnel a décidé de reporter au 31 décembre 2017 la date de prise d'effet de la déclaration d'inconstitutionnalité des dispositions de l'article L. 811-5 du code de la sécurité intérieure.

Le Conseil constitutionnel a en outre jugé que, jusqu'à ce qu'elles soient modifiées par une nouvelle loi et au plus tard jusqu'au 31 décembre 2017, les dispositions de l'article L. 811-5 du code de la sécurité intérieure ne doivent pas 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 autorisation du Premier ministre en vertu de la loi du 24 juillet 2015 et de la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales. Pour parfaire le strict encadrement de la mise en œuvre des dispositions de l'article L. 811-5 du code de la sécurité intérieure pendant cette période transitoire, il a exigé que la CNCTR soit régulièrement informée sur le champ et la nature des mesures prises en application de cet article.

La Commission nationale de contrôle des interceptions de sécurité (CNCIS) avait pris position à plusieurs reprises sur la portée des dispositions de l'article 20 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, ensuite codifiées à l'article L. 241-3 du code de la sécurité intérieure puis transférées au nouvel article L. 811-5 du même code par la loi du 24 juillet 2015. Elle estimait que ces dispositions devaient être interprétées strictement et ne pouvaient notamment servir de fondement à la mise en œuvre d'interceptions de communications individualisables. Elle a en outre mis en doute leur utilité et suggéré qu'elles ne soient pas reprises par la loi du 24 juillet 2015. Elle n'a pas été suivie par le législateur sur ce dernier point.

Exerçant son contrôle sur un champ de techniques de renseignement plus large que celui couvert par la CNCIS, la CNCTR a la même approche que cette dernière sur la portée à donner aux dispositions de l'article L. 811-5 du code de la sécurité intérieure. Cette exception au régime de contrôle institué par la loi du 24 juillet 2015 et par celle du 30 novembre 2015 pour assurer la protection de la vie privée, notamment du secret des correspondances, doit, selon elle, être interprétée strictement. La CNCTR a estimé ainsi que l'article L. 811-5 du code ne peut avoir pour effet de faire échapper l'une quelconque des techniques de renseignement prévues par la loi du 24 juillet 2015 au régime d'autorisation préalable et de contrôle établi par cette loi. C'est notamment le cas du recueil de données de connexion et des interceptions de sécurité des communications émises ou reçues par un téléphone

portable : elles doivent faire l'objet d'une autorisation préalable du Premier ministre, après avis de la CNCTR, dans les conditions fixées par les articles L. 851-1 et L. 852-1 du code de la sécurité intérieure, bien que les communications interceptées empruntent la voie hertzienne. La CNCTR a constaté que son interprétation de la loi était partagée par les pouvoirs publics.

En conséquence, la CNCTR recommande au Premier ministre de demander à chacun des ministres exerçant la tutelle de services de renseignement concernés de veiller à ce que toutes les techniques de renseignement mentionnées dans la loi du 24 juillet 2015 et dans celle du 30 novembre 2015 ne puissent être mises en œuvre qu'après avoir été préalablement autorisées par lui, conformément à ces lois. Elle recommande que chacun des ministres définisse dans une instruction adressée aux services concernés relevant de son autorité les conditions — notamment les motifs, le champ d'application et la nature des techniques — dans lesquelles ces services pourront être autorisés à invoquer les dispositions de l'article L. 811-5 du code de la sécurité intérieure. Elle recommande en outre que ces instructions soient soumises à son avis.

La CNCTR est chargée par le Conseil constitutionnel de suivre la mise en œuvre de l'article L. 811-5 du code de la sécurité intérieure pendant la période transitoire durant laquelle les pouvoirs publics demeurent autorisés à appliquer ces dispositions. Elle doit s'assurer qu'aucune technique d'interception de correspondance et de recueil de données individualisables n'est mise en œuvre dans le cadre de l'article L. 811-5 sans avoir été préalablement autorisée en application des dispositions du livre VIII du code de la sécurité intérieure. Aux fins de ce contrôle, la CNCTR doit être régulièrement informée sur le champ et la nature des mesures prises en application de l'article L. 811-5. Cette information doit la mettre à même de vérifier la conformité de ces mesures à la réserve d'interprétation émise par le Conseil constitutionnel, de recommander, si elle les estime non conformes à cette réserve, leur interruption et la destruction des renseignements collectés et, dans l'hypothèse où sa recommandation ne serait pas suivie, de saisir le Conseil d'État, dans les conditions prévues aux articles L. 833-6 à L. 833-8 du code de la sécurité intérieure ainsi qu'à l'article L. 854-9 du même code.

La CNCTR examine avec chacun des services concernés les modalités précises lui permettant d'être régulièrement informée des mesures prises par eux en application de l'article L. 811-5 du code de la sécurité intérieure.

La CNCTR souhaite enfin être consultée sur les dispositions nouvelles que le législateur pourrait élaborer pour tirer les conséquences de la déclaration d'inconstitutionnalité de l'article L. 811-5 du code de la sécurité intérieure.

Annexe n° 5

Règlement intérieur de la Commission nationale de contrôle des techniques de renseignement

La Commission nationale de contrôle des techniques de renseignement,

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

Vu le code de justice administrative ;

Vu la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique ;

Vu la loi n° 2015-912 du 24 juillet 2015 relative au renseignement ;

Vu le décret n° 2014-90 du 31 janvier 2014 portant application de l'article 2 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, notamment ses articles 1 à 4 ;

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

DECIDE :

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

Article 1er

Les membres et agents de la Commission nationale de contrôle des techniques de renseignement, ci-après dénommée « la commission »,

s'abstiennent de tout comportement de nature à faire naître un doute sur l'indépendance de l'institution. Ils doivent prévenir toute situation de conflit d'intérêt.

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

Les membres adressent au président de la commission copie de la déclaration d'intérêts prévue par l'article 11 de la loi du 11 octobre 2013 susvisée.

Article 2

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

Les membres et agents de la commission ne peuvent recevoir aucune instruction d'une quelconque autorité.

Article 3

Les membres et agents de la commission observent le secret de la défense nationale et le devoir de confidentialité auxquels ils sont tenus par la loi.

Cette obligation se perpétue après le terme du mandat de membre ou des fonctions d'agent de la commission.

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

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

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

En outre, les membres et agents de la commission sont astreints à un devoir de discrétion sur l'ensemble des activités de la commission.

Article 4

Dans le traitement des demandes soumises à la commission, l'impartialité et la neutralité doivent être observées.

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

Article 5

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

Ils ne se départissent jamais de la courtoisie requise.

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

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

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

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

Article 6

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

II – Formation plénière et formation restreinte

Article 7

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

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

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

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

Les formations plénière et restreinte de la commission statuent à la majorité des membres présents ou participant au délibéré dans les conditions fixées à l'article 8, le président ayant voix prépondérante en cas de partage égal des voix.

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

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

Article 8

Lorsque la formation plénière ou restreinte se réunit en urgence, il peut être fait recours à tous moyens de communication électronique dès lors que le secret des échanges est assuré.

Article 9

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

Article 10

Les membres ont, dans les locaux de la commission, accès à tout moment aux avis émis sur les demandes mentionnées à l'article L. 821-2 du code de la sécurité intérieure et aux suites données à ces avis par le Premier ministre.

Article 11

La formation plénière débat des principes et des modalités qui régissent les avis sur les demandes mentionnées à l'article L. 821-2 du code de la sécurité intérieure ainsi que des contrôles opérés par la commission sur la mise en œuvre des techniques de renseignement.

Article 12

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

Les résultats des contrôles et les suites données sont portées à la connaissance de la formation plénière de la commission.

Article 13

Lorsque le Premier ministre n'a pas donné suite à un avis de la commission sur une demande mentionnée à l'article L. 821-2 du code de la sécurité intérieure, la formation plénière en est informée dans les meilleurs délais et débat des suites à donner.

La formation plénière est informée des recommandations adressées au Premier ministre, tendant à ce que la mise en œuvre d'une technique soit interrompue et les renseignements collectés détruits.

Elle débat des suites données par le Premier ministre à ces recommandations.

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

Article 14

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

III – Secrétariat et agents de la commission

Article 15

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

Le secrétaire général anime et coordonne leur action.

IV – Traitement des demandes

Article 16

Le président fixe, en concertation avec les membres et agents de la commission, les conditions dans lesquelles les avis sont rendus sur les demandes mentionnées à l'article L. 821-2 du code de la sécurité intérieure.

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

Article 17

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

Article 18

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

Lorsque toutes les informations nécessaires à un examen approprié de la demande n'ont pas été communiquées, la commission invite le service à l'origine de la demande à lui transmettre sans délai les renseignements nécessaires.

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

Article 19

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

V – Rapport public, communication et relations extérieures

Article 20

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

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

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

Article 21

Le rapport public, débattu et approuvé en formation plénière, est remis par le président au Premier ministre et aux présidents des deux assemblées.

Le président invite les parlementaires membres de la commission à l'accompagner lors de la visite qu'il rend au président de leur assemblée respective.

Article 22

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

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

Article 23

Si la formation plénière de la commission envisage de suspendre ou de mettre fin au mandat de l'un de ses membres pour l'un des motifs énoncés à l'article L. 831-1 du code de la sécurité intérieure, elle sollicite de ce dernier des observations écrites et l'entend sur sa demande. La formation plénière délibère hors sa présence.

Article 24

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

Annexe n° 6

Décret du 1er octobre 2015 relatif à la composition de la Commission nationale de contrôle des techniques de renseignement

Par décret du Président de la République en date du 1er octobre 2015 :

M. Francis DELON est nommé président de la Commission nationale de contrôle des techniques de renseignement.

M. Patrick PUGES est nommé membre de la Commission nationale de contrôle des techniques de renseignement en qualité de personnalité qualifiée pour ses connaissances en matière de communications électroniques.

La commission comprend en outre :

1° Mme Jacqueline DE GUILLENCHMIDT, membre nommée par le vice-président du Conseil d'État ;

2° M. Franck TERRIER et Mme Christine PENICHON, membres nommés conjointement par le premier président et par le procureur général de la Cour de cassation ;

3° M. Pascal POPELIN et Mme Catherine VAUTRIN, membres nommés par l'Assemblée nationale ;

4° M. Michel BOUTANT et Mme Catherine TROENDLE, membres nommés par le Sénat.

Les nominations prennent effet le 3 octobre 2015.

Annexe n° 7

Liste des autorités de contrôle étrangères rencontrées

Autorités nationales de contrôle

- Délégation des commissions de gestion, Assemblée fédérale, Suisse, octobre 2015 ;
- Comité R, Belgique, décembre 2015 ;
- Interception of Communications Commissioner's Office, Grande-Bretagne, avril 2016 ;
- Stortingets kontrollutvalg for etterretnings (EOS), Norvège, avril 2016
- G10-Kommission, Allemagne, septembre 2016 ;
- Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, Pays-Bas, octobre 2016.

Organisations internationales

- Agence européenne des droits fondamentaux (FRA), Union européenne, février 2016 ;
- Haut-commissariat aux droits de l'Homme, rapporteur spécial pour le droit à la vie privée, Organisation des nations unies, octobre 2016.

Annexe n° 8

Décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015

Loi relative au renseignement

Le Conseil constitutionnel a été saisi, le 25 juin 2015, sous le numéro 2015-713 DC, par le président du Sénat, dans les conditions prévues à l'article 61, deuxième alinéa, de la Constitution, de la loi relative au renseignement,

Et, le même jour, par le Président de la République,

Et, le même jour, par M^me^ Laure de LA RAUDIÈRE, M. Pierre LELLOUCHE, M^me^ Laurence ABEILLE, M. Éric ALAUZET, M^mes^ Brigitte ALLAIN, Isabelle ATTARD, Danielle AUROI, M. Denis BAUPIN, M^me^ Michèle BONNETON, M. Sergio CORONADO, M^mes^ Cécile DUFLOT, Véronique MASSONNEAU, Barbara POMPILI, M. Jean-Louis ROUMEGAS, M^me^ Eva SAS, MM. Damien ABAD, Élie ABOUD, Yves ALBARELLO, Julien AUBERT, Patrick BALKANY, Sylvain BERRIOS, Étienne BLANC, Xavier BRETON, Luc CHATEL, Gérard CHERPION, Alain CHRÉTIEN, Philippe COCHET, Jean-Louis COSTES, Marc-Philippe DAUBRESSE, Claude de GANAY, Bernard DEBRÉ, Jean-Pierre DECOOL, Lucien DEGAUCHY, Patrick DEVEDJIAN, Nicolas DHUICQ, M^mes^ Sophie DION, Virginie DUBY-MULLER, MM. Sauveur GANDOLFI-SCHEIT, Hervé GAYMARD, Franck GILARD, Charles-Ange GINESY, Claude GOASGUEN, Jean-Pierre GORGES, M^mes^ Claude GREFF, Anne GROMMERCH, Arlette GROSSKOST, MM. Henri GUAINO, Jean-Jacques GUILLET, Antoine HERTH, Patrick HETZEL, Philippe HOUILLON, Denis JACQUAT, Jacques KOSSOWSKI, M^me^ Valérie LACROUTE, M. Jean-François LAMOUR, M^me^ Isabelle LE CALLENNEC, MM. Marc LE FUR, Bruno LE MAIRE,

Alain LEBOEUF, Jean LEONETTI, M. Céleste LETT, M^me^ Véronique LOUWAGIE, MM. Lionnel LUCA, Jean-François MANCEL, Thierry MARIANI, Hervé MARITON, Alain MARSAUD, Philippe ARMAND, Patrice MARTIN-LALANDE, Alain MARTY, Philippe MEUNIER, Pierre MORANGE, Yannick MOREAU, Pierre MOREL-A-L'HUISSIER, Alain MOYNE-BRESSAND, M^me^ Valérie PÉCRESSE, MM. Jacques PÉLISSARD, Bernard PERRUT, Jean-Frédéric POISSON, M^me^ Bérengère POLETTI, MM. Frédéric REISS, Franck RIESTER, Arnaud ROBINET, Martial SADDIER, Paul SALEN, M^me^ Claudine SCHMID, MM. Thierry SOLÈRE, Éric STRAUMANN, Alain SUGUENOT, Lionel TARDY, Jean-Charles TAUGOURDEAU, Michel VOISIN, M^mes^ Marie-Jo ZIMMERMANN, Véronique BESSE, MM. Gilbert COLLARD, Jean LASSALLE, M^me^ Marion MARÉCHAL-LE PEN, MM. Charles de COURSON, Yannick FAVENNEC, Jean-Christophe FROMANTIN, Maurice LEROY, Hervé MORIN, Arnaud RICHARD, Edouard PHILIPPE, Noël MAMÈRE et Jean-Claude MIGNON, députés.

LE CONSEIL CONSTITUTIONNEL,

Vu la Constitution ;

Vu l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel ;

Vu la loi organique n° 2001-692 du 1^er^ août 2001 relative aux lois de finances ;

Vu le code de la défense ;

Vu le code des douanes ;

Vu le code de justice administrative ;

Vu le code pénal ;

Vu le code des postes et des communications électroniques ;

Vu le code de la sécurité intérieure ;

Vu la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

Vu les observations du Gouvernement, enregistrées le 7 juillet 2015 ;

Vu les observations en réplique présentées par les députés requérants, enregistrées le 21 juillet 2015 ;

Le rapporteur ayant été entendu ;

1. Considérant que le Président de la République, le président du Sénat et plus de soixante députés défèrent au Conseil constitutionnel la loi relative au renseignement ; que le Président de la République demande au Conseil constitutionnel de se prononcer sur la conformité au droit au respect de la vie privée, à la liberté de communication et au droit à un recours juridictionnel effectif des articles L. 811-3, L. 821-5 à L. 821-7, L. 822-2 et L. 841-1 du code de la sécurité intérieure tels qu'ils résultent de l'article 2 de la loi, des articles L. 851-3, L. 851-5, L. 851-6 et du paragraphe II de l'article L. 852-1 du même code tels qu'ils résultent de l'article 5 de la loi, des articles L. 853-1 à L. 853-3 du même code tels qu'ils résultent de l'article 6 de la loi ainsi que des articles L. 773-2 à L. 773-7 du code de justice administrative tels qu'ils résultent de l'article 10 de la loi ; que le président du Sénat n'invoque à l'encontre de ce texte aucun grief particulier ; que les députés requérants contestent la conformité à la Constitution, et en particulier au droit au respect de la vie privée et à la liberté d'expression, des articles L. 811-3, L. 811-4, L. 821-1, L. 821-7 et L. 831-1 du code de la sécurité intérieure tels qu'ils résultent de l'article 2 de la loi, des articles L. 851-1 à L. 851-6 et de l'article L. 852-1 du même code tels qu'ils résultent de l'article 5 de la loi, des articles L. 853-1 à L. 853-3 et L. 854-1 du même code tels qu'ils résultent de l'article 6 de la loi ainsi que des articles L. 773-3 et L. 773-6 du code de justice administrative tels qu'ils résultent de l'article 10 de la loi ;

- SUR LES NORMES DE RÉFÉRENCE :

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

3. Considérant qu'en vertu de l'article 5 de la Constitution, le Président de la République est le garant de l'indépendance nationale et de l'intégrité du territoire ; qu'aux termes du premier alinéa de l'article 20 : « *Le Gouvernement détermine et conduit la politique de la Nation* » ; qu'en vertu de l'article 21, le Premier ministre « *dirige l'action du Gouvernement* » et « *est responsable de la Défense nationale* » ; que le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire ;

4. Considérant qu'aux termes de l'article 66 de la Constitution : « *Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi* » ;

5. Considérant qu'aux termes de l'article 16 de la Déclaration de 1789 : « *Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution* » ; que sont garantis par cette disposition le droit des personnes intéressées à exercer un recours juridictionnel effectif, le droit à un procès équitable ainsi que le principe du contradictoire ;

- SUR CERTAINES DISPOSITIONS DE L'ARTICLE 2 :

6. Considérant que l'article 2 de la loi déférée complète, par les titres I^{er} à IV, le livre VIII du code de la sécurité intérieure créé par l'article 1er de la même loi ; que le titre I^{er} est consacré aux dispositions générales et comprend les articles L. 811-1 à L. 811-4 ; que le titre II est consacré à la procédure applicable aux techniques de recueil de renseignement soumises à autorisation et comprend les articles L. 821-1 à L. 822-4 ; que le titre III est relatif à la commission nationale de contrôle des techniques de renseignement et comprend les articles L. 831-1 à L. 833-11 ; que le titre IV est consacré aux recours relatifs à la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État et comprend les articles L. 841-1 et L. 841-2 ;

En ce qui concerne l'article L. 811-3 du code de la sécurité intérieure :

7. Considérant que l'article L. 811-3 du code de la sécurité intérieure énumère les finalités pour lesquelles les services spécialisés de renseignement peuvent recourir aux techniques définies aux articles L. 851-1 à L. 854-1 du même code tels qu'ils résultent des articles 5 et 6 de la loi déférée, pour le seul exercice de leurs missions respectives, afin de recueillir des renseignements ; que ces finalités correspondent à « *la défense et la promotion des intérêts fondamentaux de la Nation suivants : 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;*

« 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

« 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;

« 4° La prévention du terrorisme ;

« 5° La prévention :

« a) Des atteintes à la forme républicaine des institutions ;

« b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;

« c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;

« 6° La prévention de la criminalité et de la délinquance organisées ;

« 7° La prévention de la prolifération des armes de destruction massive » ;

8. Considérant que les députés requérants font valoir que les finalités énumérées par le législateur sont trop larges, au regard des techniques de recueil de renseignement prévues par la loi déférée, et insuffisamment définies ; qu'il en résulterait une atteinte disproportionnée au droit au respect de la vie privée ainsi qu'à la liberté d'expression ;

9. Considérant que le recueil de renseignement au moyen des techniques définies au titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative ; qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions ; qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs ;

10. Considérant qu'en retenant, pour déterminer les finalités énumérées aux 1° à 4°, des définitions faisant référence à certains des intérêts mentionnés à l'article 410-1 du code pénal, le législateur a précisément circonscrit les finalités ainsi poursuivies et n'a pas retenu des critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative ; qu'il en va de même pour les finalités définies au a) du 5°, faisant référence aux incriminations pénales du chapitre II du titre Ier du livre IV du code pénal, de celles définies au b) du 5°, faisant référence aux dispositions de l'article L. 212-1 du code de la sécurité intérieure, de celles définies au c) du 5°, faisant référence aux incriminations pénales définies aux articles 431-1 à 431-10 du code pénal, de celles définies au 6°, faisant référence aux incriminations pénales énumérées à l'article 706-73 du code de procédure pénale et aux délits punis par l'article 414 du code des douanes commis en bande organisée et de celles définies au 7°, faisant référence aux incriminations pénales définies aux articles L. 2339-14 à L. 2339-18 du code de la défense ;

11. Considérant que les dispositions de l'article L. 811-3 doivent être combinées avec celles de l'article L. 801-1, dans sa rédaction résultant de l'article 1er de la loi déférée, aux termes desquelles la décision de recourir aux techniques de renseignement et les techniques choisies devront être proportionnées à la finalité poursuivie et aux motifs invoqués ; qu'il en résulte que les atteintes au droit au respect de la vie privée doivent être proportionnées à l'objectif poursuivi ; que la Commission nationale de contrôle des techniques de renseignement et le Conseil d'État sont chargés de s'assurer du respect de cette exigence de proportionnalité ;

12. Considérant qu'il résulte de ce qui précède que les dispositions de l'article L. 811-3 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

En ce qui concerne l'article L. 811-4 du code de la sécurité intérieure :

13. Considérant que l'article L. 811-4 du code de la sécurité intérieure renvoie à un décret en Conseil d'État la désignation des services, autres que les services spécialisés de renseignement, qui peuvent être autorisés à recourir aux techniques définies au titre V du livre VIII du code de la sécurité intérieure ; qu'il renvoie également à ce décret la délimitation, pour chaque service, des finalités et des techniques qui peuvent donner lieu à autorisation ;

14. Considérant que, selon les députés requérants, en renvoyant au pouvoir réglementaire le soin de déterminer les services non spécialisés qui pourront recourir aux techniques de recueil de renseignement ainsi que celles de ces techniques qu'il leur sera loisible de mettre en œuvre, le législateur n'a pas fixé lui-même des règles concernant des garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que le législateur aurait ainsi méconnu l'étendue de sa compétence ;

15. Considérant qu'en définissant les techniques de recueil de renseignement qui peuvent être mises en œuvre par les services de renseignement et les finalités pour lesquelles elles peuvent l'être tout en confiant au pouvoir réglementaire le soin d'organiser ces services visés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure, le législateur n'est pas resté en deçà de la compétence que lui attribue l'article 34 de la Constitution pour fixer « *les règles concernant … les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » ; que les dispositions de l'article L. 811-4 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

En ce qui concerne l'article L. 821-1 du code de la sécurité intérieure :

16. Considérant que l'article L. 821-1 du code de la sécurité intérieure prévoit que les techniques de recueil de renseignement définies aux articles L. 851-1 à L. 853-3 du même code sont mises en œuvre sur le territoire national par des agents individuellement désignés et habilités, sur autorisation préalable du Premier ministre délivrée après avis de la Commission nationale de contrôle des techniques de renseignement ;

17. Considérant que, selon les députés requérants, en prévoyant une autorisation délivrée par le pouvoir exécutif, après avis de la Commission nationale de contrôle des techniques de renseignement, et en permettant que l'autorisation puisse être délivrée en dépit d'un avis défavorable de cette commission, les dispositions contestées présenteraient des garanties insuffisantes au regard des droits et libertés constitutionnellement garantis, et notamment de la liberté d'expression et de communication ; qu'en ne plaçant pas le recours à ces techniques sous le contrôle du juge judiciaire, le législateur méconnaîtrait tant les exigences de l'article 66 de la Constitution que celles de l'article 16 de la Déclaration de 1789 ;

18. Considérant, en premier lieu, que l'autorisation, sollicitée par une demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, est délivrée par le Premier ministre à des agents individuellement désignés et habilités pour mettre en œuvre sur le territoire national des techniques de recueil de renseignement, pour une durée maximale de quatre mois ; qu'elle est subordonnée à l'avis préalable de la Commission nationale de contrôle des techniques de renseignement ; que le législateur s'est fondé sur l'article 21 de la Constitution pour confier au Premier ministre le pouvoir d'autoriser la mise en œuvre des techniques de recueil de renseignement dans le cadre de la police administrative ;

19. Considérant qu'en elle-même, la procédure d'autorisation par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement ne méconnaît ni le droit au respect de la vie privée, ni l'inviolabilité du domicile ni le secret des correspondances ;

20. Considérant, en deuxième lieu, que ces dispositions, qui sont relatives à la délivrance d'autorisations de mesures de police administrative par le Premier ministre après consultation d'une autorité administrative indépendante, ne privent pas les personnes d'un recours juridictionnel à l'encontre des décisions de mise en œuvre à leur égard des techniques de recueil de renseignement ; que les exigences de l'article 16 de la Déclaration de 1789 ne sont donc pas méconnues ;

21. Considérant, en troisième lieu, que ces dispositions ne portent pas d'atteinte à la liberté individuelle ;

22. Considérant qu'il résulte de tout ce qui précède que les dispositions de l'article L. 821-1 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

En ce qui concerne l'article L. 821-5 du code de la sécurité intérieure :

23. Considérant que l'article L. 821-5 du code de la sécurité intérieure institue une procédure dérogatoire de délivrance de l'autorisation de mettre en œuvre des techniques de recueil de renseignement en cas d'urgence absolue et pour les seules finalités mentionnées aux 1°, 4° et a) du 5° de l'article L. 811-3 du même code ; que, dans ce cas, l'autorisation du Premier ministre est délivrée sans avis préalable de la Commission nationale de contrôle des techniques de renseignement, laquelle est informée sans délai et reçoit dans les vingt-quatre heures à compter de la délivrance de l'autorisation tous les éléments de motivation de l'autorisation ainsi que ceux justifiant le caractère d'urgence absolue ;

24. Considérant, d'une part, que la procédure dérogatoire prévue par l'article L. 821-5 n'est pas applicable lorsque la mise en œuvre des techniques de recueil de renseignement exige l'introduction dans un lieu privé à usage d'habitation en application du paragraphe V de l'article L. 853-1 ou du paragraphe V de l'article L. 853-2 et n'est donc pas susceptible d'affecter l'inviolabilité du domicile ;

25. Considérant, d'autre part, que la procédure dérogatoire prévue par l'article L. 821-5 est réservée à certaines des finalités mentionnées à l'article L. 811-3, qui sont relatives à la prévention d'atteintes particulièrement graves à l'ordre public, et doit être motivée par le caractère d'urgence absolue du recours à la technique de recueil de renseignement ; que cette procédure n'est pas applicable aux techniques de recueil de renseignement prévues aux articles L. 851-2 et L. 851-3 et au 1° du paragraphe I de l'article L. 853-2 ; qu'elle n'est pas non plus applicable lorsqu'une technique prévue à l'article L. 853-1 ou au 2° de l'article L. 853-2 doit être mise en œuvre au moyen de l'introduction dans un lieu d'habitation ; que la Commission nationale de contrôle des techniques de renseignement, qui doit en être informée sans délai, doit recevoir l'ensemble des éléments de motivation ainsi que la

justification du caractère d'urgence absolue dans un délai maximal de vingt-quatre heures ; que la commission dispose de l'ensemble des moyens relatifs au contrôle de la mise en œuvre d'une technique de recueil de renseignement qui lui sont conférés par les articles L. 833-1 à L. 833-11 pour s'assurer que le cadre légal a été respecté ; que l'autorisation du Premier ministre de mettre en œuvre les techniques de recueil de renseignement selon cette procédure dérogatoire est placée sous le contrôle juridictionnel du Conseil d'État, chargé d'apprécier les motifs qui en ont justifié l'usage ; que, par suite, les dispositions de l'article L. 821-5 du code de la sécurité intérieure ne portent pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances ;

26. Considérant qu'il résulte de ce qui précède que les dispositions de l'article L. 821-5 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

En ce qui concerne l'article L. 821-6 du code de la sécurité intérieure :

27. Considérant que l'article L. 821-6 du code de la sécurité intérieure institue une procédure dérogatoire d'installation, d'utilisation et d'exploitation des appareils ou dispositifs techniques de localisation en temps réel d'une personne, d'un véhicule ou d'un objet, d'identification d'un équipement terminal ou du numéro d'abonnement ainsi que de localisation de cet équipement ou d'interception des correspondances émises ou reçues par cet équipement, en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement ; que cette procédure permet aux agents individuellement désignés et habilités d'installer, utiliser et exploiter sans autorisation préalable ces appareils ou dispositifs techniques ; que le Premier ministre, le ministre concerné et la Commission nationale de contrôle des techniques de renseignement en sont informés sans délai et par tout moyen ; que le Premier ministre peut ordonner à tout moment d'interrompre la mise en œuvre de la technique et de détruire sans délai les renseignements collectés ; qu'une autorisation doit être ensuite délivrée par le Premier ministre, dans un délai de quarante-huit heures, après avis rendu par la commission au vu des éléments de motivation mentionnés à l'article L. 821-4 du même code et de ceux justifiant le recours à la procédure d'urgence ;

28. Considérant, d'une part, que la procédure prévue à l'article L. 821-6 peut être utilisée pour la mise en place des techniques de recueil de renseignement prévues par les articles L. 851-5, L. 851-6 et par le paragraphe II de l'article L. 852-1 du code de la sécurité intérieure ; que ces procédures permettent à l'autorité administrative d'utiliser un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet, ou de recueillir ou d'intercepter, au moyen d'un appareil ou d'un dispositif, sans le consentement de leur auteur les données de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés et les correspondances émises ou reçues par un équipement terminal ;

29. Considérant, d'autre part, qu'à l'inverse des autres procédures dérogatoires, y compris celle instituée par l'article L. 821-5 du même code, la procédure prévue par l'article L. 821-6 permet de déroger à la délivrance préalable d'une autorisation par le Premier ministre ou par l'un de ses collaborateurs directs habilités au secret de la défense nationale auxquels il a délégué cette attribution, ainsi qu'à la délivrance d'un avis préalable de la Commission nationale de contrôle des techniques de renseignement ; qu'elle ne prévoit pas non plus que le Premier ministre et le ministre concerné doivent être informés au préalable de la mise en œuvre d'une technique dans ce cadre ; que, par suite, les dispositions de l'article L. 821-6 portent une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances ; que les dispositions de l'article L. 821-6 du code de la sécurité intérieure doivent être déclarées contraires à la Constitution ;

30. Considérant que, par voie de conséquence, la dernière phrase du premier alinéa de l'article L. 821-7 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi déférée, qui est indissociable des dispositions de l'article L. 821-6, doit également être déclarée contraire à la Constitution ; qu'il en va de même des mots : « *et L. 821-6* » au septième alinéa de l'article L. 833-9 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi déférée ;

En ce qui concerne l'article L. 821-7 du code de la sécurité intérieure :

31. Considérant que l'article L. 821-7 du code de la sécurité intérieure interdit qu'un parlementaire, un magistrat, un avocat ou un journaliste puisse être l'objet d'une demande de mise en œuvre, sur le territoire national, d'une technique de recueil de renseignement définie aux articles L. 851-1 à L. 853-3 à raison de l'exercice de son mandat ou de sa profession ; qu'il impose un examen en formation plénière par la Commission nationale de contrôle des techniques de renseignement d'une demande concernant l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles ; qu'il interdit le recours à la procédure dérogatoire prévue par l'article L. 821-5 ; que la commission, qui est informée des modalités d'exécution des autorisations délivrées en application du présent article, et à laquelle sont transmises les transcriptions des renseignements collectés sur ce fondement, veille au caractère nécessaire et proportionné des atteintes portées aux garanties attachées à l'exercice des activités professionnelles ou mandats ;

32. Considérant que, selon les députés requérants, ces dispositions n'assurent pas une protection suffisante contre l'atteinte indirecte au secret des sources des journalistes ainsi qu'à la confidentialité des échanges entre avocats et clients ; qu'il en résulterait une atteinte au droit au respect de la vie privée ainsi que, pour les avocats, aux droits de la défense et au droit à un procès équitable, et pour les journalistes, à la liberté d'expression ; qu'en outre, l'absence d'incrimination pénale des agents qui révèleraient le contenu des renseignements collectés permettrait le contournement des garanties légales de la protection du secret professionnel de ces professions ;

33. Considérant que les députés requérants contestent également l'absence d'application des dispositions contestées aux professeurs d'université et maîtres de conférences, en méconnaissance du principe fondamental reconnu par les lois de la République d'indépendance des enseignants-chercheurs ;

34. Considérant, en premier lieu, que les dispositions contestées prévoient un examen systématique par la Commission nationale de contrôle des techniques de recueil de renseignement siégeant en formation plénière d'une demande de mise en œuvre d'une technique de renseignement concernant

un membre du Parlement, un magistrat, un avocat ou un journaliste ou leurs véhicules, bureaux ou domiciles, laquelle ne peut intervenir à raison de l'exercice du mandat ou de la profession ; que la procédure dérogatoire prévue par l'article L. 821-5 du code de la sécurité intérieure n'est pas applicable ; qu'il incombe à la commission, qui est destinataire de l'ensemble des transcriptions de renseignements collectés dans ce cadre, de veiller, sous le contrôle juridictionnel du Conseil d'État, à la proportionnalité tant des atteintes portées au droit au respect de la vie privée que des atteintes portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats ; qu'il résulte de ce qui précède que les dispositions de l'article L. 821-7 ne portent pas une atteinte manifestement disproportionnée au droit au respect de la vie privée, à l'inviolabilité du domicile et au secret des correspondances ;

35. Considérant, en deuxième lieu, que l'article 226-13 du code pénal incrimine la révélation d'une information à caractère secret par une personne qui en est dépositaire ; que, par suite, le grief tiré de l'absence d'incrimination pénale des agents qui révèleraient les renseignements ou données collectés manque en fait ;

36. Considérant, en troisième lieu, que le principe d'indépendance des enseignants-chercheurs n'implique pas que les professeurs d'université et maîtres de conférences doivent bénéficier d'une protection particulière en cas de mise en œuvre à leur égard de techniques de recueil de renseignement dans le cadre de la police administrative ;

37. Considérant qu'il résulte de tout de ce qui précède que le surplus des dispositions de l'article L. 821-7 du code de la sécurité intérieure, qui ne méconnaissent aucune exigence constitutionnelle, doivent être déclarées conformes à la Constitution ;

En ce qui concerne l'article L. 822-2 du code de la sécurité intérieure :

38. Considérant que l'article L. 822-2 du code de la sécurité intérieure fixe les durées de conservation maximales des renseignements collectés par la mise en œuvre d'une technique de recueil de renseignement définie aux

articles L. 851-1 à L. 853-3 du même code ; que ces durées sont de trente jours à compter de leur recueil pour les correspondances interceptées et les paroles captées, de cent vingt jours à compter de leur recueil pour les données informatiques et les images, de quatre ans à compter de leur recueil pour les données de connexion et de six ans à compter de leur recueil pour les données chiffrées ;

39. Considérant qu'en prévoyant de telles durées de conservation en fonction des caractéristiques des renseignements collectés ainsi qu'une durée maximale de conservation de six ans à compter du recueil des données chiffrées, au-delà de laquelle les renseignements collectés doivent être détruits, le législateur n'a méconnu aucune exigence constitutionnelle ; que les dispositions de l'article L. 822-2 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

En ce qui concerne l'article L. 831-1 du code de la sécurité intérieure :

40. Considérant que l'article L. 831-1 du code de la sécurité intérieure est relatif à la composition de la Commission nationale de contrôle des techniques de renseignement, qui est qualifiée d'autorité administrative indépendante ; qu'elle est composée de neuf membres, dont un président ; qu'elle comprend deux députés et deux sénateurs, désignés, respectivement, pour la durée de la législature par l'Assemblée nationale et pour la durée de leur mandat par le Sénat, deux membres du Conseil d'État nommés par le vice-président du Conseil d'État, deux magistrats hors hiérarchie de la Cour de cassation nommés conjointement par le Premier président et par le procureur général de la Cour de cassation et une personnalité qualifiée pour sa connaissance en matière de communications électroniques nommée sur proposition du président de l'autorité de régulation des communications électroniques et des postes ; que son président est nommé par décret du Président de la République parmi les membres issus du Conseil d'État ou de la Cour de cassation ; que la durée du mandat des membres non parlementaires est fixée à six ans ; que le mandat des membres n'est pas renouvelable ; que les membres du Conseil d'État et les magistrats de la Cour de cassation sont renouvelés par moitié tous les trois ans ; que la commission peut suspendre le mandat d'un de ses membres ou y mettre fin en cas d'incompatibilité, d'empêchement ou de manquement ;

41. Considérant que les députés requérants soutiennent que la composition de la Commission nationale de contrôle des techniques de renseignement est fixée en méconnaissance du principe de séparation des pouvoirs dès lors, d'une part, qu'un seul de ses neuf membres est désigné eu égard à ses compétences en matière de communications électroniques et, d'autre part, que les membres du Parlement sont minoritaires ;

42. Considérant, d'une part, que la présence d'une seule personnalité qualifiée pour sa connaissance en matière de communications électroniques au sein de la Commission nationale de contrôle des techniques de renseignement est sans incidence sur le respect du principe de la séparation des pouvoirs ;

43. Considérant, d'autre part, que la présence de membres du Parlement parmi les membres de la Commission nationale de contrôle des techniques de renseignement n'est pas de nature à porter atteinte au principe de la séparation des pouvoirs, garanti par l'article 16 de la Déclaration de 1789, dès lors qu'ils sont astreints, en vertu du troisième alinéa de l'article L. 832-5 du code de la sécurité intérieure, au respect des secrets protégés aux articles 226-13 et 413-10 du code pénal ;

44. Considérant que l'article L. 831-1 du code de la sécurité intérieure doit être déclaré conforme à la Constitution ;

En ce qui concerne certaines dispositions de l'article L. 832-4 du code de la sécurité intérieure :

45. Considérant que l'article L. 832-4 du code de la sécurité intérieure est relatif aux moyens accordés à la Commission nationale de contrôle des techniques de renseignement ; qu'à ce titre, la deuxième phrase du premier alinéa de cet article dispose que les crédits de la commission sont inscrits au programme « Protection des droits et libertés » de la mission « Direction de l'action du Gouvernement » ;

46. Considérant que le 1° du paragraphe II de l'article 34 de la loi organique du 1er août 2001 susvisée, à laquelle renvoie l'article 34 de la Constitution, réserve à un texte de loi de finances le soin de fixer « *pour le budget général, par mission, le montant des autorisations d'engagement et des crédits de paiement* » ;

47. Considérant que la deuxième phrase du premier alinéa de l'article L. 832-4, qui empiète sur le domaine exclusif d'intervention des lois de finances, doit être déclarée contraire à la Constitution ;

En ce qui concerne l'article L. 841-1 du code de la sécurité intérieure :

48. Considérant que l'article L. 841-1 du code de la sécurité intérieure prévoit que « *Sous réserve des dispositions particulières prévues à l'article L. 854-1 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* » ; qu'en vertu du 1° du même article, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'elle ne fait pas, ou n'a pas fait, l'objet d'une surveillance irrégulière, sous réserve de l'exercice d'une réclamation préalable auprès de la Commission nationale de contrôle des techniques de renseignement conformément à l'article L. 833-4 du même code ; qu'en vertu du 2° de l'article L. 841-1, le Conseil d'État peut être saisi par ladite commission lorsqu'elle estime que ses avis ou recommandations n'ont pas été suivis d'effet ou que les suites qui y ont été données sont insuffisantes, ou par au moins trois de ses membres ; qu'en vertu du cinquième alinéa de l'article L. 841-1, une juridiction administrative ou une autorité judiciaire saisie d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité d'une technique de recueil de renseignement a la faculté de saisir le Conseil d'État à titre préjudiciel ;

49. Considérant que l'article L. 841-1 du code de la sécurité intérieure, qui met en œuvre le droit à un recours juridictionnel effectif, doit, à l'exception des mots : « *Sous réserve des dispositions particulières prévues à l'article L. 854-1 du présent code,* », être déclaré conforme à la Constitution ;

- SUR CERTAINES DISPOSITIONS DE L'ARTICLE 5 :

50. Considérant que l'article 5 de la loi complète le livre VIII du code de la sécurité intérieure par un titre V intitulé « *Des techniques de recueil de renseignement soumises à autorisation* » au sein duquel il est inséré un chapitre Ier intitulé « *Des accès administratifs aux données de connexion* » comprenant les articles L. 851-1 à L. 851-7 et un chapitre II intitulé « *Des interceptions de sécurité* » comprenant l'article L. 852-1 ;

51. Considérant que les techniques de recueil de renseignement prévues aux articles L. 851-1 à L. 851-6 et à l'article L. 852-1 s'exercent, sauf disposition spécifique, dans les conditions prévues au chapitre Ier du titre II du code de la sécurité intérieure ; qu'ainsi, elles sont autorisées par le Premier ministre, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, après avis préalable de la Commission nationale de contrôle des techniques de renseignement ; que ces techniques ne peuvent être mises en œuvre que par des agents individuellement désignés et habilités ; qu'elles sont réalisées sous le contrôle de la Commission nationale de contrôle des techniques de renseignement ; que la composition et l'organisation de cette autorité administrative indépendante sont définies aux articles L. 831-1 à L. 832-5 du code de la sécurité intérieure dans des conditions qui assurent son indépendance ; que ses missions sont définies aux articles L. 833-1 à L. 833-11 du même code dans des conditions qui assurent l'effectivité de son contrôle ; que, conformément aux dispositions de l'article L. 841-1 du même code, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la Commission nationale de contrôle des techniques de renseignement ; qu'enfin, en application des dispositions de l'article L. 871–6 du même code, les opérations matérielles nécessaires à la mise en place des techniques mentionnées aux articles L. 851-1 à L. 851-4 et L. 852-1 ne peuvent être exécutées, dans leurs réseaux respectifs, que par des agents qualifiés des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications ;

En ce qui concerne les articles L. 851-1 et L. 851-2 du code de la sécurité intérieure :

52. Considérant que l'article L. 851-1 du code de la sécurité intérieure reprend la procédure de réquisition administrative de données techniques de connexion prévue auparavant à l'article L. 246-1 du même code autorisant l'autorité administrative à recueillir des informations ou documents traités ou conservés par leurs réseaux ou services de communications

électroniques, auprès des opérateurs de communications électroniques, auprès des personnes offrant, au titre d'une activité professionnelle principale ou accessoire, au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau et auprès de celles qui assurent, 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 ; que, par exception aux dispositions de l'article L. 821-2 du même code, lorsque la demande sera relative à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ou au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, elle sera directement transmise à la Commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement ;

53. Considérant que l'article L. 851-2 du code de la sécurité intérieure permet à l'administration, pour les seuls besoins de la prévention du terrorisme, de recueillir en temps réel, sur les réseaux des opérateurs et personnes mentionnés à l'article L. 851-1, les informations ou documents mentionnés à ce même article relatifs à une personne préalablement identifiée comme présentant une menace ;

54. Considérant que les députés requérants font valoir que le législateur a méconnu l'étendue de sa compétence en ne définissant pas suffisamment les données de connexion pouvant faire l'objet d'un recueil par les autorités administratives et que la procédure porte une atteinte disproportionnée au droit au respect de la vie privée compte tenu de la nature des données pouvant être recueillies, de l'ampleur des techniques pouvant être utilisées et des finalités poursuivies ;

55. Considérant, en premier lieu, que l'autorisation de recueil de renseignement prévue par les articles L. 851-1 et L. 851-2 porte uniquement sur les informations ou documents traités ou conservés par les réseaux ou services de communications électroniques des personnes mentionnées au considérant 52 ; que selon les dispositions du paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées par les opérateurs de communications électroniques

et les personnes offrant au public une connexion permettant une telle communication portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, les données conservées par les personnes offrant un accès à des services de communication en ligne et celles assurant le stockage de diverses informations pour mise à disposition du public par ces services sont celles 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 ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées ;

56. Considérant, en second lieu, que cette technique de recueil de renseignement est mise en œuvre dans les conditions et avec les garanties rappelées au considérant 51 ; qu'elle ne pourra être mise en œuvre que pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure ; qu'elle est autorisée pour une durée de quatre mois renouvelable conformément à l'article L. 821-4 du même code ; qu'en outre, lorsque le recueil des données a lieu en temps réel, il ne pourra être autorisé que pour les besoins de la prévention du terrorisme, pour une durée de deux mois renouvelable, uniquement à l'égard d'une personne préalablement identifiée comme présentant une menace et sans le recours à la procédure d'urgence absolue prévue à l'article L. 821-5 du même code ; que, par suite, le législateur a assorti la procédure de réquisition de données techniques de garanties propres à assurer entre, d'une part, le respect de la vie privée des personnes et, d'autre part, la prévention des atteintes à l'ordre public et celle des infractions, une conciliation qui n'est pas manifestement déséquilibrée ;

57. Considérant qu'il résulte de tout ce qui précède que les articles L. 851-1 et L. 851-2 du code de la sécurité intérieure doivent être déclarés conformes à la Constitution ;

En ce qui concerne l'article L. 851-3 du code de la sécurité intérieure :

58. Considérant que l'article L. 851-3 du code de la sécurité intérieure prévoit qu'il pourra être imposé aux opérateurs et aux personnes mentionnées à l'article L. 851-1 du même code la mise en œuvre, sur leur réseau, de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ; que ces traitements automatisés utiliseront exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles répondant à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent ; que, lorsque ces traitements détecteront des données susceptibles de caractériser l'existence d'une menace terroriste, l'identification de la ou des personnes concernées et le recueil des données y afférentes pourront être autorisés par le Premier ministre ou par l'une des personnes déléguées par lui ;

59. Considérant que les députés requérants soutiennent que, compte tenu du nombre de données susceptibles d'être contrôlées et de l'insuffisance des garanties concernant les « faux positifs », la technique prévue par ces dispositions porte une atteinte disproportionnée au droit au respect de la vie privée ;

60. Considérant que la technique de recueil de renseignement prévue à l'article L. 851-3 est mise en œuvre dans les conditions et avec les garanties rappelées au considérant 51 ; qu'elle ne peut être mise en œuvre qu'aux fins de prévention du terrorisme ; que tant le recours à la technique que les paramètres du traitement automatisé sont autorisés après avis de la Commission nationale de contrôle des techniques de renseignement ; que la première autorisation d'utilisation de cette technique est délivrée pour une durée limitée à deux mois et que la demande de renouvellement doit comporter un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements ; que les traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent ; que, lorsqu'une donnée détectée par le traitement automatisé

est susceptible de caractériser l'existence d'une menace terroriste, une nouvelle autorisation du Premier ministre sera nécessaire, après avis de la Commission nationale de contrôle des techniques de renseignement, afin d'identifier la personne concernée ; que ces données sont exploitées dans un délai de soixante jours à compter de ce recueil et sont détruites à l'expiration de ce délai sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste ; que l'autorisation d'usage de cette technique ne peut être délivrée selon la procédure d'urgence absolue prévue à l'article L. 821-5 ; que, par suite, ces dispositions ne portent pas une atteinte manifestement disproportionnée au droit au respect de la vie privée ; que les dispositions de l'article L. 851-3 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

En ce qui concerne les articles L. 851-4, L. 851-5 et L. 851-6 du code de la sécurité intérieure :

61. Considérant que l'article L. 851-4 du code de la sécurité intérieure autorise l'autorité administrative à requérir des opérateurs la transmission en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés mentionnés à l'article L. 851-1 ; que, selon l'article L. 851-5, l'autorité administrative peut utiliser un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet ; que l'article L. 851-6 prévoit la possibilité pour cette même autorité de recueillir, au moyen d'un appareil ou d'un dispositif permettant d'intercepter, sans le consentement de leur auteur, des paroles ou des correspondances émises, transmises ou reçues par la voie électronique ou d'accéder à des données informatiques, les données de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ;

62. Considérant que, selon les députés requérants, au regard des finalités justifiant leur mise en œuvre, ces techniques portent une atteinte disproportionnée au droit au respect de la vie privée ;

63. Considérant que les techniques de recueil de renseignement précitées sont mises en œuvre dans les conditions et avec les garanties rappelées au considérant 51 et pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure ; que lorsque la mise en œuvre de la technique prévue à l'article L. 851-5 impose l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3 ; que l'autorisation d'utilisation de la technique prévue à l'article L. 851-6 est délivrée pour une durée de deux mois renouvelable dans les mêmes conditions de durée ; que les appareils ou dispositifs utilisés dans le cadre de cette dernière technique font l'objet d'une inscription dans un registre spécial tenu à la disposition de la Commission nationale de contrôle des techniques de renseignement ; que le nombre maximal de ces appareils ou dispositifs pouvant être utilisés simultanément est arrêté par le Premier ministre, après avis de cette commission ; que les informations ou documents recueillis par ces appareils ou dispositifs doivent être détruits dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre et, en tout état de cause, dans un délai maximal de quatre-vingt-dix jours à compter de leur recueil ; que, dans ces conditions, les dispositions critiquées ne portent pas une atteinte manifestement disproportionnée au droit au respect de la vie privée ; que, par suite, les dispositions des articles L. 851-4, L. 851-5 et L. 851-6 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

En ce qui concerne l'article L. 852-1 du code de la sécurité intérieure :

64. Considérant que le paragraphe I de l'article L. 852-1 du code de la sécurité intérieure autorise les interceptions administratives de correspondances émises par la voie des communications électroniques ; que les personnes appartenant à l'entourage d'une personne concernée par l'autorisation d'interception peuvent également faire l'objet de ces interceptions lorsqu'elles sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation ;

65. Considérant que le paragraphe II de ce même article prévoit que, pour les finalités mentionnées aux 1°, 4° et a) du 5° de l'article L. 811-3, l'utilisation d'un appareil ou d'un dispositif permettant d'intercepter, sans le consentement de leur auteur, des paroles ou des correspondances émises, transmises ou reçues par la voie électronique ou d'accéder à des données

informatiques peut être autorisée afin d'intercepter des correspondances émises ou reçues par un équipement terminal ; que les correspondances interceptées sont détruites dès qu'il apparaît qu'elles sont sans lien avec l'autorisation délivrée, au plus tard trente jours à compter de leur recueil ;

66. Considérant que, selon les députés requérants, au regard des finalités justifiant leur mise en œuvre, ces techniques portent une atteinte disproportionnée au droit au respect de la vie privée ;

67. Considérant que les techniques d'interception de correspondance prévues au paragraphe I de l'article L. 852-1 sont mises en œuvre dans les conditions et avec les garanties rappelées au considérant 51 ; qu'elles ne pourront être mises en œuvre que pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure ; que le nombre maximal des autorisations d'interception en vigueur simultanément est arrêté par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement ; qu'afin de faciliter le contrôle de cette commission, l'exécution de ces interceptions sera centralisée ; qu'en outre, en ce qui concerne les interceptions réalisées au moyen de la technique prévue au paragraphe II de l'article L. 851-2, l'autorisation ne pourra être délivrée que pour certaines des finalités mentionnées à l'article L. 811-3, qui sont relatives à la prévention d'atteintes particulièrement graves à l'ordre public ; que les correspondances ainsi interceptées seront détruites dès qu'il apparaîtra qu'elles sont sans lien avec l'autorisation délivrée et au plus tard trente jours à compter de leur recueil ; qu'il résulte de ce qui précède que le législateur n'a pas, par les dispositions précitées, opéré une conciliation manifestement déséquilibrée entre, d'une part, la prévention des atteintes à l'ordre public et celle des infractions et, d'autre part, le droit au respect de la vie privée et le secret des correspondances ; que, par suite, les dispositions de l'article L. 852-1 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

- SUR CERTAINES DISPOSITIONS DE L'ARTICLE 6 :

68. Considérant que l'article 6 de la loi complète le titre V du livre VIII du code de sécurité intérieure par un chapitre III intitulé « *De la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques* » comprenant les articles L. 853-1 à L. 853-3 et par un chapitre IV intitulé « *Des mesures de surveillance internationale* » comprenant un article L. 854-1 ;

En ce qui concerne les articles L. 853-1 à L. 853-3 du code de la sécurité intérieure :

69. Considérant que l'article L. 853-1 du code de la sécurité intérieure autorise, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé ; que l'article L. 853-2 du même code prévoit, dans les mêmes conditions, l'utilisation de dispositifs techniques permettant d'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre ou d'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ;

70. Considérant que l'article L. 853-3 du code de la sécurité intérieure permet, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'introduction dans un véhicule ou dans un lieu privé aux seules fins de mettre en place, d'utiliser ou de retirer les dispositifs techniques mentionnés aux articles L. 851-5, L. 853-1 et L. 853-2 ;

71. Considérant que les députés requérants soutiennent que ces techniques doivent, compte tenu de leur caractère intrusif, être contrôlées par le juge judiciaire et qu'elles portent une atteinte disproportionnée à l'inviolabilité du domicile et au droit au respect de la vie privée ;

72. Considérant, en premier lieu, que les techniques de recueil de renseignement prévues aux articles L. 853-1 et L. 853-2, mises en place, le cas échéant, en application de l'article L. 853-3, à la suite de l'introduction dans un lieu privé ou dans un véhicule ne constituant pas un lieu privé à usage d'habitation, s'exercent, sauf disposition spécifique, dans les conditions prévues au chapitre Ier du titre II du code de la sécurité intérieure rappelées au considérant 51 ; que ces techniques ne peuvent être utilisées que pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure et si les renseignements recherchés ne peuvent être recueillis par un autre moyen légalement autorisé ; qu'il appartiendra à la Commission nationale de contrôle des techniques de renseignement de s'assurer lors de l'examen de la demande du respect de cette condition ; que l'autorisation est délivrée pour une durée de deux mois ou de trente jours selon la technique utilisée ; que le service autorisé à recourir à la technique de recueil de renseignement rend compte à la commission nationale de contrôle des techniques de renseignement de sa mise en œuvre ; que l'utilisation des dispositifs techniques et, le cas échéant, l'introduction dans un lieu privé ou un véhicule, ne peuvent être le fait que d'agents individuellement désignés et habilités appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 et dont la liste est fixée par décret en Conseil d'État ; que lorsque l'introduction dans un lieu privé ou dans un véhicule est nécessaire pour utiliser un dispositif technique permettant d'accéder à des données stockées dans un système informatique, l'autorisation ne peut être donnée qu'après avis exprès de la Commission nationale de contrôle des techniques de renseignement, statuant en formation restreinte ou plénière ; que l'exigence de cet avis exprès préalable exclut l'application de la procédure d'urgence prévue à l'article L. 821-5 ; qu'il résulte de ce qui précède que le législateur a entouré la mise en œuvre des techniques prévues aux articles L. 853-1 à L. 853-3, le cas échéant lorsqu'elles imposent l'introduction dans un lieu privé ou un véhicule, qui n'est pas à usage d'habitation, de dispositions de nature à garantir que les restrictions apportées au droit au respect de la vie privée ne revêtent pas un caractère manifestement disproportionné ;

73. Considérant, en deuxième lieu, que lorsque la mise en œuvre des techniques de recueil de renseignement prévues aux articles L. 853-1 et L. 853-2 impose l'introduction dans un lieu privé à usage d'habitation, l'autorisation ne peut être donnée qu'après avis exprès de la Commission nationale de contrôle des techniques de renseignement, statuant en formation restreinte ou plénière ; que l'exigence de cet avis exprès préalable exclut l'application de la procédure d'urgence prévue à l'article L. 821-5 ; que, lorsque cette introduction est autorisée après avis défavorable de la Commission nationale de contrôle des techniques de renseignement, le Conseil d'État est immédiatement saisi par le président de la commission ou par l'un des membres de celle-ci mentionnés aux 2° et 3° de l'article L. 831-1 ; que, sauf si l'autorisation a été délivrée pour la prévention du terrorisme et que le Premier ministre a ordonné sa mise en œuvre immédiate, la décision d'autorisation ne peut être exécutée avant que le Conseil d'État ait statué ; qu'il résulte de ce qui précède que le législateur a entouré la mise en œuvre des techniques prévues aux articles L. 853-1 à L. 853-3, lorsqu'elles imposent l'introduction dans un lieu privé à usage d'habitation, de dispositions de nature à garantir que les restrictions apportées au droit au respect de la vie privée et à l'inviolabilité du domicile ne revêtent pas un caractère manifestement disproportionné ;

74. Considérant, en troisième lieu, que les dispositions contestées ne portent pas atteinte à la liberté individuelle ;

75. Considérant qu'il résulte de tout ce qui précède que les articles L. 853-1, L. 853-2 et L. 853-3 du code de la sécurité intérieure doivent être déclarés conformes à la Constitution ;

En ce qui concerne l'article L. 854-1 du code de la sécurité intérieure :

76. Considérant que le paragraphe I de l'article L. 854-1 du code de la sécurité intérieure autorise, aux seules fins de protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code, la surveillance des communications émises ou reçues à l'étranger ; que le deuxième alinéa de ce paragraphe prévoit les mentions que les autorisations de surveillance délivrées en application de cet article devront comporter ; que le troisième alinéa de ce paragraphe indique que ces autorisations seront délivrées sur demande motivée des ministres mentionnés au premier alinéa de l'article L. 821-2 du même code pour une durée de quatre mois renouvelable ; que le

quatrième alinéa de ce paragraphe dispose qu'un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, définit les conditions d'exploitation, de conservation et de destruction des renseignements collectés, ainsi que les conditions de traçabilité et de contrôle par la commission de la mise en œuvre des mesures de surveillance ; que le cinquième alinéa prévoit qu'un décret en Conseil d'État non publié pris après avis de ladite commission et porté à la connaissance de la délégation parlementaire au renseignement précise, en tant que de besoin, les modalités de mise en œuvre de ces mesures de surveillance ;

77. Considérant que les députés requérants soutiennent que ces dispositions méconnaissent le droit au respect de la vie privée ;

78. Considérant qu'en ne définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1, ni celles du contrôle par la Commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre, le législateur n'a pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que, par suite, les dispositions du paragraphe I de l'article L. 854-1, qui méconnaissent l'article 34 de la Constitution, doivent être déclarés contraires à la Constitution ;

79. Considérant qu'il en va de même, par voie de conséquence, des paragraphes II et III du même article L. 854-1, qui en sont inséparables ; qu'il y a également lieu, par voie de conséquence, de déclarer contraires à la Constitution les mots : « *, à l'exception de ceux mentionnés à l'article L. 854-1* » figurant au troisième alinéa de l'article L. 833-2 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi, les mots : « *Sous réserve des dispositions particulières prévues à l'article L. 854-1 du présent code,* » figurant au premier alinéa de l'article L. 841-1 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi, les mots : « *et de l'article L. 854-1 du code de la sécurité intérieure* » figurant à l'article L. 773-1 du code de justice administrative dans sa rédaction résultant de l'article 10 de la loi ainsi que le paragraphe IV de l'article 26 de la loi ;

- SUR CERTAINES DISPOSITIONS DE L'ARTICLE 10 :

80. Considérant que l'article 10 de la loi déférée modifie le code de justice administrative ; que le 1° de cet article 10 insère dans ce code un nouvel article L. 311-4-1 qui attribue au Conseil d'État la compétence pour connaître, en premier et dernier ressort, des requêtes concernant la mise en œuvre des techniques de recueil de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État ; que le 2° de cet article 10 insère dans le titre VII du livre VII un nouveau chapitre III bis intitulé « *Le contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* » comprenant les articles L. 773-1 à L. 773-8 ;

En ce qui concerne l'article L. 773-2 du code de justice administrative :

81. Considérant que l'article L. 773-2 du code de justice administrative est relatif à l'organisation retenue au sein du Conseil d'État pour statuer sur ces requêtes dans le respect du secret de la défense nationale, dont la méconnaissance est sanctionnée par l'article 413-10 du code pénal ; que les premier et deuxième alinéas de l'article L. 773-2 déterminent les formations de jugement appelées à statuer sur ces requêtes au fond ou sur les questions de droit qu'elles sont susceptibles de soulever ; que le troisième alinéa de cet article L. 773-2, d'une part, fixe les modalités d'habilitation au secret de la défense nationale des membres des formations de jugement mentionnées au premier alinéa de l'article, de leur rapporteur public et des agents qui les assistent et, d'autre part, prévoit que les mêmes personnes sont astreintes au respect du secret professionnel et du secret de la défense nationale ; que le quatrième alinéa de l'article L. 773-2 prévoit que les membres de la formation de jugement et le rapporteur public sont autorisés à connaître de l'ensemble des pièces, y compris celles relevant du secret de la défense nationale, en possession soit de la Commission nationale de contrôle des techniques de renseignement soit des services spécialisés de renseignement ou des autres services administratifs, mentionnés respectivement aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure ;

82. Considérant que les dispositions de l'article L. 773-2 du code de justice administrative ne portent pas atteinte au secret de la défense nationale, qui participe des exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation ; qu'elles doivent être déclarées conformes à la Constitution ;

En ce qui concerne les articles L. 773-3, L. 773-4 et L. 773-5 du code de justice administrative :

83. Considérant que les articles L. 773-3, L. 773-4 et L. 773-5 sont relatifs à la prise en compte du secret de la défense nationale pour l'organisation de la procédure contradictoire ;

84. Considérant que l'article L. 773-3 dispose, en son premier alinéa, que les exigences de la contradiction « *sont adaptées à celles du secret de la défense nationale* » ; qu'à cette fin, le deuxième alinéa de cet article prévoit que la Commission nationale de contrôle des techniques de renseignement est informée de toute requête présentée sur le fondement de l'article L. 841-1 du code de la sécurité intérieure ; qu'elle reçoit communication de l'ensemble des pièces produites par les parties et est invitée à présenter des observations écrites ou orales ; que le troisième alinéa du même article prévoit que la formation chargée de l'instruction entend les parties séparément lorsqu'est en cause le secret de la défense nationale ; que l'article L. 773-4 prévoit que le président de la formation de jugement ordonne le huis-clos lorsqu'est en cause ce secret ; que l'article L. 773-5 prévoit que la formation de jugement peut relever d'office tout moyen ;

85. Considérant que les députés requérants reprochent à l'article L. 773-3 de porter atteinte au droit à un procès équitable dès lors qu'il n'opère pas une juste conciliation entre le respect de la procédure contradictoire et celui du secret de la défense nationale ; que, selon eux, la possibilité accordée au juge de relever d'office tout moyen serait insuffisante pour pallier l'absence de respect de la procédure contradictoire ;

86. Considérant que les dispositions des articles L. 773-3 et L. 773-4 ne trouvent à s'appliquer que lorsqu'est en cause le secret de la défense nationale ; qu'eu égard aux possibilités de saisine du Conseil d'État, à l'information donnée à la Commission nationale de contrôle des techniques de renseignement lorsqu'une requête est présentée par une personne, à la possibilité, le cas échéant, donnée à ladite commission de présenter des observations et, enfin, à la possibilité donnée à la formation de jugement de relever d'office tout moyen, le législateur a opéré une conciliation qui n'est

pas manifestement déséquilibrée entre, d'une part, le droit des personnes intéressées à exercer un recours juridictionnel effectif, le droit à un procès équitable et le principe du contradictoire et, d'autre part, les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation, dont participe le secret de la défense nationale ;

87. Considérant que les dispositions des articles L. 773-3, L. 773-4 et L. 773-5 du code de justice administrative doivent être déclarées conformes à la Constitution ;

En ce qui concerne les articles L. 773-6 et L. 773-7 du code de justice administrative :

88. Considérant que l'article L. 773-6 est relatif à la motivation des décisions du Conseil d'État lorsqu'il considère qu'aucune illégalité n'entache la mise en œuvre d'une technique de recueil de renseignement ; que, dans cette hypothèse, la décision se borne à indiquer 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 de recueil de renseignement ; qu'il en va de même en l'absence d'illégalité relative à la conservation de renseignements ;

89. Considérant que l'article L. 773-7 est relatif à la motivation des décisions du Conseil d'État et aux prérogatives de ce dernier lorsqu'il constate qu'une technique de recueil de renseignement est ou a été mise en œuvre irrégulièrement ou qu'un renseignement a été conservé illégalement ; que le premier alinéa de cet article prévoit que le Conseil d'État est compétent pour annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés ; que le deuxième alinéa prévoit que le Conseil d'État, lorsqu'il est saisi par une juridiction sur renvoi préjudiciel ou par la personne intéressée, informe cette dernière ou la juridiction qu'une illégalité a été commise, sans révéler aucun élément couvert par le secret de la défense nationale ; que cet alinéa prévoit également que la formation de jugement, saisie de conclusions indemnitaires, peut condamner l'État à réparer le préjudice subi ; que le troisième alinéa de cet article prévoit que, lorsque la formation de jugement estime que l'illégalité constatée est susceptible de constituer une infraction, elle en avise le procureur de la République ;

90. Considérant que les députés requérants reprochent à l'article L. 773-6 de porter atteinte au droit à un procès équitable dès lors que la motivation des décisions du Conseil d'État rendues lorsqu'aucune illégalité n'a été commise dans la mise en œuvre de techniques de recueil de renseignement ne permet pas à la personne intéressée de savoir si elle a fait ou non l'objet d'une mesure de surveillance ;

91. Considérant que les dispositions de l'article L. 773-6 ne portent, en elles-mêmes, aucune atteinte au droit au procès équitable ; que le Conseil d'État statue en toute connaissance de cause sur les requêtes concernant la mise en œuvre des techniques de recueil de renseignement dont il est saisi sur le fondement de l'article L. 841-1 du code de la sécurité intérieure, dès lors qu'en vertu de l'article L. 773-2 du code de justice administrative, les membres de la formation de jugement et le rapporteur public sont autorisés à connaître de l'ensemble des pièces, y compris celles relevant du secret de la défense nationale, en possession soit de la commission nationale de contrôle des techniques de renseignement soit des services spécialisés de renseignement ou des autres services administratifs, mentionnés respectivement aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure ; qu'en vertu de l'article L. 773-3, la Commission nationale de contrôle des techniques de renseignement est informée de toute requête présentée sur le fondement de l'article L. 841-1, reçoit communication de l'ensemble des pièces produites par les parties et est invitée à présenter des observations écrites ou orales ; qu'en vertu de l'article L. 773-5, la formation de jugement peut relever d'office tout moyen ; qu'ainsi, en adoptant les article L. 773-6 et L. 773-7, le législateur a opéré une conciliation qui n'est pas manifestement déséquilibrée entre, d'une part, le droit des personnes intéressées à exercer un recours juridictionnel effectif et le droit à un procès équitable et, d'autre part, le secret de la défense nationale ;

92. Considérant que les dispositions des articles L. 773-6 et L. 773-7 du code de justice administrative doivent être déclarées conformes à la Constitution ;

93. Considérant qu'il n'y a lieu, pour le Conseil constitutionnel, de soulever d'office aucune autre question de conformité à la Constitution,

D É C I D E :

Article 1er.- Sont contraires à la Constitution les dispositions suivantes de la loi relative au renseignement :

- à l'article 2, l'article L. 821-6, la dernière phrase du premier alinéa de l'article L. 821-7, la deuxième phrase du premier alinéa de l'article L. 832-4, les mots : « *, à l'exception de ceux mentionnés à l'article L. 854-1* » figurant au troisième alinéa de l'article L. 833-2, les mots : « *et L. 821-6* » figurant au septième alinéa de l'article L. 833-9 et les mots : « *Sous réserve des dispositions particulières prévues à l'article L. 854-1 du présent code,* » figurant au premier alinéa de l'article L. 841-1 du code de la sécurité intérieure ;

- à l'article 6, l'article L. 854-1 du code de la sécurité intérieure ;

- à l'article 10, les mots : « *et de l'article L. 854-1 du code de la sécurité intérieure* » figurant à l'article L. 773-1 du code de justice administrative ;

- le paragraphe IV de l'article 26.

Article 2.- Sont conformes à la Constitution les dispositions suivantes de la même loi :

- à l'article 2, les articles L. 811-3, L. 811-4, L. 821-1 et L. 821-5, le surplus de l'article L. 821-7, les articles L. 822-2 et L. 831-1 et le surplus de l'article L. 841-1 du code de la sécurité intérieure ;

- à l'article 5, les articles L. 851-1, L. 851-2, L. 851-3, L. 851-4, L. 851-5, L. 851-6 et L. 852-1 du code de la sécurité intérieure ;

- à l'article 6, les articles L. 853-1, L. 853-2, L. 853-3 du code de la sécurité intérieure ;

- à l'article 10, les articles L. 773-2, L. 773-3, L. 773-4, L. 773-5, L. 773-6 et L. 773-7 du code de justice administrative.

Article 3.- La présente décision sera publiée au Journal officiel de la République française.

Délibéré par le Conseil constitutionnel dans sa séance du 23 juillet 2015, où siégeaient : M. Jean-Louis DEBRÉ, Président, Mmes Claire BAZY MALAURIE, Nicole BELLOUBET, MM. Guy CANIVET, Michel CHARASSE, Renaud DENOIX de SAINT MARC, Lionel JOSPIN et Mme Nicole MAESTRACCI.

Annexe n° 9

Décision du Conseil constitutionnel n° 2015-722 DC du 26 novembre 2015

Loi relative aux mesures de surveillance des communications électroniques internationales

Le Conseil constitutionnel a été saisi, dans les conditions prévues à l'article 61, deuxième alinéa, de la Constitution, de la loi relative aux mesures de surveillance des communications électroniques internationales, sous le numéro 2015-722 DC le 12 novembre 2015, par MM. Bruno RETAILLEAU, Pascal ALLIZARD, Philippe BAS, François BONHOMME, Gilbert BOUCHET, François-Noël BUFFET, Mme Agnès CANAYER, M. Jean-Noël CARDOUX, Mme Caroline CAYEUX, MM. Patrick CHAIZE, Daniel CHASSEING, Alain CHATILLON, Philippe DALLIER, Mme Isabelle DEBRÉ, MM. Francis DELATTRE, Gérard DÉRIOT, Mmes Catherine DEROCHE, Chantal DESEYNE, Catherine DI FOLCO, MM. Eric DOLIGÉ, Philippe DOMINATI, Mme Marie-Annick DUCHÊNE, M. Alain DUFAUT, Mme Nicole DURANTON, M. Louis DUVERNOIS, Mme Dominique ESTROSI SASSONE, M. Michel FORISSIER, Mme Colette GIUDICELLI, M. Daniel GREMILLET, Mme Pascale GRUNY, MM. Alain GOURNAC, Jacques GROSPERRIN, Charles GUENÉ, Alain HOUPERT, Benoît HURÉ, Jean-François HUSSON, Mme Corinne IMBERT, MM. Roger KAROUTCHI, Guy-Dominique KENNEL, Marc LAMÉNIE, Mme Elisabeth LAMURE, MM. Daniel LAURENT, Antoine LEFÈVRE, Dominique de LEGGE, Jean-Baptiste LEMOYNE, Gérard LONGUET, Michel MAGRAS, Didier MANDELLI, Patrick MASCLET, Mmes Colette MÉLOT, Marie MERCIER, Brigitte MICOULEAU, M. Alain MILON, Mme Patricia MORHET-RICHAUD, MM. Philippe MOUILLER, Philippe NACHBAR, Louis NÈGRE, Louis-Jean de NICOLA, Cyril PELLEVAT, Jackie PIERRE, François PILLET,

Rémy POINTEREAU, Ladislas PONIATOWSKI, Hugues PORTELLI, M^me^ Sophie PRIMAS, MM. Michel RAISON, André REICHARDT, Charles REVET, Bruno SIDO, M^me^ Catherine TROENDLÉ, MM. Michel VASPART, Alain VASSELLE et Jean-Pierre VOGEL, sénateurs.

LE CONSEIL CONSTITUTIONNEL,

Vu la Constitution ;

Vu l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel ;

Vu le code de justice administrative ;

Vu le code de la sécurité intérieure ;

Vu les observations du Gouvernement, enregistrées le 23 novembre 2015 ;

Le rapporteur ayant été entendu ;

1. Considérant que plus de soixante sénateurs défèrent au Conseil constitutionnel la loi relative aux mesures de surveillance des communications électroniques internationales ; qu'ils demandent au Conseil constitutionnel de se prononcer sur la conformité au droit au respect de la vie privée, au secret des correspondances et au droit à un recours juridictionnel effectif des articles L. 854-1, L. 854-2, L. 854-5 et L. 854-9 du code de la sécurité intérieure tels qu'ils résultent de l'article 1^er^ de la loi ;

- SUR LES NORMES DE RÉFÉRENCE :

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

3. Considérant qu'en vertu de l'article 5 de la Constitution, le Président de la République est le garant de l'indépendance nationale et de l'intégrité du territoire ; qu'aux termes du premier alinéa de l'article 20 : « *Le Gouvernement détermine et conduit la politique de la Nation* » ; qu'en vertu de l'article 21, le Premier ministre « *dirige l'action du Gouvernement* » et « *est responsable de la Défense nationale* » ; que le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire ;

4. Considérant qu'aux termes de l'article 16 de la Déclaration de 1789 : « *Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution* » ; qu'est garanti par cette disposition le droit des personnes intéressées à exercer un recours juridictionnel effectif ;

- SUR CERTAINES DISPOSITIONS DE L'ARTICLE 1er :

5. Considérant que le 1° de l'article 1er de la loi déférée insère dans le titre V du livre VIII du code de la sécurité intérieure un chapitre IV, comprenant les articles L. 854-1 à L. 854-9, consacré aux mesures de surveillance des communications électroniques internationales ; que les articles L. 854-1, L. 854-2, L. 854-5 et les premier à troisième et le sixième alinéas de l'article L. 854-9 sont relatifs aux conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales ainsi qu'aux conditions d'exploitation, de conservation et de destruction des renseignements collectés, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement ; que les quatrième et cinquième alinéas de l'article L. 854-9 sont relatifs à la procédure juridictionnelle de contrôle de ces mesures de surveillance ;

En ce qui concerne les articles L. 854-1, L. 854-2, L. 854-5 et les premier à troisième et le sixième alinéas de l'article L. 854-9 du code de la sécurité intérieure :

6. Considérant que l'article L. 854-1 autorise la surveillance des communications qui sont émises ou reçues à l'étranger et délimite le champ de celles de ces communications qui sont susceptibles de faire l'objet de mesures de surveillance dans les conditions prévues par les autres dispositions du chapitre IV du titre V du livre VIII du code de la sécurité intérieure ; que cet article prévoit que les mesures prises à ce titre ne peuvent avoir pour objet d'assurer la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, à l'exception du cas où 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, soit sont identifiées comme présentant une menace au regard des intérêts fondamentaux de la Nation ; qu'hormis ces hypothèses, les communications électroniques qui sont échangées entre des personnes ou des équipements utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, lorsqu'elles sont interceptées au moyen des mesures de surveillance prévues par le chapitre IV susmentionné, sont instantanément détruites ;

7. Considérant que l'article L. 854-2 détermine la procédure d'autorisation de mise en œuvre des mesures de surveillance des communications électroniques internationales ; que son paragraphe I fixe les conditions dans lesquelles l'interception des communications émises ou reçues à l'étranger est autorisée ; que son paragraphe II prévoit les conditions dans lesquelles les données de connexion ainsi interceptées peuvent faire l'objet d'une exploitation non individualisée ; que son paragraphe III détermine les conditions dans lesquelles les communications et les données de connexion ainsi interceptées peuvent être exploitées, y compris de manière individualisée ;

8. Considérant que l'article L. 854-5 fixe les durées maximales de conservation des renseignements collectés par la mise en œuvre des mesures de surveillance des communications électroniques internationales, exception faite des correspondances interceptées qui renvoient à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national ; que ces durées sont d'un an à compter de leur première exploitation, dans la limite de quatre ans à compter de leur recueil pour les correspondances interceptées, de six ans à compter de leur recueil pour les données de connexion et de huit ans à compter de leur recueil pour les renseignements chiffrés ;

9. Considérant que les premier à troisième et le sixième alinéas de l'article L. 854-9 sont relatifs aux pouvoirs dont dispose la commission nationale de contrôle des techniques de renseignement pour vérifier si les mesures de surveillance internationale sont régulièrement mises en œuvre ;

10. Considérant, en premier lieu, que le recueil de renseignement au moyen des mesures de surveillance prévues au chapitre IV du titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative ; qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions ; qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs ;

11. Considérant, en deuxième lieu, que l'article L. 854-1 permet la surveillance « *aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3* » ; qu'ainsi, le législateur a précisément circonscrit les finalités permettant de recourir au régime d'autorisation des mesures de surveillance des communications émises ou reçues à l'étranger prévu par l'article L. 854-1 et n'a pas retenu des critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative ;

12. Considérant, en troisième lieu, que l'autorisation d'intercepter des communications électroniques émises ou reçues à l'étranger est délivrée par le Premier ministre et désigne les réseaux de communication sur lesquels les interceptions sont admises ; que l'autorisation d'exploiter ces interceptions est délivrée par le Premier ministre ou par l'un de ses délégués sur demande motivée des ministres de la défense, de l'intérieur ou chargés de l'économie, du budget ou des douanes ou de leurs délégués ; que cette exploitation est réalisée par un service spécialisé de renseignement ; que les autorisations d'interception ou d'exploitation sont délivrées pour une durée limitée ; que l'autorisation d'exploiter de manière non individualisée les données de connexion interceptées précise le type de traitements automatisés pouvant être mis en œuvre ;

13. Considérant, en quatrième lieu, que le législateur a prévu des durées de conservation en fonction des caractéristiques des renseignements collectés ainsi qu'une durée maximale de conservation de huit ans à compter du recueil des renseignements chiffrés, au-delà desquelles les renseignements collectés doivent être détruits ; qu'en outre, en vertu de l'article L. 854-6, les transcriptions ou extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités mentionnées à l'article L. 811-3 ;

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

15. Considérant qu'il résulte de tout ce qui précède que les dispositions des articles L. 854-1, L. 854-2, L. 854-5 et des premier à troisième et sixième alinéas de l'article L. 854-9 ne portent pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances ; que le législateur a précisément défini les conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales, celles d'exploitation, de conservation et de destruction des renseignements collectés ainsi que celles du contrôle exercé par la Commission nationale de contrôle des techniques de renseignement ; que ces dispositions doivent être déclarées conformes à la Constitution ;

En ce qui concerne les quatrième et cinquième alinéas de l'article L. 854-9 du code de la sécurité intérieure :

16. Considérant que le quatrième alinéa de l'article L. 854-9 prévoit que la Commission nationale de contrôle des techniques de renseignement exerce son contrôle de sa propre initiative ou sur réclamation de toute personne souhaitant vérifier qu'aucune mesure de surveillance n'est ou n'a été mise en œuvre irrégulièrement à son égard ; que, lorsqu'elle est saisie d'une réclamation, la commission indique à son auteur qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer la mise en œuvre de mesures de surveillance ;

17. Considérant que le cinquième alinéa de ce même article est relatif aux pouvoirs de la commission lorsqu'elle constate qu'un manquement a été commis dans la mise en œuvre d'une mesure de surveillance internationale ; que la commission adresse au Premier ministre une recommandation tendant à ce que le manquement cesse et que les renseignement collectés soient, le cas échéant, détruits ; que, si le Premier ministre n'a pas donné suite ou a insuffisamment donné suite à cette recommandation, le président de la commission ou trois de ses membres peuvent saisir le Conseil d'État d'une requête dans les conditions prévues par le chapitre III bis du titre VII du livre VII du code de la justice administrative ;

18. Considérant que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure ; qu'en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale ; que les dispositions des quatrième et cinquième alinéas de l'article L. 854-9 doivent être déclarées conformes à la Constitution ;

19. Considérant qu'il n'y a lieu, pour le Conseil constitutionnel, de soulever d'office aucune question de conformité à la Constitution,

D É C I D E :

Article 1er.- Au 1° de l'article 1er de la loi relative aux mesures de surveillance des communications électroniques internationales, sont conformes à la Constitution les articles L. 854-1, L. 854-2, L. 854-5 et L. 854-9 du code de la sécurité intérieure.

Article 2.- La présente décision sera publiée au Journal officiel de la République française.

Délibéré par le Conseil constitutionnel dans sa séance du 26 novembre 2015, où siégeaient : M. Jean-Louis DEBRÉ, Président, Mmes Claire BAZY MALAURIE, Nicole BELLOUBET, MM. Guy CANIVET, Renaud DENOIX de SAINT MARC, Valéry GISCARD d'ESTAING, Jean-Jacques HYEST, Lionel JOSPIN et Mme Nicole MAESTRACCI.

Annexe n° 10

Décision du Conseil constitutionnel n° 2016-590 QPC du 21 octobre 2016

La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne]

LE CONSEIL CONSTITUTIONNEL A ÉTÉ SAISI le 25 juillet 2016 par le Conseil d'État (décision nos 394922, 394925, 397844 et 397851 du 22 juillet 2016), dans les conditions prévues à l'article 61-1 de la Constitution, d'une question prioritaire de constitutionnalité. Cette question a été posée pour les associations La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs et igwan.net, par la SCP Spinosi et Sureau, avocat au Conseil d'État et à la Cour de cassation. Elle a été enregistrée au secrétariat général du Conseil constitutionnel sous le n° 2016-590 QPC. Elle est relative à la conformité aux droits et libertés que la Constitution garantit de l'article L. 811-5 du code de la sécurité intérieure, dans sa rédaction issue de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

Au vu des textes suivants :

- la Constitution ;

- l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel ;

- le code de procédure pénale ;

- le code de la sécurité intérieure ;

- la loi n° 2015-912 du 24 juillet 2015 relative au renseignement ;

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

Au vu des pièces suivantes :

- les observations présentées pour les associations requérantes par la SCP Spinosi et Sureau, enregistrées les 22 août et 6 septembre 2016 ;

- les observations présentées par le Premier ministre, enregistrées le 22 août 2016 ;

- les pièces produites et jointes au dossier ;

Après avoir entendu Me Patrice SPINOSI, avocat au Conseil d'État et à la Cour de cassation, pour les associations requérantes, et M. Xavier POTTIER, désigné par le Premier ministre, à l'audience publique du 11 octobre 2016 ;

Et après avoir entendu le rapporteur ;

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

1. L'article L. 811-5 du code de la sécurité intérieure, dans sa rédaction issue de la loi du 24 juillet 2015 mentionnée ci-dessus, prévoit : « *Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent livre, ni à celles de la sous-section 2 de la section 3 du chapitre Ier du titre III du livre Ier du code de procédure pénale* ».

2. Selon les associations requérantes, en autorisant des mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne sans définir les conditions de collecte, d'exploitation, de conservation et de destruction des renseignements ainsi recueillis et sans prévoir aucun dispositif de contrôle de ces mesures, le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée et au droit à un recours juridictionnel effectif. En outre, il aurait méconnu l'étendue de sa compétence dans des conditions affectant ces mêmes droits.

- Sur le fond :

3. Selon l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression* ». La liberté proclamée par cet article implique le droit au respect de la vie privée et le secret des correspondances. Pour être conformes à la Constitution, les atteintes à ce droit doivent être justifiées par un motif d'intérêt général et mises en œuvre de manière adéquate et proportionnée à cet objectif.

4. Les dispositions contestées permettent aux pouvoirs publics de prendre, à des fins de défense des intérêts nationaux, des mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne. Selon l'article L. 871-2 du code de la sécurité intérieure, pour l'exécution de ces mesures, le ministre de la défense ou le ministre de l'intérieur peuvent requérir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires pour la réalisation et l'exploitation des interceptions autorisées par la loi.

5. Les mesures de surveillance et de contrôle autorisées par les dispositions contestées ne sont pas soumises aux dispositions relatives au renseignement figurant au livre VIII du code de la sécurité intérieure, qui définit les techniques de recueil de renseignement soumises à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement, et qui détermine les voies de recours relatives à la mise en œuvre de ces techniques. Ces mesures ne sont pas non plus soumises aux dispositions de la sous-section 2 de la section 3 du chapitre I^{er} du titre III du livre Ier du code de procédure pénale, qui encadrent les interceptions de correspondances émises par la voie de communications électroniques prescrites par un juge d'instruction.

6. En premier lieu, dès lors qu'elles permettent aux pouvoirs publics de prendre des mesures de surveillance et de contrôle de toute transmission empruntant la voie hertzienne, sans exclure que puissent être interceptées des communications ou recueillies des données individualisables, les dispositions contestées portent atteinte au droit au respect de la vie privée et au secret des correspondances.

7. En deuxième lieu, en prévoyant que les mesures de surveillance et de contrôle peuvent être prises aux seules fins de défense des intérêts nationaux, les dispositions contestées mettent en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation. Toutefois, elles n'interdisent pas que ces mesures puissent être utilisées à des fins plus larges que la seule mise en œuvre de ces exigences.

8. En dernier lieu, les dispositions contestées ne définissent pas la nature des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre. Elles ne soumettent le recours à ces mesures à aucune condition de fond ni de procédure et n'encadrent leur mise en œuvre d'aucune garantie.

9. Il résulte de ce qui précède que, faute de garanties appropriées, les dispositions contestées portent une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration de 1789. Par conséquent et sans qu'il soit besoin d'examiner les autres griefs, l'article L. 811-5 du code de la sécurité intérieure doit être déclaré contraire à la Constitution.

- Sur les effets de la déclaration d'inconstitutionnalité :

10. Selon le deuxième alinéa de l'article 62 de la Constitution : « *Une disposition déclarée inconstitutionnelle sur le fondement de l'article 61-1 est abrogée à compter de la publication de la décision du Conseil constitutionnel ou d'une date ultérieure fixée par cette décision. Le Conseil constitutionnel détermine les conditions et limites dans lesquelles les effets que la disposition a produits sont susceptibles d'être remis en cause* ». En principe, la déclaration d'inconstitutionnalité doit bénéficier à l'auteur de la question prioritaire de constitutionnalité et la disposition déclarée contraire

à la Constitution ne peut être appliquée dans les instances en cours à la date de la publication de la décision du Conseil constitutionnel. Cependant, les dispositions de l'article 62 de la Constitution réservent à ce dernier le pouvoir tant de fixer la date de l'abrogation et de reporter dans le temps ses effets que de prévoir la remise en cause des effets que la disposition a produits avant l'intervention de cette déclaration.

11. 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.

12. 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.

LE CONSEIL CONSTITUTIONNEL DÉCIDE :

Article 1er.- L'article L. 811-5 du code de la sécurité intérieure, dans sa rédaction issue de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, est contraire à la Constitution.

Article 2.- La déclaration d'inconstitutionnalité de l'article 1er prend effet dans les conditions prévues aux paragraphes 11 et 12 de cette décision.

Article 3.- Cette décision sera publiée au Journal officiel de la République française et notifiée dans les conditions prévues à l'article 23-11 de l'ordonnance du 7 novembre 1958 susvisée.

Jugé par le Conseil constitutionnel dans sa séance du 20 octobre 2016, où siégeaient : M. Laurent FABIUS, Président, M[mes] Claire BAZY MALAURIE, Nicole BELLOUBET, MM. Michel CHARASSE, Jean-Jacques HYEST, Lionel JOSPIN, M[mes] Corinne LUQUIENS, Nicole MAESTRACCI et M. Michel PINAULT.

Annexe n° 11

Décision du Conseil d'État statuant au contentieux

N° 396958

Publié au recueil Lebon

Formation spécialisée

M^me^ Catherine DE SALINS, rapporteur

M^me^ Béatrice BOURGEOIS-MACHUREAU, rapporteur public

Lecture du mercredi 19 octobre 2016

AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête et un mémoire en réplique, enregistrés les 10 février et 22 juin 2016 au secrétariat du contentieux du Conseil d'État, M. A... B... demande au Conseil d'État :

1°) de vérifier si des techniques de renseignement ont été mises en œuvre à son égard ;

2°) le cas échéant, de constater qu'elles l'ont été illégalement.

Vu les autres pièces du dossier ;

Vu :

- le code de la sécurité intérieure ;

- le code de justice administrative ;

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

et après avoir entendu en séance :

- le rapport de M^me^ Catherine DE SALINS, conseiller d'État,

- et, hors la présence des parties, les conclusions de M^me^ Béatrice BOURGEOIS-MACHUREAU, rapporteur public ;

1. Aux termes de l'article L. 833-1 du code la sécurité intérieure : « *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, soit le 3 octobre 2015, y compris celles qui, initiées avant cette date, ont continué à être mises en œuvre après.

3. L'article L. 773-6 du code de justice administrative dispose que : « *Lorsque la formation de jugement constate l'absence d'illégalité dans la mise en œuvre d'une technique de recueil de renseignement, la décision indique au requérant ou à la juridiction de renvoi qu'aucune illégalité n'a été commise, sans confirmer ni infirmer la mise en œuvre d'une technique. Elle procède de la même manière en l'absence d'illégalité relative à la conservation des renseignements* » et l'article L. 773-7 du même code : « *Lorsque la formation de jugement constate qu'une technique de recueil de renseignement est ou a été mise en œuvre illégalement ou qu'un renseignement a été conservé illégalement, elle peut annuler l'autorisation et ordonner la destruction des renseignements irrégulièrement collectés./ Sans faire état d'aucun élément protégé par le secret de la défense nationale, elle informe la personne concernée ou la juridiction de renvoi qu'une illégalité a été commise. Saisie de conclusions en ce sens lors d'une requête concernant la mise en œuvre d'une technique de renseignement ou ultérieurement, elle peut condamner l'État à indemniser le préjudice subi./ Lorsque la formation de jugement estime que l'illégalité constatée est susceptible de constituer une infraction, elle en avise le procureur de la République et transmet l'ensemble des éléments du dossier au vu duquel elle a statué à la Commission consultative du secret de la défense nationale, afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République* ». 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, le 23 novembre 2015, la Commission nationale de contrôle des techniques de renseignement (CNCTR) afin de vérifier qu'aucune technique de renseignement n'était irrégulièrement mise en œuvre à son égard. Par lettre du 8 décembre 2015, le président de la CNCTR 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. Dans le dernier état de son argumentation, M. B... demande au Conseil d'État de vérifier si des techniques de renseignement ont été mises en œuvre à son égard et, le cas échéant, de constater qu'elles l'ont été illégalement. Il résulte de ce qui a été dit au point 2 que ces conclusions, qui se rapportent à la mise en œuvre éventuelle de techniques de renseignement postérieurement à l'entrée en vigueur, le 3 octobre 2015, de la loi du 24 juillet 2015, sont recevables, que la décision de les mettre en œuvre ait été prise avant comme après cette date, contrairement à ce que le Premier ministre soutient en défense.

5. 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 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 CNCTR sont destinataires, la formation spécialisée annule le cas échéant l'autorisation et ordonne la destruction des renseignements irrégulièrement collectés.

6. La formation spécialisée a examiné, selon les modalités décrites au point précédent, les éléments fournis par la CNCTR, 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 à M. B... que la vérification qu'il a sollicitée a été effectuée et n'appelle aucune mesure de la part du Conseil d'État.

D E C I D E :

———————

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

Article 2 : 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° 12

Décision du Conseil d'État statuant au contentieux

N° 397623

Mentionné aux tables du recueil Lebon

Formation spécialisée

M. Mattias GUYOMAR, rapporteur

M^me^ Emmanuelle CORTOT-BOUCHER, rapporteur public

Lecture du mercredi 19 octobre 2016

AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête sommaire et un mémoire complémentaire, enregistrés au secrétariat du contentieux du Conseil d'État les 2 mars et 1^er^ juin 2016, M^me^ B... A... demande au Conseil d'État :

1°) de vérifier si des techniques de renseignement ont été mises en œuvre pour surveiller ses communications électroniques internationales ;

2°) le cas échéant, de constater qu'elles l'ont été illégalement ;

3°) de mettre à la charge de l'État une somme de 512 euros au titre de l'article L. 761-1 du code de justice administrative.

Vu les autres pièces du dossier ;

Vu :

- la Constitution ;

- la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;

- le code de la sécurité intérieure ;

- la loi n° 2015-1556 du 30 novembre 2015 ;

- la décision du Conseil constitutionnel n° 2015-722 DC du 26 novembre 2015 ;

- le code de justice administrative ;

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

et après avoir entendu en séance :

- le rapport de M. Mattias GUYOMAR, conseiller d'État,

- et les conclusions de M^me^ Emmanuelle CORTOT-BOUCHER, rapporteur public ;

Considérant ce qui suit :

1. Aux termes de l'article L. 854-9 du code de la sécurité intérieure, issu de la loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales : « *La Commission nationale de contrôle des techniques de renseignement reçoit communication de toutes les décisions et autorisations mentionnées à l'article L. 854-2. Elle dispose d'un accès permanent, complet et direct aux dispositifs de traçabilité mentionnés à l'article L. 854-4, aux renseignements collectés, aux transcriptions et extractions réalisées ainsi qu'aux relevés mentionnés à l'article L. 854-6. À sa demande, elle peut contrôler les dispositifs techniques nécessaires à l'exécution des décisions et des autorisations. Si*

la surveillance des personnes mentionnées au troisième alinéa de l'article L. 854-1 n'a pas déjà fait l'objet d'une autorisation spécifique, leur identité est portée sans délai à la connaissance de la commission. La commission peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions. L'article L. 833-3 est applicable aux contrôles effectués par la commission en application du présent article. De sa propre initiative ou sur réclamation de toute personne souhaitant vérifier qu'aucune mesure de surveillance n'est irrégulièrement mise en œuvre à son égard, la commission s'assure que les mesures mises en œuvre au titre du présent chapitre respectent les conditions qu'il fixe ainsi que celles définies par les textes pris pour son application et par les décisions et autorisations du Premier ministre ou de ses délégués. Elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer la mise en œuvre de mesures de surveillance. Lorsqu'elle constate un manquement au présent chapitre, la commission adresse au Premier ministre une recommandation tendant à ce que le manquement cesse et que les renseignements collectés soient, le cas échéant, détruits. Lorsque le Premier ministre ne donne pas suite à cette recommandation ou que les suites qui y sont données sont estimées insuffisantes, le Conseil d'État, statuant dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, peut être saisi par le président ou par au moins trois membres de la commission. La commission peut adresser à tout moment au Premier ministre les recommandations et les observations qu'elle juge nécessaires au titre du contrôle qu'elle exerce sur l'application du présent chapitre ».

Il résulte de ces dispositions que la Commission nationale de contrôle des techniques de renseignement (CNCTR) exerce son contrôle de sa propre initiative ou sur réclamation de toute personne souhaitant vérifier qu'aucune mesure de surveillance des communications électroniques internationales n'est ou n'a été mise en œuvre irrégulièrement à son égard. Lorsqu'elle constate qu'un manquement a été commis dans la mise en œuvre d'une mesure de surveillance internationale, la Commission adresse au Premier ministre une recommandation tendant à ce que le manquement cesse et que les renseignements collectés soient, le cas échéant, détruits. Si le Premier ministre n'a pas donné suite ou a insuffisamment donné suite à cette recommandation, le président de la Commission ou trois de ses membres peuvent saisir le Conseil d'État d'une requête. Alors même que la personne

faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale en prévoyant que la Commission peut former un recours à l'encontre d'une mesure de surveillance internationale, ainsi que l'a jugé le Conseil constitutionnel dans sa décision n° 2015-722 DC du 26 novembre 2015.

2. Le 2 novembre 2015, Mme A... a saisi la CNCTR d'une demande tendant à vérifier si des techniques de renseignement ont été mises en œuvre pour surveiller ses communications électroniques internationales. Par courrier du 23 décembre 2015, la Commission a informé l'intéressée qu'il avait été procédé aux vérifications nécessaires. Mme A... demande au Conseil d'État de vérifier si des techniques de renseignement ont été mises en œuvre pour surveiller ses communications électroniques internationales et, le cas échéant, de constater, qu'elles sont illégales.

3. Il résulte des dispositions citées au point 1 que Mme A... n'est pas recevable à saisir le Conseil d'État d'une requête dirigée contre la décision du 23 décembre 2015 de la Commission. Il s'ensuit que la fin de non-recevoir opposée par le Premier ministre doit être accueillie.

4. Il résulte de ce qui précède que les conclusions de Mme A... doivent être rejetées, y compris celles présentées au titre de l'article L. 761-1 du code de justice administrative.

D E C I D E :

Article 1er : La requête de Mme A... est rejetée.

Article 2 : La présente décision sera notifiée à Mme B... A..., au Premier ministre et à la Commission nationale de contrôle des techniques de renseignement.

Notes

COMMISSION NATIONALE DE CONTRÔLE
DES TECHNIQUES DE RENSEIGNEMENT

35, rue Saint-Dominique - 75007 Paris
Tél. : 01 42 75 69 31

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Novembre 2016.